Centre de la sécurité des télécommunications
Communications Security Establishment

Conseils en matière de sécurité des technologies de l'information

La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie

Catalogue des contrôles de sécurité

ITSG-33 – Annexe 3A

Décembre 2014

Canada

Avant-propos

L'annexe 3A (*Catalogue des contrôles de sécurité*) du document intitulé *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (ITSG-33) est un document NON CLASSIFIÉ, publié avec l'autorisation du chef du Centre de la sécurité des télécommunications (CST).

Les propositions de modification devraient être envoyées au représentant des Services à la clientèle de la Sécurité des TI du CST par l'intermédiaire des responsables de la sécurité des TI du ministère.

Les demandes de copies supplémentaires ou de modification de la distribution devraient être soumises au représentant des Services à la clientèle de la Sécurité des TI du CST.

Pour de plus amples renseignements, prière de communiquer avec les Services à la clientèle de la Sécurité des TI du CST, par courriel à l'adresse itsclientservices@cse-cst.gc.ca ou par téléphone au 613-991-7654.

Date d'entrée en vigueur

La présente publication entre en vigueur le 30 décembre 2014.

Signé initialement par

Toni Moffa

Chef adjointe, Sécurité des TI

Sommaire

La présente annexe fait partie du document intitulé *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (ITSG-33) de la série Conseils en matière de sécurité des technologies de l'information (TI) publiée par le Centre de la sécurité des télécommunications (CST). Elle contient la définition des contrôles de sécurité sur laquelle les spécialistes de la sécurité peuvent se fonder pour sélectionner les contrôles qui serviront à protéger les systèmes d'information du gouvernement du Canada (GC) et à gérer les risques liés à la sécurité des TI. La présente annexe peut également servir de base à l'élaboration des profils de contrôle de sécurité d'un domaine ou d'un ministère. La mise en œuvre d'un ensemble exhaustif de contrôles de sécurité favorise la réalisation des activités opérationnelles du GC.

La présente annexe comprend la définition des contrôles de sécurité s'appliquant aux ministères qui réalisent des activités opérationnelles aux niveaux de sensibilité et de criticité allant de très faible à très élevé dans des domaines non classifiés, protégés et classifiés.

La présente annexe a été créée comme outil pour faciliter le travail des spécialistes de la sécurité chargés de la protection des systèmes d'information, conformément aux lois du GC ainsi qu'aux politiques, aux directives et aux normes du Secrétariat du Conseil du Trésor (SCT) applicables.

Les annexes 1 et 2 de l'ITSG-33 contiennent des conseils sur la façon d'utiliser le catalogue pour sélectionner les contrôles de sécurité, de même que les améliorations de contrôle afin de protéger les systèmes d'information et de gérer les risques liés à la sécurité des TI.

Table des matières

Avant-propos ..... **ii**

Date d'entrée en vigueur ..... **ii**

Sommaire ..... **iii**

Table des matières ..... **iv**

Liste des figures ..... **xi**

Liste des acronymes, des abréviations et des sigles ..... **xii**

1. Introduction **1**
1.1 Objet 1
1.2 Portée et champ d'application 1
1.3 Auditoire 1
1.4 Structure de la publication 2
1.5 Définitions 2

2. Organisation du document **3**
2.1 Structure du catalogue des contrôles de sécurité 3
2.2 Classes 4
2.3 Familles 4
2.4 Format de la définition des contrôles de sécurité 5

3. Définition des contrôles de sécurité **9**
3.1 FAMILLE : CONTRÔLE D'ACCÈS 10
AC-1 POLITIQUE ET PROCÉDURES DE CONTRÔLE D'ACCÈS 10
AC-2 GESTION DES COMPTES 10
AC-3 APPLICATION DE L'ACCÈS 14
AC-4 APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION 18
AC-5 SÉPARATION DES TÂCHES 23
AC-6 DROIT D'ACCÈS MINIMAL 24
AC-7 TENTATIVES D'OUVERTURE DE SESSION INFRUCTUEUSES 26
AC-8 AVIS D'UTILISATION SYSTÈME 27
AC-9 AVIS D'OUVERTURE DE SESSION PRÉCÉDENTE (ACCÈS) 28
AC-10 CONTRÔLE DE SESSIONS SIMULTANÉES 29
AC-11 VERROUILLAGE DE SESSION 29
AC-12 FIN DE SESSION 30
AC-13 SURVEILLANCE ET EXAMEN — CONTRÔLE D'ACCÈS 31
AC-14 OPÉRATIONS PERMISES SANS IDENTIFICATION NI AUTHENTIFICATION 31
AC-15 MARQUAGE AUTOMATIQUE 31
AC-16 ATTRIBUTS DE SÉCURITÉ 31
AC-17 ACCÈS À DISTANCE 35
AC-18 ACCÈS SANS FIL 36
AC-19 CONTRÔLE D'ACCÈS POUR LES DISPOSITIFS MOBILES 38
AC-20 UTILISATION DE SYSTÈMES D'INFORMATION EXTERNES 39
AC-21 COLLABORATION ET ÉCHANGE D'INFORMATION ENTRE UTILISATEURS 42
AC-22 CONTENU ACCESSIBLE AU PUBLIC 42

AC-23 PROTECTION CONTRE L'EXPLORATION DE DONNÉES 43
AC-24 DÉCISIONS DE CONTRÔLE D'ACCÈS 43
AC-25 MONITEUR DE RÉFÉRENCE 44
3.2 FAMILLE : SENSIBILISATION ET FORMATION 46
AT-1 POLITIQUE ET PROCÉDURES DE FORMATION ET DE SENSIBILISATION À LA SÉCURITÉ 46
AT-2 SENSIBILISATION À LA SÉCURITÉ 46
AT-3 FORMATION À LA SÉCURITÉ AXÉE SUR LES RÔLES 47
AT-4 DOSSIERS DE FORMATION À LA SÉCURITÉ 49
AT-5 CONTACTS AVEC LES GROUPES ET LES ASSOCIATIONS DE SÉCURITÉ 49
3.3 FAMILLE : VÉRIFICATION ET RESPONSABILITÉ 50
AU-1 POLITIQUE ET PROCÉDURES DE VÉRIFICATION ET DE RESPONSABILITÉ 50
AU-2 ÉVÉNEMENTS VÉRIFIABLES 50
AU-3 CONTENU DES ENREGISTREMENTS DE VÉRIFICATION 52
AU-4 CAPACITÉ DE STOCKAGE DES VÉRIFICATIONS 52
AU-5 INTERVENTION EN CAS D'ÉCHECS DE VÉRIFICATION 53
AU-6 EXAMEN, ANALYSE ET RAPPORTS DE VÉRIFICATION 54
AU-7 RÉDUCTION DES VÉRIFICATIONS ET GÉNÉRATION DE RAPPORTS 57
AU-8 ESTAMPILLES TEMPORELLES 58
AU-9 PROTECTION DE L'INFORMATION DE VÉRIFICATION 59
AU-10 NON-RÉPUDIATION 60
AU-11 CONSERVATION DES ENREGISTREMENTS DE VÉRIFICATION 62
AU-12 GÉNÉRATION D'ENREGISTREMENTS DE VÉRIFICATION 62
AU-13 SURVEILLANCE DE LA DIVULGATION D'INFORMATION 63
AU-14 VÉRIFICATION DES SESSIONS 64
AU-15 CAPACITÉ DE VÉRIFICATION SECONDAIRE 64
AU-16 VÉRIFICATION TRANS-ORGANISATIONNELLE 65
3.4 FAMILLE : ÉVALUATION DE SÉCURITÉ ET AUTORISATION 66
CA-1 POLITIQUES ET PROCÉDURES D'ÉVALUATION DE SÉCURITÉ ET D'AUTORISATION 66
CA-2 ÉVALUATIONS DE SÉCURITÉ 66
CA-3 CONNEXIONS DES SYSTÈMES D'INFORMATION 69
CA-4 CERTIFICATION DE SÉCURITÉ 70
CA-5 PLAN D'ACTION ET JALONS 71
CA-6 AUTORISATION DE SÉCURITÉ 71
CA-7 SURVEILLANCE CONTINUE 72
CA-8 TESTS DE PÉNÉTRATION 73
CA-9 CONNEXIONS DES SYSTÈMES D'INFORMATION INTERNES 75
3.5 FAMILLE : GESTION DES CONFIGURATIONS 76
CM-1 POLITIQUE ET PROCÉDURES DE GESTION DES CONFIGURATIONS 76
CM-2 CONFIGURATION DE RÉFÉRENCE 76
CM-3 CONTRÔLE DES CHANGEMENTS DE CONFIGURATION 78
CM-4 ANALYSE CONCERNANT LES RÉPERCUSSIONS SUR LA SÉCURITÉ 80
CM-5 RESTRICTIONS D'ACCÈS CONCERNANT LES CHANGEMENTS 81
CM-6 PARAMÈTRES DE CONFIGURATION 83
CM-7 FONCTIONNALITÉ MINIMALE 84
CM-8 INVENTAIRE DES COMPOSANTS DE SYSTÈME D'INFORMATION 86
CM-9 PLAN DE GESTION DES CONFIGURATIONS 88
CM-10 RESTRICTIONS RELATIVES À L'UTILISATION DES LOGICIELS 89
CM-11 LOGICIELS INSTALLÉS PAR L'UTILISATEUR 90

3.6 FAMILLE : PLANIFICATION D'URGENCE (PLANIFICATION DE LA CONTINUITÉ) 92
CP-1 POLITIQUE ET PROCÉDURES DE PLANIFICATION D'URGENCE 92
CP-2 PLAN D'URGENCE 93
CP-3 FORMATION EN MESURES D'URGENCE 96
CP-4 TESTS ET EXERCICES RELATIFS AU PLAN D'URGENCE 97
CP-5 MISE À JOUR DU PLAN D'URGENCE 98
CP-6 SITE DE STOCKAGE DE SECOURS 98
CP-7 SITE DE TRAITEMENT DE SECOURS 99
CP-8 SERVICES DE TÉLÉCOMMUNICATIONS 100
CP-9 SAUVEGARDE DU SYSTÈME D'INFORMATION 102
CP-10 REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION 103
CP-11 PROTOCOLES DES COMMUNICATIONS DE SECOURS 105
CP-12 MODE SANS ÉCHEC 105
CP-13 MÉCANISMES DE SÉCURITÉ DE SECOURS 105
3.7 FAMILLE : IDENTIFICATION ET AUTHENTIFICATION 107
IA-1 POLITIQUE ET PROCÉDURES D'IDENTIFICATION ET D'AUTHENTIFICATION 107
IA-2 IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS ORGANISATIONNELS) 107
IA-3 IDENTIFICATION ET AUTHENTIFICATION DES DISPOSITIFS 111
IA-4 GESTION DES IDENTIFICATEURS 112
IA-5 GESTION DES AUTHENTIFIANTS 114
IA-6 RÉINJECTION D'AUTHENTIFICATION 118
IA-7 AUTHENTIFICATION DES MODULES CRYPTOGRAPHIQUES 119
IA-8 IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS NON ORGANISATIONNELS) 119
IA-9 IDENTIFICATION ET AUTHENTIFICATION DES SERVICES 120
IA-10 IDENTIFICATION ET AUTHENTIFICATION ADAPTIVES 121
IA-11 RÉAUTHENTIFICATION 121
3.8 FAMILLE : INTERVENTION EN CAS D'INCIDENT 123
IR-1 POLITIQUE ET PROCÉDURES D'INTERVENTION EN CAS D'INCIDENT 123
IR-2 FORMATION SUR LES INTERVENTIONS EN CAS D'INCIDENT 124
IR-3 TESTS ET EXERCICES RELATIFS AUX INTERVENTIONS EN CAS D'INCIDENT 124
IR-4 TRAITEMENT DES INCIDENTS 125
IR-5 SURVEILLANCE DES INCIDENTS 128
IR-6 SIGNALEMENT DES INCIDENTS 128
IR-7 ASSISTANCE EN CAS D'INCIDENT 129
IR-8 PLAN D'INTERVENTION EN CAS D'INCIDENT 130
IR-9 INTERVENTION EN CAS DE FUITE D'INFORMATION 131
IR-10 ÉQUIPE D'ANALYSE DE LA SÉCURITÉ DE L'INFORMATION INTÉGRÉE 132
3.9 FAMILLE : MAINTENANCE 134
MA-1 POLITIQUE ET PROCÉDURES DE MAINTENANCE DES SYSTÈMES 134
MA-2 MAINTENANCE CONTRÔLÉE 134
MA-3 OUTILS DE MAINTENANCE 135
MA-4 TÉLÉMAINTENANCE 137
MA-5 PERSONNEL DE MAINTENANCE 139
MA-6 MAINTENANCE OPPORTUNE 140
3.10 FAMILLE : PROTECTION DES SUPPORTS 142
MP-1 POLITIQUE ET PROCÉDURES DE PROTECTION DES SUPPORTS 142

MP-2 ACCÈS AUX SUPPORTS 142
MP-3 MARQUAGE DES SUPPORTS 143
MP-4 ENTREPOSAGE DES SUPPORTS 144
MP-5 TRANSPORT DES SUPPORTS 145
MP-6 NETTOYAGE DES SUPPORTS 146
MP-7 UTILISATION DES SUPPORTS 148
MP-8 DÉCLASSEMENT DES SUPPORTS 149
3.11 FAMILLE : PROTECTION PHYSIQUE ET ENVIRONNEMENTALE 151
PE-1 POLITIQUE ET PROCÉDURES DE PROTECTION PHYSIQUE ET ENVIRONNEMENTALE 151
PE-2 AUTORISATIONS D'ACCÈS PHYSIQUE 151
PE-3 CONTRÔLE D'ACCÈS PHYSIQUE 153
PE-4 CONTRÔLE D'ACCÈS AUX SUPPORTS DE TRANSMISSION 155
PE-5 CONTRÔLE D'ACCÈS AUX DISPOSITIFS DE SORTIE 156
PE-6 SURVEILLANCE DE L'ACCÈS PHYSIQUE 157
PE-7 CONTRÔLE DES VISITEURS 158
PE-8 REGISTRE DES ACCÈS 158
PE-9 ÉQUIPEMENT ET CÂBLAGE D'ALIMENTATION 158
PE-10 ARRÊT D'URGENCE 159
PE-11 ALIMENTATION D'URGENCE 159
PE-12 ÉCLAIRAGE DE SÉCURITÉ 160
PE-13 PROTECTION CONTRE L'INCENDIE 160
PE-14 CONTRÔLE DE LA TEMPÉRATURE ET DE L'HUMIDITÉ 161
PE-15 PROTECTION CONTRE LES DÉGÂTS D'EAU 162
PE-16 LIVRAISON ET RETRAIT 162
PE-17 AUTRES LIEUX DE TRAVAIL 163
PE-18 EMPLACEMENT DES COMPOSANTS DU SYSTÈME D'INFORMATION 163
PE-19 FUITES D'INFORMATION 164
PE-20 SURVEILLANCE ET SUIVI DES ACTIFS 164
3.12 FAMILLE : PLANIFICATION 166
PL-1 POLITIQUE ET PROCÉDURES DE PLANIFICATION DE LA SÉCURITÉ 166
PL-2 PLAN DE SÉCURITÉ DU SYSTÈME 166
PL-3 MISE À JOUR DU PLAN DE SÉCURITÉ DES SYSTÈMES 168
PL-4 RÈGLES DE CONDUITE 168
PL-5 ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE 169
PL-6 PLANIFICATION DES ACTIVITÉS RELATIVES À LA SÉCURITÉ 169
PL-7 CONCEPTS D'OPÉRATION DE SÉCURITÉ 169
PL-8 ARCHITECTURE DE SÉCURITÉ DE L'INFORMATION 170
PL-9 GESTION CENTRALISÉE 171
3.13 FAMILLE : SÉCURITÉ DU PERSONNEL 173
PS-1 POLITIQUE ET PROCÉDURES DE SÉCURITÉ DU PERSONNEL 173
PS-2 CATÉGORISATION DES POSTES 173
PS-3 ENQUÊTE DE SÉCURITÉ SUR LE PERSONNEL 174
PS-4 CESSATION D'EMPLOI 175
PS-5 TRANSFERT DU PERSONNEL 176
PS-6 ENTENTES D'ACCÈS 177
PS-7 SÉCURITÉ DU PERSONNEL DE TIERCES PARTIES 178
PS-8 SANCTIONS IMPOSÉES AU PERSONNEL 178
3.14 FAMILLE : ÉVALUATION DES RISQUES 180
RA-1 POLITIQUE ET PROCÉDURES D'ÉVALUATION DES RISQUES 180

RA-2 CATÉGORISATION DE SÉCURITÉ 180
RA-3 ÉVALUATION DES RISQUES 181
RA-4 MISE À JOUR DE L'ÉVALUATION DES RISQUES 182
RA-5 ANALYSE DES VULNÉRABILITÉS 182
RA-6 DÉPISTAGE DES CONTRE-MESURES DE SURVEILLANCE TRECHNIQUE 184
3.15 FAMILLE : ACQUISITION DES SYSTÈMES ET DES SERVICES 185
SA-1 POLITIQUE ET PROCÉDURES D'ACQUISITION DES SYSTÈMES ET DES SERVICES 185
SA-2 AFFECTATION DES RESSOURCES 185
SA-3 CYCLE DE DÉVELOPPEMENT DE SYSTÈME 186
SA-4 PROCESSUS D'ACQUISITION 187
SA-5 DOCUMENTATION RELATIVE AUX SYSTÈMES D'INFORMATION 190
SA-6 RESTRICTIONS RELATIVES À L'UTILISATION DES LOGICIELS 192
SA-7 LOGICIELS INSTALLÉS PAR L'UTILISATEUR 192
SA-8 PRINCIPES D'INGÉNIERIE DE SÉCURITÉ 192
SA-9 SERVICES DE SYSTÈME D'INFORMATION EXTERNES 192
SA-10 GESTION DES CONFIGURATIONS PAR LES DÉVELOPPEURS 195
SA-11 TESTS DE SÉCURITÉ EFFECTUÉS PAR LES DÉVELOPPEURS 197
SA-12 PROTECTION DE LA CHAÎNE D'APPROVISIONNEMENT 201
SA-13 FIABILITÉ 205
SA-14 ANALYSE DE CRITICITÉ 206
SA-15 PROCESSUS DE DÉVELOPPEMENT, NORMES ET OUTILS 206
SA-16 FORMATION OFFERTE PAR LE DÉVELOPPEUR 210
SA-17 ARCHITECTURE ET CONCEPTION DE SÉCURITÉ DU DÉVELOPPEUR 210
SA-18 RÉSISTANCE AU TRAFIQUAGE ET DÉTECTION 213
SA-19 AUTHENTICITÉ DES COMPOSANTS 214
SA-20 DÉVELOPPEMENT SUR MESURE DES COMPOSANTS ESSENTIELS 215
SA-21 SÉLECTION DES DÉVELOPPEURS 215
SA-22 COMPOSANTS SYSTÈMES NON PRIS EN CHARGE 216
3.16 FAMILLE : PROTECTION DES SYSTÈMES ET DES COMMUNICATIONS 218
SC-1 POLITIQUE ET PROCÉDURES DE PROTECTION DES SYSTÈMES ET DES COMMUNICATIONS 218
SC-2 PARTITIONNEMENT DES APPLICATIONS 218
SC-3 ISOLEMENT DES FONCTIONS DE SÉCURITÉ 219
SC-4 INFORMATION CONTENUE DANS LES RESSOURCES PARTAGÉES 221
SC-5 PROTECTION CONTRE LES DÉNIS DE SERVICE 222
SC-6 DISPONIBILITÉ DES RESSOURCES 223
SC-7 PROTECTION DES FRONTIÈRES 223
SC-8 CONFIDENTIALITÉ ET INTÉGRITÉ DES TRANSMISSIONS 229
SC-9 CONFIDENTIALITÉ DES TRANSMISSIONS 230
SC-10 DÉCONNEXION RÉSEAU 230
SC-11 CHEMIN DE CONFIANCE 231
SC-12 ÉTABLISSEMENT ET GESTION DES CLÉS CRYPTOGRAPHIQUES 231
SC-13 PROTECTION CRYPTOGRAPHIQUE 232
SC-14 PROTECTION DE L'ACCÈS PUBLIC 234
SC-15 DISPOSITIFS D'INFORMATIQUE COOPÉRATIVE 234
SC-16 TRANSMISSION DES ATTRIBUTS DE SÉCURITÉ 235
SC-17 CERTIFICATS D'INFRASTRUCTURE À CLÉ PUBLIQUE 235
SC-18 CODE MOBILE 236
SC-19 VOIX SUR PROTOCOLE INTERNET 237

SC-20 SERVICE SÉCURISÉ DE RÉSOLUTION DE NOM OU D'ADRESSE (SOURCE AUTORISÉE) 237
SC-21 SERVICE SÉCURISÉ DE RÉSOLUTION DE NOM OU D'ADRESSE (RÉSOLVEUR RÉCURSIF OU CACHE) 238
SC-22 ARCHITECTURE ET FOURNITURE DE SERVICES DE RÉSOLUTION DE NOM OU D'ADRESSE 239
SC-23 AUTHENTICITÉ DES SESSIONS 239
SC-24 DÉFAILLANCE DANS UN ÉTAT CONNU 240
SC-25 NŒUDS LÉGERS 241
SC-26 PIÈGES À PIRATES 241
SC-27 APPLICATIONS INDÉPENDANTES DES PLATEFORMES 241
SC-28 PROTECTION DE L'INFORMATION INACTIVE 242
SC-29 HÉTÉROGÉNÉITÉ 243
SC-30 DISSIMULATION ET DÉTOURNEMENT 243
SC-31 ANALYSE DES VOIES CLANDESTINES 245
SC-32 PARTITIONNEMENT DES SYSTÈMES D'INFORMATION 246
SC-33 INTÉGRITÉ DE LA PRÉPARATION DES TRANSMISSIONS 246
SC-34 PROGRAMMES EXÉCUTABLES NON MODIFIABLES 247
SC-35 CLIENTS-LEURRES 248
SC-36 TRAITEMENT ET STOCKAGE RÉPARTIS 248
SC-37 VOIES DE D'ACHEMINEMENT HORS BANDE 249
SC-38 SÉCURITÉ DES OPÉRATIONS 249
SC-39 ISOLEMENT DES PROCESSUS 250
SC-40 PROTECTION DES LIAISONS SANS FIL 251
SC-41 ACCÈS AUX PORTS ET AUX DISPOSITIFS D'E/S 252
SC-42 CAPACITÉ DE CAPTATION ET DONNÉES 252
SC-43 RESTRICTIONS CONCERNANT L'UTILISATION 254
SC-44 CHAMBRES DE DÉTONATION 254
SC-100 AUTHENTIFICATION DE LA SOURCE 254
SC-101 SYSTÈMES DE TÉLÉCOMMUNICATIONS NON CLASSIFIÉS DANS LES INSTALLATIONS SÉCURISÉES 255
3.17 FAMILLE : INTÉGRITÉ DE L'INFORMATION ET DES SYSTÈMES 257
SI-1 POLITIQUE ET PROCÉDURES LIÉES À L'INTÉGRITÉ DE L'INFORMATION ET DES SYSTÈMES 257
SI-2 CORRECTION DES DÉFAUTS 257
SI-3 PROTECTION CONTRE LES CODES MALVEILLANTS 259
SI-4 SURVEILLANCE DES SYSTÈMES D'INFORMATION 262
SI-5 ALERTES, AVIS ET DIRECTIVES DE SÉCURITÉ 267
SI-6 VÉRIFICATION DE LA FONCTIONNALITÉ DE SÉCURITÉ 268
SI-7 INTÉGRITÉ DES LOGICIELS, DES MICROLOGICIELS ET DE L'INFORMATION 269
SI-8 PROTECTION ANTIPOURRIEL 273
SI-9 RESTRICTIONS RELATIVES À LA SAISIE D'INFORMATION 273
SI-10 VALIDATION DE LA SAISIE D'INFORMATION 273
SI-11 TRAITEMENT DES ERREURS 275
SI-12 TRAITEMENT ET CONSERVATION DES SORTIES D'INFORMATION 276
SI-13 PRÉVENTION DES PANNES PRÉVISIBLES 276
SI-14 NON-PERSISTANCE 277
SI-15 FILTRAGE DES SORTIES D'INFORMATION 278
SI-16 PROTECTION DE LA MÉMOIRE 278
SI-17 PROCÉDURES DE SÉCURITÉ INTÉGRÉE 279

4. Références 280
4.1 Références supplémentaires 285

Liste des figures

Figure 1 – Structure du catalogue des contrôles de sécurité.....3

Liste des acronymes, des abréviations et des sigles

AFU	Approbation d'utilisation (pour *Approval for Use*)
ASCII	*American Standard Code for Information Interchange*
ASM	Agent de sécurité du ministère
CD	Disque compact (pour *Compact Disc*)
CDS	Cycle de développement des systèmes
CEE	*Common Event Expression*
CNB	Code national du bâtiment
CNPI	Code national de prévention des incendies
CNSSI	*Committee on National Security Systems Instructions*
COMSEC	Sécurité des communications (pour *Communications Security*)
CONOPS	Concept d'opération
COTS	Commercial sur étagère (pour *Commercial-off-the-Shelf*)
CST	Centre de la sécurité des télécommunications
CVC	Chauffage, ventilation et climatisation
CVE	Vulnérabilités et expositions courantes (pour *Common Vulnerabilities and Exposures*)
CWE	Énumération des faiblesses courantes (pour *Common Weakness Enumeration*)
DAC	Contrôle d'accès discrétionnaire (pour *Discretionary Access Control*)
DHCP	Protocole DHCP (pour *Dynamic Host Configuration Protocol*)
DMZ	Zone démilitarisée (pour *Demilitarized Zone*)
DNS	Système de noms de domaine (pour *Domain Name System*)
DVD	Disque numérique polyvalent ou disque vidéonumérique (pour *Digital Versatile Disk* ou *Digital Video Disk*)
EAP	Protocole EAP (pour *Extensible Authentification Protocol*)
EMR	Évaluation des menaces et des risques
FIPS	Norme FIPS (pour *Federal Information Processing Standard*)
FTP	Protocole FTP (pour *File Transfer Protocol*)
GC	Gouvernement du Canada
GIS	Gestion de l'information de sécurité
GOTS	Gouvernemental sur étagère (pour *Government-off-the-Shelf*)
GRC	Gendarmerie royale du Canada
HTTP	Protocole de transfert hypertexte (pour *Hypertext Transfer Protocol*)
ICP	Infrastructure à clé publique
ID	Identificateur
IEEE	*Institute of Electrical and Electronics Engineers*

IP	Protocole Internet (pour *Internet Protocol*)
IPv6	Protocole Internet, version 6 (pour *Internet Protocol Version 6*)
ITSB	Bulletin en matière de sécurité des technologies de l'information (pour *Information Technology Security Bulletin*)
ITSD	Directive en matière de sécurité des technologies de l'information (pour *Information Technology Security Directive*)
ITSG	Conseils en matière de sécurité des technologies de l'information (pour *Information Technology Security Guidance*)
ITSPSR	Rapport sur les produits et systèmes de la sécurité des technologies de l'information (pour *Information Technology Security Product and System Review*)
LAN	Réseau local (pour *Local Area Network*)
MAC	Contrôle d'accès au support (pour *Media Access Control*)
MAC	Contrôle d'accès non discrétionnaire (pour *Mandatory Access Control*)
MLS	Sécurité multiniveau (pour *Multilevel Secure* ou *Multilevel Security*)
MSL	Niveau multisécurité (pour *Multiple Security Level*)
NIP	Numéro d'identification personnel
NIST	*National Institute of Standards and Technology*
NTSWG	*National Telecommunications Security Working Group*
PCA	Planification de la continuité des activités
PDF	Format de document portable (pour *Portable Document Format*)
PEAP	Protocole PEAP (pour *Protected Extensible Authentication Protocol*)
PUB	Publication
PVMC	Programme de validation des modules cryptographiques
RBAC	Contrôle d'accès basé sur les rôles (pour *Role-Based Access Control*)
RPV	Réseau privé virtuel
SCAP	Protocole SCAP (pour *Security Content Automation Protocol*)
SCI	Informations sensibles cloisonnées (pour *Sensitive Compartmented Information*)
SCIF	Installation renfermant des informations sensibles cloisonnées (pour *Sensitive Compartmented Information Facility*)
SCT	Secrétariat du Conseil du Trésor du Canada
SSH	Protocole SSH (pour *Secure Shell*)
STI	Système téléphonique informatisé
STIG	*Security Technical Implementation Guide*
STO	Service téléphonique ordinaire
TAD	Répondeur téléphonique (pour *Telephone Answering Device*)
TCP	Protocole de contrôle de transmission (pour *Transmission Control Protocol*)
TFS	Confidentialité du trafic (pour *Traffic Flow Security*)

TLS	Protocole de sécurité de la couche transport (pour *Transport Layer Security*)
TPSGC	Travaux publics et Services gouvernementaux Canada
UHF	Onde décimétrique (pour *Ultra-High Frequency*)
USB	Bus série universel (pour *Universal Serial Bus*)
UTC	Temps universel coordonné (pour *Coordinated Universal Time*)
UUENCODE	Codage UNIX (pour *UNIX to UNIX Encoding*)
VAF	Vérification approfondie de la fiabilité
VHF	Onde métrique (pour *Very High Frequency*)
VoIP	Voix sur protocole Internet (pour *Voice over Internet Protocol*)
XML	Langage de balisage extensible (pour *Extensible Markup Language*)

1. Introduction

1.1 Objet

La présente annexe fait partie du document intitulé *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (ITSG-33) [référence 57] de la série Conseils en matière de sécurité des technologies de l'information (TI) publiée par le Centre de la sécurité des télécommunications (CST). Elle contient la définition des contrôles de sécurité sur laquelle les spécialistes de la sécurité peuvent se fonder pour sélectionner les contrôles qui serviront à protéger les systèmes d'information du gouvernement du Canada (GC) et à gérer les risques liés à la sécurité des TI. La mise en œuvre d'un ensemble exhaustif de contrôles de sécurité favorise la réalisation des activités opérationnelles du GC.

Le catalogue des contrôles de sécurité :

- appuie le respect des lois du GC et des politiques, directives et normes du Secrétariat du Conseil du Trésor du Canada (SCT) en matière de protection des systèmes d'information;
- est conçu pour répondre aux besoins actuels des ministères en matière de protection ainsi qu'aux exigences et aux technologies en évolution constante;
- présente une méthode uniforme et reproductible pour la sélection et la spécification des contrôles de sécurité;
- jette les bases pour l'élaboration de méthodes et de procédures d'évaluation de l'efficacité des contrôles de sécurité;
- améliore la communication en proposant un lexique commun qui facilite la discussion relative à la gestion des risques liés aux TI.

1.2 Portée et champ d'application

Le catalogue des contrôles de sécurité (annexe 3A) comprend la définition des contrôles de sécurité s'appliquant aux ministères qui réalisent des activités opérationnelles aux niveaux de sensibilité et de criticité allant de très faible à très élevé dans des domaines non classifiés, protégés et classifiés.

L'annexe 3A peut aider les spécialistes de la sécurité durant le processus de définition et de mise en œuvre de fonctions de sécurité des TI ministérielles. Elle peut également leur être utile durant le processus de mise en œuvre d'un système d'information lorsque vient le temps de sélectionner les contrôles de sécurité propres au système. Le catalogue peut également servir de base à l'élaboration des profils de contrôle de sécurité d'un domaine ou d'un ministère.

1.3 Auditoire

La présente annexe s'adresse :

- aux agents de sécurité des ministères (ASM), aux coordonnateurs de la sécurité des TI et aux spécialistes de la sécurité appuyant les activités de gestion des risques liés à la sécurité des TI;
- aux personnes qui participent à la définition, à la conception, au développement, à l'installation et à l'exploitation des systèmes d'information et plus particulièrement aux autorisateurs, aux gestionnaires

de projet, aux architectes de sécurité, aux spécialistes de la sécurité, aux évaluateurs de la sécurité et aux membres des groupes opérationnels de TI.

1.4 Structure de la publication

La présente annexe fait partie d'une série de documents portant sur la gestion des risques liés à la sécurité des TI au sein du GC. Les autres documents de la série sont les suivants :

- *ITSG-33, Aperçu – La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*
- *ITSG-33, Annexe 1 – Activités de gestion des risques liés à la sécurité des TI*
- *ITSG-33, Annexe 2 – Activités de gestion des risques liés à la sécurité des systèmes d'information*
- *ITSG-33, Annexe 4A – Profils de contrôle de sécurité*
- *ITSG-33, Annexe 5 – Glossaire*

1.5 Définitions

Pour obtenir une définition des principaux termes utilisés dans la présente annexe, prière de consulter l'annexe 5 de l'ITSG-33.

2. Organisation du document

2.1 Structure du catalogue des contrôles de sécurité

Les contrôles de sécurité définis dans le présent catalogue sont organisés par classe et par famille, tel qu'il est illustré dans la Figure 1. Chacun de ces éléments est détaillé dans les sous-sections suivantes.

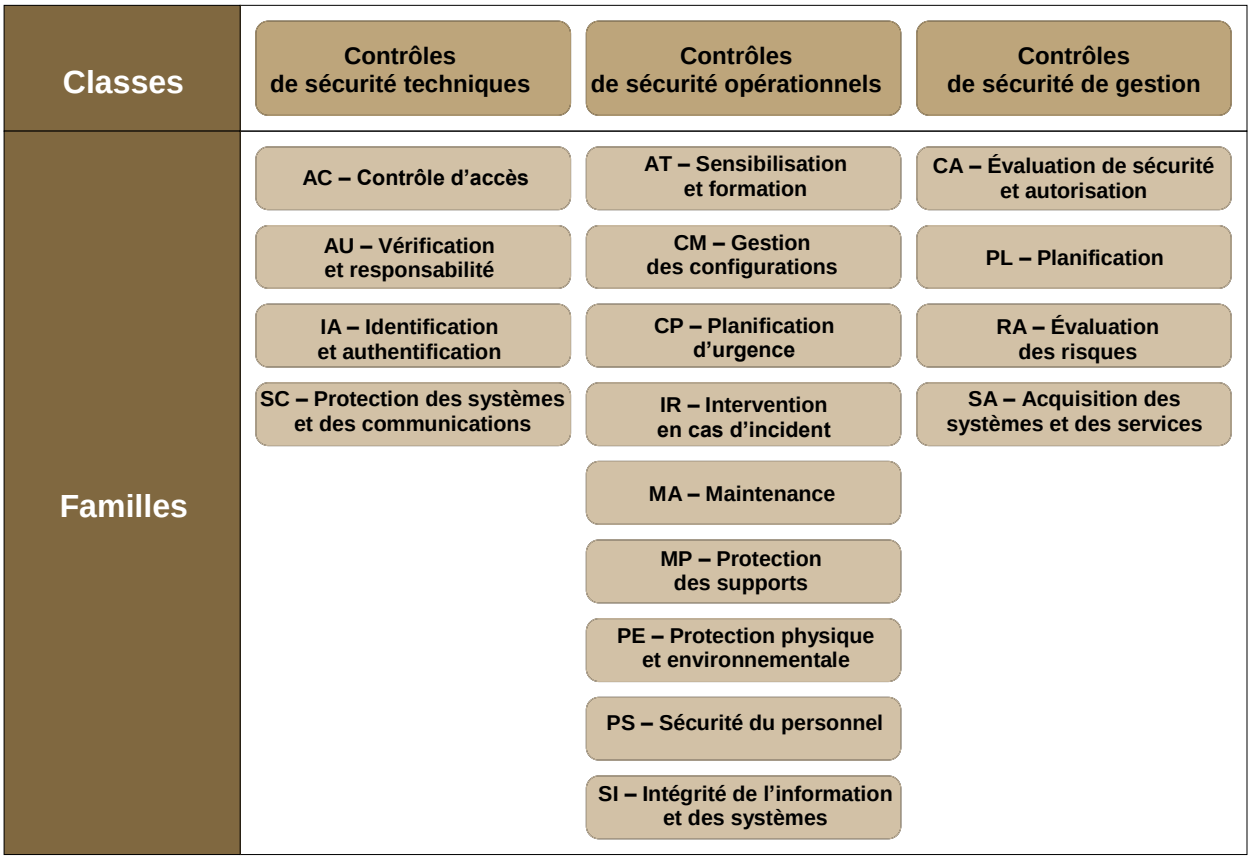

Figure 1 – Structure du catalogue des contrôles de sécurité

2.2 Classes

Les classes de contrôle de sécurité sont définies comme suit :

- la classe *Contrôles de sécurité de gestion* comprend les contrôles de sécurité portant principalement sur les activités qui se rapportent à la gestion de la sécurité des TI et aux risques liés à la sécurité des TI;
- la classe *Contrôles de sécurité techniques* comprend les contrôles de sécurité qui sont mis en œuvre et exécutés par les systèmes d'information principalement par l'intermédiaire de mécanismes de sécurité que l'on retrouve dans les composants matériels, logiciels et micrologiciels;
- la classe *Contrôles de sécurité opérationnels* comprend les contrôles de sécurité des systèmes d'information qui sont mis en œuvre principalement par l'intermédiaire de processus exécutés par des personnes.

Les classes de contrôle de sécurité ne sont pas exclusives. Dans certains cas, il se peut que le personnel doive exécuter des procédures manuelles pour appliquer les fonctionnalités de sécurité de certains contrôles techniques, alors que des contrôles opérationnels pourraient nécessiter le recours à la technologie intégrée au système d'information.

2.3 Familles

Chaque classe de contrôles de sécurité est divisée en famille. La classe Contrôles de sécurité techniques comprend les familles suivantes :

- **Contrôle d'accès :** contrôles permettant d'autoriser ou d'interdire l'accès utilisateur aux ressources dans le système d'information.
- **Vérification et responsabilité :** contrôles permettant de recueillir, d'analyser et de stocker les enregistrements de vérification associés aux opérations utilisateur exécutées dans le système d'information.
- **Identification et authentification :** contrôles permettant de vérifier l'identification unique et l'authentification des utilisateurs qui tentent d'accéder aux ressources du système d'information.
- **Protection des systèmes et des communications :** contrôles permettant de protéger le système d'information lui-même ainsi que ses communications internes et externes.

La classe Contrôles de sécurité opérationnels inclut les familles suivantes :

- **Sensibilisation et formation :** contrôles qui concernent la formation des utilisateurs sur la sécurité du système d'information.
- **Gestion des configurations :** contrôles permettant la gestion et le contrôle de tous les composants du système d'information (p. ex. éléments matériels, logiciels et de configuration).
- **Planification d'urgence :** contrôles permettant d'assurer la disponibilité des services du système d'information dans l'éventualité d'une panne de composant ou d'un désastre.
- **Intervention en cas d'incident :** contrôles permettant de détecter et de signaler les incidents de sécurité liés au système d'information, et d'y intervenir.

- **Maintenance :** contrôles permettant d'assurer la maintenance du système d'information et sa disponibilité permanente.
- **Protection des supports :** contrôles permettant de protéger les supports du système d'information (p. ex. disques et bandes) tout au long de leur cycle de vie.
- **Protection physique et environnementale :** contrôles liés à l'accès physique à un système d'information et à la protection de l'équipement environnemental auxiliaire (c.-à-d. alimentation, climatisation, câblage) servant à son exploitation.
- **Sécurité du personnel :** contrôles servant à appliquer les procédures nécessaires afin de veiller à ce que tout le personnel ayant accès au système d'information possède les autorisations requises ainsi que les niveaux d'habilitation appropriés.
- **Intégrité de l'information et du système :** contrôles permettant de protéger l'intégrité des composants du système d'information et des données traitées par ce système.

La classe Contrôles de sécurité de gestion inclut les familles suivantes :

- **Évaluation de sécurité et autorisation :** contrôles qui concernent l'évaluation de sécurité et l'autorisation du système d'information.
- **Planification :** contrôles qui concernent les activités de planification de la sécurité, y compris les évaluations des facteurs relatifs à la vie privée.
- **Évaluation des risques :** contrôles qui concernent l'exécution des évaluations des risques et de l'analyse des vulnérabilités.
- **Acquisition des systèmes et des services :** contrôles qui concernent la passation de marchés pour l'acquisition des produits et des services nécessaires à la mise en œuvre et à l'exploitation du système d'information.

2.4 Format de la définition des contrôles de sécurité

Le format de la définition des contrôles de sécurité utilisé dans le catalogue est décrit dans la présente section. Un contrôle de sécurité (AC-17 Accès distant) est donné en exemple pour illustrer les divers éléments de la définition :

- Numéro du contrôle : on attribue à chaque contrôle un numéro unique (p. ex. AC-17). **Tous les contrôles dont le numéro commence à la valeur 100 (p. ex. SC-100) sont des contrôles de sécurité propres au Canada.**
- Section *Contrôle* : inclut une description du contrôle de sécurité formulée à l'aide d'un ou de plusieurs énoncés concis portant sur la capacité de sécurité particulière requise pour protéger un aspect d'un système d'information. On attribue une désignation alphabétique distincte (p. ex. (A), (B), etc.) à chaque énoncé; l'énoncé doit être respecté pour que le contrôle de sécurité connexe soit appliqué. **Tous les énoncés qui commencent par AA (p. ex. AC-17 (AA)) sont propres au Canada.**

- Section *Conseils supplémentaires* facultative : inclut de l'information supplémentaire sur le contrôle de sécurité pour en faciliter la mise en œuvre, dont de l'information sur tout autre contrôle de sécurité connexe. Cette section ne comprend aucun énoncé auquel il faut se conformer pour mettre en œuvre le contrôle de sécurité.
- Section *Améliorations du contrôle* facultative : inclut une définition, formulée à l'aide d'énoncés concis, des capacités de sécurité supplémentaires qui permettent d'accroître la robustesse d'un contrôle de sécurité. On attribue à chaque amélioration une désignation numérique distincte (p. ex. (1), (2), etc.). **Toutes les améliorations dont le numéro commence à la valeur 100 (p. ex. AC-17 (100)) sont des améliorations propres au Canada.**
- Section *Conseils supplémentaires sur l'amélioration* : inclut de l'information détaillée supplémentaire sur les améliorations, y compris de l'information sur tout autre contrôle de sécurité connexe. Cette section ne comprend aucune amélioration supplémentaire à laquelle il faut se conformer pour mettre en œuvre l'amélioration du contrôle.
- Section *Références* : inclut des références aux politiques, aux directives, aux normes et aux lignes directrices qui concernent le contrôle de sécurité. Cette section vise à fournir de l'information supplémentaire ou un contexte que le lecteur peut juger utile pour sélectionner et mettre en œuvre le contrôle de sécurité. La portée de la référence peut être de nature générale ou précise, selon le type de contrôle (p. ex. lignes directrices du GC sur l'authentification ou norme technique de configuration de la sécurité).

Un grand nombre des contrôles et des améliorations contiennent des paramètres de contrôle de sécurité définis par l'organisation. Ce sont essentiellement des paramètres substituables que les spécialistes de la sécurité peuvent remplacer, durant le processus de sélection, par des valeurs propres au contexte de leur organisation. À titre d'exemple, prière de consulter le texte en italique dans l'amélioration AC-17 (9) à la page suivante (c.-à-d. *délai défini par l'organisation*).

AC-17 ACCÈS À DISTANCE

Contrôle :

(A) L'organisation définit et consigne les restrictions d'utilisation, les exigences en matière de configuration et de connexion, ainsi que les directives de mise en œuvre de chaque type d'accès à distance autorisé.

(B) L'organisation autorise l'accès à distance au système d'information avant d'autoriser de telles connexions.

(AA) L'organisation s'assure que tous les employés qui travaillent à l'extérieur de ses locaux protègent l'information conformément aux exigences minimales précisées dans la *Norme opérationnelle sur la sécurité matérielle* du SCT [référence 6].

Conseils supplémentaires : Un accès distant est l'accès des utilisateurs (ou des processus exécutés en leur nom) aux systèmes d'information organisationnels à l'aide de réseaux externes (p. ex. Internet). Les méthodes d'accès à distance comprennent notamment l'accès par ligne commutée, à large bande et sans fil. Les organisations utilisent souvent des réseaux privés virtuels (RPV) chiffrés pour augmenter la confidentialité et l'intégrité des connexions à distance. Cette utilisation ne rend pas l'accès non distant; toutefois, lorsque les RPV sont dotés des contrôles de sécurité appropriés (p. ex. employant des techniques de chiffrement pour la protection de la confidentialité et de l'intégrité), leur utilisation peut assurer à l'organisation qu'elle peut traiter ce type de connexion efficacement comme des réseaux internes. Néanmoins, les connexions RPV traversent des réseaux externes, et les RPV chiffrés n'augmentent pas la disponibilité des connexions distantes. Par ailleurs, les RPV dotés de tunnels chiffrés peuvent avoir une incidence sur la capacité de l'organisation de surveiller adéquatement le trafic de communication réseau à des fins de détection de programmes malveillants. Les contrôles d'accès à distance s'appliquent aux systèmes d'information autres que les serveurs Web publics ou les systèmes conçus pour l'accès public. Ce contrôle porte sur l'autorisation avant de permettre l'accès distant, sans préciser les formats de cette autorisation. Bien que les organisations puissent utiliser des ententes sur la sécurité des interconnexions pour autoriser les connexions d'accès à distance, ce contrôle ne requiert pas de telles ententes. Le contrôle AC-3 porte sur l'application des restrictions d'accès pour les connexions à distance. Contrôles connexes : AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10 et SI-4.

Améliorations du contrôle :

(1) ACCÈS À DISTANCE | SURVEILLANCE ET CONTRÔLE AUTOMATISÉS

Le système d'information surveille et contrôle les méthodes d'accès à distance.

Conseils supplémentaires sur l'amélioration : La surveillance et le contrôle automatisés des sessions d'accès à distance permettent aux organisations de détecter les cyberattaques et de s'assurer du respect constant des politiques d'accès à distance grâce à la vérification des activités de connexion des utilisateurs distants sur une variété de composants du système d'information (p. ex. les serveurs, les postes de travail, les ordinateurs bloc-notes, les téléphones intelligents et les tablettes). Contrôles connexes : AU-2 et AU-12.
[…]

(9) ACCÈS À DISTANCE | DÉCONNEXION ET DÉSACTIVATION DE L'ACCÈS

L'organisation fournit la capacité de déconnecter ou de désactiver rapidement l'accès à distance au système d'information dans un délai de [*Affectation : délai défini par l'organisation*].

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle exige que les organisations aient la capacité de déconnecter rapidement à distance les utilisateurs ayant accès au système d'information et/ou de désactiver l'accès distant. La vitesse de la déconnexion ou de la désactivation dépend de la criticité des fonctions opérationnelles et des missions, ainsi que de la nécessité d'éliminer l'accès distant immédiat ou futur aux systèmes d'information organisationnels.

(100) L'accès à distance à des comptes privilégiés s'effectue à partir de consoles de gestion spécialisées régies entièrement par les politiques de sécurité du système et utilisées exclusivement à cette fin (p. ex. l'accès à Internet n'est pas autorisé).

Références :
SCT, *Norme opérationnelle sur la sécurité matérielle* [référence 6].
SCT, *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* [référence 7].

3. Définition des contrôles de sécurité

Cette section définit les contrôles de sécurité.

Pour satisfaire aux besoins du GC en matière d'interopérabilité, le présent catalogue s'inscrit dans la suite logique du catalogue publié par le National Institute of Standards and Technology (NIST) des États-Unis, dans le document intitulé *Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations* [référence 1]. La définition des contrôles a été modifiée et développée pour adapter le catalogue au contexte du GC.

Les contrôles de sécurité présentés dans le catalogue sont susceptibles de changer au fil du temps, dans la mesure où des contrôles seront annulés, révisés et ajoutés. Afin d'assurer la stabilité des plans de sécurité et des outils automatisés de mise en œuvre, les contrôles de sécurité et améliorations de contrôle ne seront pas renumérotés chaque fois qu'un contrôle ou qu'une amélioration est annulé. Les numéros de contrôle ou d'amélioration annulés seront conservés dans le catalogue à des fins historiques.

3.1 FAMILLE : CONTRÔLE D'ACCÈS

CLASSE : TECHNIQUE

AC-1 POLITIQUE ET PROCÉDURES DE CONTRÔLE D'ACCÈS

Contrôle :

(A) L'organisation élabore et consigne, ainsi que diffuse aux [*Affectation : personnel ou rôles définis par l'organisation*] :

(a) une politique de contrôle d'accès qui définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et le respect;

(b) des procédures pour faciliter la mise en œuvre de la politique de contrôle d'accès et des contrôles d'accès connexes.

(B) L'organisation examine et met à jour :

(a) la politique de contrôle d'accès tous les [*Affectation : fréquence définie par l'organisation*];

(b) les procédures de contrôle d'accès tous les [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : Ce contrôle porte sur l'établissement de la politique et les procédures nécessaires à la mise en œuvre efficace des contrôles de sécurité et des améliorations dans la famille AC. La politique et les procédures reflètent les lois du GC ainsi que les politiques, directives et normes du SCT applicables. Les politiques et les procédures du programme de sécurité organisationnel peuvent rendre facultatives les politiques et procédures propres au système. La politique peut être intégrée à la politique générale sur la sécurité de l'information des organisations ou, inversement, elle peut être représentée par de multiples politiques compte tenu de la nature complexe de certaines organisations. Les procédures peuvent être établies pour le programme de sécurité général et pour des systèmes d'information particuliers, au besoin. La stratégie organisationnelle de gestion des risques est un facteur clé dans l'établissement de la politique et des procédures.

Améliorations du contrôle :

Aucune

Références :

SCT, *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* [référence 7].

AC-2 GESTION DES COMPTES

Contrôle :

(A) L'organisation établit et sélectionne les types de compte de système d'information suivants pour appuyer les fonctions opérationnelles et ses missions : [*Affectation : types de compte de système d'information définis par l'organisation*].

(B) L'organisation nomme des gestionnaires de compte pour les comptes de système d'information.

(C) L'organisation établit les conditions pour les membres des groupes et des rôles.

(D) L'organisation précise les utilisateurs autorisés du système d'information, les membres des groupes et des rôles, ainsi que les autorisations d'accès (c.-à-d. les droits d'accès) et autres attributs (au besoin) pour chaque compte.

(E) L'organisation doit obtenir l'approbation de [*Affectation : personnel ou rôles définis par l'organisation*] pour les demandes de création de comptes de système d'information.

(F) L'organisation crée, active, modifie, désactive et retire les comptes de système d'information conformément aux [*Affectation : conditions ou procédures définies par l'organisation*].

(G) L'organisation surveille l'utilisation des comptes de système d'information.

(H) L'organisation informe les gestionnaires de compte :

(a) lorsque les comptes ne sont plus requis;

(b) lorsque les utilisateurs quittent leur poste ou sont transférés;

(c) lorsque l'utilisation du système d'information ou le besoin de connaître d'un utilisateur change.

(I) L'organisation autorise l'accès au système d'information selon :

(a) une autorisation d'accès valide;

(b) l'utilisation prévue du système;

(c) d'autres attributs exigés par l'organisation ou des missions ou fonctions opérationnelles connexes.

(J) L'organisation examine les comptes pour s'assurer qu'ils sont conformes aux exigences en matière de gestion des comptes tous les [*Affectation : fréquence définie par l'organisation*].

(K) L'organisation établit un processus de réattribution des justificatifs d'identité de compte partagé ou de groupe (s'ils sont déployés) lorsque des utilisateurs sont retirés du groupe.

Conseils supplémentaires : Les types de compte de système d'information comprennent, par exemple, les comptes individuels, les comptes partagés, les comptes de groupe, les comptes système, les comptes anonymes ou d'invité, les comptes d'urgence, les comptes de développeur, de fabricant ou de fournisseur, les comptes temporaires ainsi que les comptes de service. Certaines exigences de gestion des comptes énoncées ci-dessus peuvent être mises en œuvre par les systèmes d'information organisationnels. L'identification des utilisateurs autorisés du système d'information et la spécification des privilèges d'accès reflètent les exigences que l'on retrouve dans d'autres contrôles de sécurité dans le plan de sécurité. Les utilisateurs nécessitant des privilèges administratifs sur les comptes du système d'information font l'objet d'un examen plus approfondi de la part des responsables appropriés de l'organisation (p. ex. propriétaire du système, propriétaire de la mission ou des activités, ou coordonnateur de la sécurité des technologies de l'information) chargés d'approuver ces comptes et l'accès privilégié. Les organisations peuvent choisir de définir les privilèges d'accès ou d'autres attributs par compte, par type de compte ou par une combinaison des deux. Les restrictions sur l'heure du jour, le jour de la semaine et le point d'origine sont d'autres exemples possibles d'attributs requis pour autoriser l'accès. Au moment de définir d'autres attributs de compte, les organisations considèrent les exigences liées au système (p. ex. la maintenance prévue et les mises à niveau système) ainsi que les exigences liées à la mission et aux opérations (p. ex. les différences de fuseau horaire, les besoins des clients et l'accès à distance dans le cadre de déplacements). Si les organisations ne considèrent pas ces facteurs, la disponibilité des systèmes d'information risque d'en subir les conséquences. Les comptes temporaires et d'urgence devraient être utilisés à court terme. Les organisations établissent des comptes temporaires dans leurs procédures standards d'activation de compte lorsque les comptes seront utilisés à court terme et que leur activation n'est pas urgente. Les organisations établissent des comptes d'urgence à la suite de situations de crise et lorsqu'il faut activer des comptes rapidement. Par conséquent, l'activation de compte d'urgence risque de contourner les processus standards d'autorisation de compte. Il ne faut pas confondre les comptes temporaires et d'urgence avec les comptes utilisés peu fréquemment

(p. ex. les comptes locaux utilisés pour réaliser des tâches particulières définies par les organisations ou lorsque les ressources réseau ne sont pas disponibles). Ces comptes demeurent activés et ne sont pas assujettis aux dates de retrait ou de désactivation automatique. Les conditions de désactivation des comptes peuvent inclure : (i) lorsque les comptes temporaires, les comptes d'urgence ou les comptes partagés ou de groupe ne sont plus requis; ou (ii) lorsque des utilisateurs sont transférés ou quittent leur poste. Les utilisateurs de certains types de compte de système d'information pourraient être appelés à suivre une formation spécialisée. Contrôles connexes : AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4 et SC-13.

Améliorations du contrôle :

(1) GESTION DES COMPTES | GESTION AUTOMATISÉE DE COMPTE DE SYSTÈME

L'organisation fait appel à des mécanismes automatisés pour appuyer la gestion des comptes du système d'information.

Conseils supplémentaires sur l'amélioration : Les mécanismes automatisés peuvent inclure : l'utilisation de courriels ou de messages texte pour aviser automatiquement les gestionnaires de compte du départ ou du transfert d'utilisateurs; l'utilisation du système d'information pour surveiller l'utilisation du compte; l'utilisation d'avis téléphoniques pour signaler toute utilisation irrégulière de compte.

(2) GESTION DES COMPTES | RETRAIT DES COMPTES TEMPORAIRES ET D'URGENCE

Le système d'information [*Sélection : retire ou désactive*] automatiquement les comptes temporaires et d'urgence après [*Affectation : délai défini par l'organisation pour chaque type de compte*].

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle exige le retrait automatique des comptes temporaires et d'urgence après une période prédéfinie, plutôt qu'à la commodité de l'administrateur système.

(3) GESTION DES COMPTES | DÉSACTIVATION DES COMPTES INACTIFS

Le système d'information désactive automatiquement les comptes inactifs après [*Affectation : délai défini par l'organisation*].

(4) GESTION DES COMPTES | VÉRIFICATION AUTOMATISÉE

Le système d'information vérifie automatiquement les activités de création, de modification, d'activation, de désactivation et de retrait des comptes, et envoie des avis à [*Affectation : personnel ou rôles définis par l'organisation*]. Contrôles connexes : AU-2 et AU-12.

(5) GESTION DES COMPTES | FERMETURE DE SESSION APRÈS UN DÉLAI D'INACTIVITÉ

L'organisation exige que les utilisateurs ferment leur session après [*Affectation : délai d'inactivité prévu ou description du moment de la fermeture de session défini par l'organisation*]. Contrôles connexes : SC-23.

(6) GESTION DES COMPTES | GESTION DYNAMIQUE DES DROITS D'ACCÈS

Le système d'information met en œuvre les capacités suivantes de gestion dynamique des droits d'accès : [*Affectation : liste des capacités de gestion dynamique des droits d'accès définie par l'organisation*].

Conseils supplémentaires sur l'amélioration : Contrairement aux approches conventionnelles de contrôle d'accès qui utilisent des comptes de système d'information statiques et des ensembles prédéfinis de droits d'accès utilisateur, les approches de contrôle d'accès dynamique (p. ex. les architectures orientées services) misent sur des décisions de contrôle d'accès valorisées à l'exécution et facilitées par une gestion dynamique des droits d'accès. Quoique les identités d'utilisateur puissent demeurer relativement constantes au fil du temps, il est possible que les droits d'accès changent plus fréquemment selon les exigences de la mission et des opérations ainsi que selon les besoins opérationnels des organisations. La gestion dynamique des droits d'accès comprend notamment la révocation immédiate des droits d'accès des utilisateurs, par opposition à forcer les utilisateurs à mettre fin à leur session et à en ouvrir une nouvelle pour refléter les changements de droits d'accès. La gestion dynamique des droits d'accès peut également désigner les mécanismes qui modifient les droits d'accès des utilisateurs en fonction de règles dynamiques,

au lieu de modifier les profils d'utilisateur précis. Ce type de gestion des droits d'accès peut inclure des ajustements automatiques des droits d'accès si les utilisateurs travaillent en dehors de leurs heures normales de travail ou si les systèmes d'information sont dans des situations contraignantes ou de maintenance d'urgence. Cette amélioration peut également inclure les effets complémentaires des changements de droits d'accès, dont les changements potentiels aux clés de chiffrement utilisées pour les communications. La gestion dynamique des droits d'accès peut appuyer les exigences en matière de résilience des systèmes d'information. Contrôle connexe : AC-16.

(7) GESTION DES COMPTES | PLANS BASÉS SUR LES RÔLES

(a) L'organisation établit et administre les comptes utilisateur privilégiés conformément à un plan de contrôle d'accès basé sur les rôles qui regroupe l'accès et les droits d'accès au système d'information permis par rôle.

(b) L'organisation surveille les attributions de rôles privilégiés.

(c) L'organisation prend [*Affectation : mesures définies par l'organisation*] lorsque les attributions de rôles privilégiés ne conviennent plus.

Conseils supplémentaires sur l'amélioration : Les rôles privilégiés sont des rôles définis par l'organisation qui sont attribués aux utilisateurs pour leur permettre d'exécuter certaines fonctions de sécurité qu'ils ne sont pas habituellement autorisés à exécuter. Ces rôles privilégiés comprennent notamment la gestion des clés, la gestion des comptes, l'administration des réseaux et des systèmes, l'administration des bases de données et l'administration Web.

(8) GESTION DES COMPTES | CRÉATION DYNAMIQUE DE COMPTES

Le système d'information crée [*Affectation : comptes de système d'information définis par l'organisation*] de façon dynamique.

Conseils supplémentaires sur l'amélioration : Les approches dynamiques de création de comptes de système d'information (p. ex. telles qu'elles sont mises en œuvre dans des architectures orientées services) ont recours à l'établissement de comptes (identités) en temps réel dans le cas des entités jusque-là inconnues. Les organisations planifient la création dynamique de comptes de système d'information en établissant des mécanismes et des relations de confiance avec les autorités appropriées pour valider les autorisations et droits d'accès connexes. Contrôle connexe : AC-16.

(9) GESTION DES COMPTES | RESTRICTIONS LIÉES À L'UTILISATION DE COMPTES PARTAGÉS ET DE COMPTES DE GROUPE

L'organisation autorise uniquement l'utilisation des comptes partagés et de groupe qui répondent aux *[Affectation : conditions relatives à l'établissement de comptes partagés et de groupe définies par l'organisation*].

(10) GESTION DES COMPTES | SUPPRESSION DES JUSTIFICATIFS D'IDENTITÉ DE COMPTES PARTAGÉS ET DE COMPTES DE GROUPE

Le système d'information supprime les justificatifs d'identité des comptes partagés ou de groupe lorsque les membres quittent le groupe.

(11) GESTION DES COMPTES | CONDITIONS D'UTILISATION

Le système d'information applique [*Affectation : circonstances et/ou conditions d'utilisation définies par l'organisation*] aux [*Affectation : comptes du système d'information définis par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les organisations peuvent décrire les conditions ou les circonstances particulières selon lesquelles les comptes du système d'information peuvent être utilisés, par exemple en limitant l'utilisation à certains jours de la semaine, à certaines heures du jour ou à une durée précise.

(12) GESTION DES COMPTES | SURVEILLANCE ET UTILISATION IRRÉGULIÈRE DES COMPTES

(a) L'organisation surveille les comptes de système d'information afin de détecter [*Affectation : utilisation irrégulière définie par l'organisation*].

(b) L'organisation signale l'utilisation irrégulière des comptes de système d'information à [*Affectation : personnel ou rôles définis par l'organisation*].

Conseils supplémentaires sur l'amélioration : L'utilisation irrégulière peut comprendre l'accès à des systèmes d'information à des heures précises de la journée et à partir d'endroits qui ne correspondent pas aux habitudes d'utilisation régulières des employés de l'organisation. Contrôle connexe : CA-7.

(13) GESTION DES COMPTES | DÉSACTIVATION DES COMPTES DES UTILISATEURS À RISQUE ÉLEVÉ

L'organisation désactive les comptes des utilisateurs qui présentent un risque élevé dans un délai de [*Affectation : délai défini par l'organisation*] après la découverte du risque.

Conseils supplémentaires sur l'amélioration : Les utilisateurs présentant un risque élevé pour les organisations comprennent les personnes sur lesquelles des preuves fiables ou du renseignement révèlent leur intention d'utiliser un accès autorisé aux systèmes d'information pour causer un préjudice ou pour permettre à des adversaires de causer un préjudice. Ces préjudices pourraient nuire aux activités et aux biens organisationnels, aux employés, à d'autres organisations ou au Canada. La coordination étroite entre les autorités responsables, les administrateurs de système d'information et les gestionnaires des ressources humaines est essentielle à l'exécution opportune de cette amélioration. Contrôle connexe : PS-4.

Références :

Aucune

AC-3 APPLICATION DE L'ACCÈS

Contrôle :

(A) Le système d'information applique les autorisations approuvées pour l'accès logique aux ressources du système et à l'information conformément aux politiques de contrôle d'accès applicables.

Conseils supplémentaires : Les politiques de contrôle d'accès (p. ex. politiques basées sur l'identité, sur les rôles ou sur les attributs) et les mécanismes d'application de l'accès (p. ex. listes de contrôle d'accès, matrices de contrôle d'accès, cryptographie) contrôlent l'accès entre les sujets ou entités actifs (c.-à-d. les utilisateurs ou les processus exécutés en leur nom) et les objets ou entités passifs (p. ex. dispositifs, fichiers, enregistrements, domaines) dans les systèmes d'information. En plus d'appliquer l'accès autorisé au système d'information et de reconnaître que les systèmes d'information peuvent héberger de nombreuses applications et services à l'appui des missions et des activités opérationnelles de l'organisation, les mécanismes d'application de l'accès peuvent également servir aux applications et aux services en vue de fournir une meilleure sécurité de l'information. Contrôles connexes : AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5 et PE-3.

Améliorations du contrôle :

(1) APPLICATION DE L'ACCÈS | ACCÈS LIMITÉ AUX FONCTIONS PRIVILÉGIÉES

[Annulée : Intégrée au contrôle AC-6]

(2) APPLICATION DE L'ACCÈS | DOUBLE AUTORISATION

Le système d'information applique une double autorisation pour [*Affectation : commandes privilégiées ou autres mesures définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : L'exécution des mécanismes de double autorisation exige l'approbation de deux personnes autorisées. Les organisations n'ont pas besoin de mécanismes de double autorisation lorsqu'il faut agir immédiatement pour assurer la sécurité publique et environnementale. La double autorisation est également appelée le contrôle par deux personnes. Contrôles connexes : CP-9 et MP-6.

(3) APPLICATION DE L'ACCÈS | CONTRÔLE D'ACCÈS NON DISCRÉTIONNAIRE

Le système d'information applique [*Affectation : politiques de contrôle d'accès non discrétionnaire définies par l'organisation*] à tous les sujets et objets lorsque la politique précise :

(a) que la politique est appliquée de façon uniforme pour tous les sujets et objets dans les frontières du système d'information;

(b) qu'un sujet ayant reçu l'accès à l'information est contraint :

- d'acheminer l'information à des sujets ou à des objets non autorisés;
- d'octroyer ses droits d'accès à d'autres sujets;
- de changer un ou plusieurs attributs de sécurité pour des sujets, des objets, le système d'information ou des composants du système d'information;
- de choisir les attributs de sécurité et les valeurs d'attribut qui seront associés aux objets nouvellement créés ou modifiés;

ou

- de changer les règles régies par le contrôle d'accès;

(c) Les [*Affectation : sujets définis par l'organisation*] peuvent accorder explicitement [*Affectation : droits d'accès définis par l'organisation (c.-à-d. sujets de confiance)*], de façon à ce qu'ils ne soient pas limités par les contraintes ci-dessus.

Conseils supplémentaires sur l'amélioration : Le contrôle d'accès non discrétionnaire ne se limite pas seulement à certaines utilisations historiques (p. ex. les mises en œuvre au moyen du modèle Bell-LaPadula). La classe ci-dessus de politiques de contrôle d'accès non discrétionnaire limite les opérations que peuvent exécuter les sujets par rapport à l'information obtenue des objets de données auxquels l'accès leur a déjà été accordé, ce qui empêche les sujets de transmettre de l'information à des sujets ou à des objets non autorisés. Elle limite également les opérations que peuvent exécuter les sujets en ce qui a trait à la propagation des privilèges de contrôle d'accès, à savoir qu'un sujet ayant un privilège ne peut pas le transmettre à d'autres sujets. La politique est appliquée de façon uniforme pour tous les sujets et objets que contrôle le système d'information. Autrement, la politique de contrôle d'accès peut être contournée. Cette application est habituellement assurée par une mise en œuvre qui répond au concept de contrôleur de référence (voir AC-25). La politique est délimitée par les frontières du système d'information (c.-à-d. une fois que l'information sort du contrôle du système, des moyens additionnels seront peut-être nécessaires pour s'assurer que les contraintes imposées sur l'information demeurent en vigueur). Les droits d'accès accordés aux sujets de confiance décrits ci-dessus sont conformes au concept du droit d'accès minimal (voir AC-6). Les sujets de confiance reçoivent seulement les droits d'accès minimaux relatifs à la politique ci-dessus qui sont nécessaires afin de satisfaire les besoins de l'organisation liés à la mission et aux opérations. Le contrôle s'applique particulièrement lorsqu'il existe un mandat (p. ex. une loi, un décret, une directive ou un règlement) qui établit une politique concernant l'accès à l'information sensible ou classifiée, où certains utilisateurs du système d'information ne sont pas autorisés à accéder à toute l'information sensible ou classifiée contenue dans le système d'information. Ce contrôle peut être appliqué en conjonction avec le contrôle AC-3 (4). Un sujet dont les activités sont limitées par les politiques de ce contrôle est toujours en mesure de réaliser ses activités en vertu des contraintes moins rigoureuses du contrôle AC-3 (4), mais les politiques du présent contrôle ont préséance sur les contraintes moins rigoureuses du contrôle AC-3 (4). Par exemple, bien qu'une politique de contrôle d'accès non discrétionnaire impose une contrainte empêchant un sujet de transmettre de l'information à un sujet ayant une étiquette de sensibilité différente, le contrôle AC-3 (4) permet au sujet de transmettre de l'information à des sujets ayant la même étiquette de sensibilité que celle du sujet. Contrôles connexes : AC-25 et SC-11.

(4) APPLICATION DE L'ACCÈS | CONTRÔLE D'ACCÈS DISCRÉTIONNAIRE

Le système d'information applique [*Affectation : politiques de contrôle d'accès discrétionnaire définies par l'organisation*] à des sujets et objets définis quand la politique précise qu'un sujet à qui l'accès à l'information a été accordé peut réaliser l'un ou l'autre des aspects suivants :

(a) acheminer l'information à des sujets ou à des objets;

(b) octroyer ses droits d'accès à d'autres sujets;

(c) changer des attributs de sécurité de sujets, d'objets, du système d'information ou de composants du système d'information;

(d) choisir les attributs de sécurité qui seront associés aux objets nouvellement créés ou modifiés;

ou

(e) changer les règles régies par le contrôle d'accès.

Conseils supplémentaires sur l'amélioration : Lors de la mise en œuvre des politiques de contrôle d'accès discrétionnaire, les sujets ne sont pas limités quant aux opérations qu'ils peuvent exécuter par rapport à l'information à laquelle ils ont déjà reçu l'accès. Ainsi, les sujets ayant déjà obtenu l'accès à l'information sont autorisés à transmettre (c.-à-d. ils peuvent choisir de transmettre) l'information à d'autres sujets ou à d'autres objets. Cette amélioration peut être appliquée en parallèle avec le contrôle AC-3 (3). Un sujet dont les activités sont limitées par les politiques du contrôle AC-3 (3) peut toujours effectuer ses activités selon les contraintes moins rigoureuses de cette amélioration de contrôle. Par conséquent, bien que le contrôle AC-3 (3) impose des contraintes empêchant un sujet de transmettre de l'information à un sujet travaillant à un niveau de sensibilité différent, le contrôle AC-3 (4) permet au sujet de transmettre de l'information à des sujets ayant le même niveau de sensibilité que celui du sujet. La politique est délimitée par les limites du système d'information. Une fois que l'information sort du contrôle du système d'information, des moyens additionnels seront peut-être nécessaires pour s'assurer que les contraintes imposées demeurent en vigueur. Alors que les définitions anciennes et traditionnelles du contrôle d'accès discrétionnaire exigeaient le contrôle d'accès basé sur l'identité, il n'est pas nécessaire d'appliquer cette limite à l'utilisation du contrôle d'accès discrétionnaire.

(5) APPLICATION DE L'ACCÈS | INFORMATION PERTINENTE EN MATIÈRE DE SÉCURITÉ

Le système d'information empêche l'accès à [*Affectation : information pertinente en matière de sécurité définie par l'organisation*] sauf lorsqu'il est en état de non-fonctionnement sécurisé.

Conseils supplémentaires sur l'amélioration : L'information pertinente en matière de sécurité désigne toute information dans les systèmes d'information susceptible d'influer sur l'exécution des fonctions de sécurité ou sur la prestation des services de sécurité, de telle façon qu'elle nuirait à l'application des politiques de sécurité du système ou à l'isolation du code et des données. L'information pertinente en matière de sécurité comprend notamment les règles de filtrage des routeurs et des coupe-feux, l'information de gestion des clés cryptographiques, les paramètres de configuration des services de sécurité et les listes de contrôle d'accès. Les systèmes d'information dans un état de non-fonctionnement sécurisé comprennent également les périodes où ils n'effectuent aucun traitement lié à la mission ou aux opérations (p. ex. le système a été mis hors ligne aux fins de maintenance, de dépannage, d'amorçage ou d'arrêt). Contrôle connexe : CM-3.

(6) APPLICATION DE L'ACCÈS | PROTECTION DE L'INFORMATION DU SYSTÈME ET DES UTILISATEURS

[Annulée : Intégrée aux contrôles MP-4 et SC-28]

(7) APPLICATION DE L'ACCÈS | CONTRÔLE D'ACCÈS BASÉ SUR LES RÔLES

Le système d'information applique une politique de contrôle d'accès basé sur les rôles à des sujets et objets définis, et il contrôle l'accès en fonction des [*Affectation : rôles et utilisateurs autorisés pour assumer ces rôles définis par l'organisation*].

Conseils supplémentaires sur l'amélioration : Le contrôle d'accès basé sur les rôles (RBAC) désigne une politique de contrôle d'accès qui limite l'accès au système d'information aux utilisateurs autorisés. Les organisations peuvent créer des rôles précis selon les fonctions du poste et les autorisations (c.-à-d. droits d'accès) nécessaires en vue d'exécuter les opérations requises sur les systèmes d'information organisationnels associés aux rôles définis par l'organisation. Lorsque les rôles organisationnels sont attribués aux utilisateurs, ceux-ci héritent des autorisations ou des privilèges définis pour ces rôles. Le RBAC simplifie l'administration des droits d'accès des organisations puisque les droits d'accès ne sont pas attribués directement à chaque utilisateur (ce qui peut représenter un nombre considérable d'utilisateurs pour les moyennes et grandes organisations), mais plutôt à des rôles. Le RBAC peut être mis en œuvre de façon discrétionnaire ou non. Pour les organisations mettant en œuvre le RBAC avec des contrôles d'accès non discrétionnaire, les exigences du contrôle AC-3 (3) définissent la portée des sujets et des objets couverts par la politique.

(8) APPLICATION DE L'ACCÈS | RÉVOCATION DES AUTORISATIONS D'ACCÈS

Le système d'information applique la révocation des autorisations d'accès à la suite de changements apportés aux attributs de sécurité des sujets et des objets en fonction des [*Affectation : règles régissant le moment de la révocation des autorisations d'accès définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : La révocation des règles d'accès peut être différente selon les types d'accès révoqué. Par exemple, si un sujet (c.-à-d. un utilisateur ou un processus) est retiré d'un groupe, il se peut que l'accès ne soit pas révoqué jusqu'à ce que l'objet (p. ex. un fichier) soit ouvert de nouveau ou jusqu'à ce que le sujet tente d'accéder de nouveau à l'objet. La révocation fondée sur les changements aux étiquettes de sécurité peut entrer en vigueur sur-le-champ. Les organisations peuvent fournir d'autres approches pour l'application immédiate des révocations dans les cas où les systèmes d'information sont incapables d'offrir cette capacité si elle est obligatoire.

(9) APPLICATION DE L'ACCÈS | DIFFUSION CONTRÔLÉE

Le système d'information ne diffuse pas l'information hors des frontières établies du système, à moins que :

(a) le [*Affectation : système d'information ou composant système défini par l'organisation*] destinataire fournisse [*Affectation : mesures de protection de sécurité définies par l'organisation*];

(b) les [*Affectation : mesures de protection de sécurité définies par l'organisation*] soient utilisées pour valider la pertinence de l'information désignée à des fins de diffusion.

Conseils supplémentaires sur l'amélioration : Les systèmes d'information peuvent seulement protéger de l'information organisationnelle dans les frontières établies du système. Des mesures de protection de sécurité additionnelles pourraient être nécessaires pour veiller à ce que cette information soit protégée de façon adéquate une fois qu'elle sort des frontières établies du système d'information. Ces mesures additionnelles s'appliquent par exemple à l'information transmise à un système d'information externe ou à l'information imprimée sur l'une de ses imprimantes. Si le système d'information est incapable de déterminer la convenance des mesures de protection fournies par des entités hors de ses frontières, à titre de contrôle d'atténuation, les organisations devraient établir, en fonction des procédures, si les systèmes d'information externes fournissent un niveau de sécurité adéquat. Les moyens servant à déterminer la convenance de la sécurité assurée par les systèmes d'information externe comprennent notamment la conduite d'inspections ou de tests périodiques, l'établissement d'ententes entre l'organisation et les organisations homologues ou d'autres processus. Les mécanismes qu'utilisent les entités externes pour protéger l'information reçue peuvent être différents de ceux qu'emploie l'organisation, mais ils doivent être suffisants afin de statuer sur la politique de sécurité pour protéger l'information. Cette amélioration de contrôle exige que les systèmes d'information se servent de mécanismes techniques ou procéduraux pour valider l'information avant de la diffuser à des systèmes externes. Par exemple, si le système d'information transmet l'information à un autre système contrôlé par une autre organisation, les mécanismes techniques servent à confirmer que les attributs de sécurité associés à l'information exportée sont appropriés pour le système destinataire. Autrement, si le système d'information transmet de l'information à une imprimante dans un espace contrôlé par l'organisation, des mécanismes procéduraux peuvent être mis en œuvre pour s'assurer que seules les personnes autorisées peuvent accéder à l'imprimante. Cette amélioration s'applique surtout lorsqu'il existe un mandat politique (p. ex. une loi, un décret, une directive ou un règlement) qui établit une politique sur l'accès à l'information et que celle-ci s'applique au-delà d'un système d'information ou d'une organisation.

(10) APPLICATION DE L'ACCÈS | DÉROGATION VÉRIFIÉE AUX MÉCANISMES DE CONTRÔLE D'ACCÈS

L'organisation utilise une dérogation vérifiée aux mécanismes automatisés de contrôle d'accès en vertu des [*Affectation : conditions définies par l'organisation*]. Contrôles connexes : AU-2 et AU-6.

Références :

Aucune

AC-4 APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION

Contrôle :

(A) Le système d'information applique des autorisations approuvées pour contrôler le flux d'information dans le système et entre les systèmes interconnectés en fonction des [*Affectation : politiques de contrôle de flux d'information définies par l'organisation*].

Conseils supplémentaires : Le contrôle de flux d'information régit le cheminement de l'information au sein d'un système d'information et entre des systèmes d'information (par opposition aux personnes autorisées à y accéder), quels que soient les accès subséquents à cette information. Les restrictions en matière de contrôle de flux comprennent notamment : empêcher l'information contrôlée à des fins d'exportation d'être transférée en clair vers Internet; bloquer le trafic entrant qui prétend provenir de l'intérieur de l'organisation; restreindre les demandes Web dans Internet qui ne proviennent pas du serveur mandataire Web interne; limiter les transferts d'information entre les organisations en fonction du contenu et des structures de données. Le transfert d'information entre des systèmes d'information représentant différents domaines de sécurité avec différentes politiques de sécurité comporte un risque de contravention à une ou à plusieurs politiques de sécurité des domaines. Dans de telles situations, les propriétaires ou gardiens de l'information fournissent des directives aux points désignés d'application des politiques entre les systèmes interconnectés. Les organisations devraient examiner la possibilité d'imposer des solutions architecturales précises lorsqu'elles doivent appliquer des politiques de sécurité précises. L'application comprend notamment : (i) l'interdiction de transférer de l'information entre systèmes interconnectés (c.-à-d. permettre l'accès à l'information seulement); (ii) l'utilisation de mécanismes matériels pour imposer des flux d'information unidirectionnels; (iii) la mise en œuvre de mécanismes remaniés de confiance pour réassigner les attributs et étiquettes de sécurité.

Les organisations utilisent couramment les mécanismes d'application et politiques de contrôle de flux d'information pour contrôler le flux d'information entre des sources et des destinations précises (p. ex. réseaux, utilisateurs et dispositifs) à l'intérieur des systèmes d'information et entre les systèmes interconnectés. Le contrôle de flux est fondé sur les caractéristiques de l'information et/ou sur son chemin. Le contrôle de flux est appliqué, par exemple, dans les dispositifs de protection des frontières (p. ex. passerelles, routeurs, gardiens, tunnels chiffrés et coupe-feux) qui utilisent des ensembles de règles ou établissent des paramètres de configuration limitant les services du système d'information et offrant une capacité de filtrage des paquets basée sur l'information d'en-tête ou une capacité de filtrage des messages basée sur le contenu (p. ex. en mettant en œuvre des recherches de mots-clés ou en utilisant les caractéristiques d'un document). Les organisations devraient également considérer la fiabilité des mécanismes de filtrage et d'inspection (c.-à-d. les composants matériels, micrologiciels et logiciels) qui sont essentiels à l'application du contrôle de flux d'information. Les améliorations 3 à 22 portent principalement sur les besoins en matière de solutions interdomaines, lesquels sont axés sur des techniques de filtrage avancées, l'analyse approfondie et des mécanismes d'application du contrôle de flux d'information mis en œuvre dans les produits interdomaines comme les gardiens à assurance élevée. De telles capacités ne sont généralement pas offertes dans des produits de technologies de l'information commerciaux sur étagère. Contrôles connexes : AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7 et SC-18.

Améliorations du contrôle :

(1) APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION | ATTRIBUTS DE SÉCURITÉ DES OBJETS

Le système d'information utilise des [*Affectation : attributs de sécurité définis par l'organisation*] associés aux [*Affectation : objets d'information, de source et de destination définis par l'organisation*] pour appliquer les [*Affectation : politiques de contrôle de flux d'information définies par l'organisation*] comme base pour les décisions concernant le contrôle de flux.

Conseils supplémentaires sur l'amélioration : Les mécanismes d'application du contrôle de flux d'information comparent les attributs de sécurité associés à l'information (contenu et structure de données) avec des objets de source et de destination, et interviennent de manière appropriée (p. ex. blocage, mise en quarantaine, avertissement de l'administrateur) lorsqu'ils identifient des flux d'information non explicitement autorisés par les politiques de contrôle de flux d'information. Par exemple, un objet d'information étiqueté Secret serait autorisé à être transmis à un objet de destination étiqueté Secret, mais un objet d'information étiqueté Très secret ne serait pas autorisé à être transmis à un objet de destination étiqueté Secret. Les attributs de sécurité peuvent inclure notamment les adresses source et destination utilisées dans les coupe-feux qui filtrent le trafic. L'application du contrôle de flux d'information basée sur des attributs de sécurité explicites peut servir, par exemple, à contrôler la diffusion de certains types d'information. Contrôle connexe : AC-16.

(2) APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION | DOMAINES DE TRAITEMENT

Le système d'information utilise des domaines de traitement protégés pour appliquer les [*Affectation : politiques de contrôle de flux d'information définies par l'organisation*] comme base pour les décisions concernant le contrôle de flux.

Conseils supplémentaires sur l'amélioration : Dans les systèmes d'information, les domaines de traitement protégés sont des espaces de traitement ayant des interactions contrôlées avec d'autres espaces de traitement, permettant ainsi le contrôle des flux d'information entre les espaces, de même qu'en provenance et à destination des objets de données ainsi que des objets d'information. Un domaine de traitement protégé peut être établi, par exemple, en mettant en œuvre un domaine et une application type. Dans le domaine et l'application type, les processus du système d'information sont attribués aux domaines; l'information est identifiée par type; les flux d'information sont contrôlés selon les accès autorisés à l'information (déterminés par domaine et type), selon la signalisation autorisée entre les domaines et selon les transitions de processus autorisées vers d'autres domaines.

(3) APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION | CONTRÔLE DYNAMIQUE DE FLUX D'INFORMATION

Le système d'information applique le contrôle dynamique de flux d'information en fonction des [*Affectation : politiques définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les politiques organisationnelles liées au contrôle dynamique de flux d'information comprennent notamment la permission ou l'interdiction des flux d'information en fonction de conditions changeantes ou de motifs liés à la mission et aux opérations. Les conditions changeantes peuvent être des changements dans la tolérance au risque de l'organisation en raison de changements dans l'immédiateté des besoins relatifs à la mission et aux opérations, des changements dans l'environnement de menace et la détection d'événements potentiellement préjudiciables et néfastes. Contrôle connexe : SI-4.

(4) APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION | VÉRIFICATION DU CONTENU DE L'INFORMATION CHIFFRÉE

Le système d'information empêche l'information chiffrée de contourner les mécanismes de vérification de contenu en [*Sélection (un ou plusieurs) : déchiffrant l'information; bloquant le flux d'information chiffrée; en mettant fin aux sessions de communication qui tentent d'acheminer l'information chiffrée;* [*procédure ou méthode définie par l'organisation*]]. Contrôle connexe : SI-4

(5) APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION | TYPES DE DONNÉES INTÉGRÉS

Le système d'information applique des [*Affectation : restrictions définies par l'organisation*] concernant l'intégration de types de données dans d'autres types de données.

Conseils supplémentaires sur l'amélioration : L'intégration de types de données dans d'autres types de données pourrait réduire l'efficacité du contrôle de flux. Les types de données intégrés comprennent notamment l'insertion de fichiers exécutables à titre d'objets dans les fichiers de traitement de texte, l'insertion de références ou d'information descriptive dans un fichier multimédia, et les types de données comprimées ou archivées qui peuvent contenir de multiples types de données intégrés. Les limites relatives à l'intégration de types de données considèrent les niveaux d'intégration et interdisent les niveaux d'intégration qui dépassent les capacités des outils d'inspection.

(6) APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION | MÉTADONNÉES

Le système d'information applique le contrôle de flux d'information en fonction des [*Affectation : métadonnées définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les métadonnées désignent de l'information servant à décrire les caractéristiques des données. Elles comprennent les métadonnées structurales décrivant des structures de données (p. ex. le format, la syntaxe et la sémantique des données) ou les métadonnées descriptives décrivant du contenu de données (p. ex. l'âge, le lieu et le numéro de téléphone). L'application des flux d'information permis en fonction des métadonnées simplifie et améliore le contrôle de flux. Les organisations considèrent la fiabilité des métadonnées selon l'exactitude des données (c.-à-d. la connaissance que les valeurs de métadonnées sont correctes par rapport aux données), l'intégrité des données (c.-à-d. la protection contre les changements non autorisés aux étiquettes de métadonnées) et la liaison entre les métadonnées et les données utiles (c.-à-d. des techniques solides et suffisantes de liaison ainsi que des niveaux appropriés d'assurance). Contrôles connexes : AC-16 et SI-7.

(7) APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION | MÉCANISMES DE FLUX UNIDIRECTIONNELS

Le système d'information applique des [*Affectation : flux unidirectionnels définis par l'organisation*] en utilisant des mécanismes matériels.

(8) APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION | FILTRES DE POLITIQUE DE SÉCURITÉ

Le système d'information applique le contrôle de flux d'information en utilisant des [*Affectation : filtres de politique de sécurité définis par l'organisation*] comme base pour les décisions de contrôle de flux pour les [*Affectation : flux d'information définis par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les filtres de politique de sécurité définis par l'organisation peuvent s'appliquer au contenu et aux structures de données. Par exemple, les filtres de politique de sécurité pour les structures de données peuvent chercher la taille maximale des fichiers, la taille maximale des champs ainsi que les types de données et de fichiers (pour les données structurées et non structurées). Les filtres de politique de sécurité pour le contenu des données peuvent chercher des mots précis (p. ex. filtres de mots à proscrire ou à autoriser), des valeurs énumérées ou des intervalles de valeur de données et du contenu caché. Les données structurées permettent l'interprétation du contenu des données par application. Les données non structurées désignent habituellement l'information numérique sans structure de données précise ou avec une structure de données qui ne permet pas d'élaborer des ensembles de règles pour traiter la sensibilité précise de l'information contenue dans les données ou les décisions connexes relatives à l'application du contrôle de flux. Les données non structurées comprennent : (i) les objets binaires, essentiellement indépendants de tout langage (c.-à-d. les fichiers d'images, les fichiers vidéo ou les fichiers audio); (ii) les objets textuels associés à des langages écrits ou imprimés (p. ex. des documents de traitement de texte, des feuilles de calcul ou des courriels de systèmes commerciaux). Les organisations peuvent mettre en œuvre plus d'un filtre de politique de sécurité pour atteindre les objectifs liés au contrôle de flux d'information (p. ex. l'utilisation de listes de mots autorisés et de listes de mots proscrits pourrait réduire les faux positifs).

(9) APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION | EXAMENS HUMAINS

Le système d'information applique l'utilisation d'examens humains pour les [*Affectation : flux d'information définis par l'organisation*] selon les modalités suivants : [*Affectation : modalités définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les organisations définissent les filtres de politique de sécurité pour toutes les situations dans lesquelles des décisions automatisées liées au contrôle de flux peuvent être prises. Lorsqu'une décision entièrement automatisée liée au contrôle de flux ne peut être prise, on peut faire appel à un examen humain au lieu du filtrage automatisé de politique de sécurité ou à titre de complément au filtrage automatisé. Les organisations peuvent faire appel aux examens humains lorsqu'elles le jugent nécessaire.

(10) APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION | ACTIVATION ET DÉSACTIVATION DES FILTRES DE POLITIQUE DE SÉCURITÉ

Le système d'information permet aux administrateurs privilégiés d'activer ou de désactiver les [*Affectation : filtres de politique de sécurité définis par l'organisation*] selon les modalités suivantes : [*Affectation : modalités définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Par exemple, comme le permet le système d'information, les administrateurs peuvent activer les filtres de politique de sécurité pour les types de données approuvés.

(11) APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION | CONFIGURATION DES FILTRES DE POLITIQUE DE SÉCURITÉ

Le système d'information permet aux administrateurs privilégiés de configurer les [*Affectation : filtres de politique de sécurité définis par l'organisation*] pour prendre en charge différentes politiques de sécurité.

Conseils supplémentaires sur l'amélioration : Par exemple, pour tenir compte des modifications apportées aux politiques de sécurité, les administrateurs peuvent changer la liste des mots à proscrire vérifiée par les mécanismes de politique de sécurité, conformément aux définitions fournies par les organisations.

(12) APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION | IDENTIFICATEURS DE TYPE DE DONNÉES

Le système d'information, lors du transfert d'information entre différents domaines de sécurité, utilise des [*Affectation : identificateurs de type de données définis par l'organisation*] pour valider les données essentielles aux décisions liées au flux d'information.

Conseils supplémentaires sur l'amélioration : Les identificateurs de type de données comprennent entre autres les noms de fichier, les types de fichier, les signatures et jetons de fichier ainsi que les signatures et jetons multiples de fichier interne. Les systèmes d'information peuvent autoriser le transfert de données seulement s'il est conforme aux spécifications du format de type de données.

(13) APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION | DÉCOMPOSITION EN SOUS-COMPOSANTS PERTINENTS

Le système d'information, lors du transfert d'information entre différents domaines de sécurité, décompose l'information en [*Affectation : sous-composants pertinents définis par l'organisation*] pour la présenter aux mécanismes d'application de politique.

Conseils supplémentaires sur l'amélioration : Les mécanismes d'application des politiques appliquent des règles de filtrage, d'inspection et/ou de nettoyage aux sous-composants d'information pertinents afin de faciliter l'application du contrôle de flux avant de transférer l'information à des domaines de sécurité différents. L'analyse syntaxique des fichiers de transfert facilite les décisions de politique concernant la source, la destination, les certificats, la classification, les pièces jointes et les autres différenciateurs de composants liés à la sécurité.

(14) APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION | CONTRAINTES RELATIVES AUX FILTRES DE POLITIQUE DE SÉCURITÉ

Le système d'information, lors du transfert d'information entre différents domaines de sécurité, applique des [Affectation : *filtres de politique de sécurité définis par l'organisation*] qui exigent des formats entièrement énumérés limitant le contenu et la structure des données.

Conseils supplémentaires sur l'amélioration : Les restrictions relatives au contenu et à la structure des données réduisent l'éventail de contenu potentiellement malveillant ou illicite dans les transactions interdomaines. Les filtres de politique de sécurité qui restreignent les structures de données comprennent notamment la restriction de la taille des fichiers et des champs. Les filtres de politique pour le contenu de données comprennent, par exemple : (i) le codage des formats pour les jeux de caractères (p. ex. les formats de transformation du jeu universel de caractères et le code normalisé américain pour l'échange d'information); (ii) la restriction des champs de caractère pour qu'ils comportent uniquement des caractères alphanumériques; (iii) l'interdiction des caractères spéciaux; (iv) la validation des structures de schéma.

(15) APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION | DÉTECTION DE L'INFORMATION NON AUTORISÉE

Le système d'information, lors du transfert d'information entre différents domaines de sécurité, examine l'information afin de détecter la présence de [*Affectation : information non autorisée définie par l'organisation*] et interdit le transfert de cette information, conformément à la [*Affectation : politique de sécurité définie par l'organisation*].

Conseils supplémentaires sur l'amélioration : La détection d'information non autorisée comprend notamment la vérification de toute l'information qui sera transférée afin de détecter les programmes malveillants et les mots à proscrire. Contrôle connexe : SI-3.

(16) APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION | TRANSFERTS D'INFORMATION SUR DES SYSTÈMES INTERCONNECTÉS

[Annulée : Intégrée au contrôle AC-4]

(17) APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION | AUTHENTIFICATION DES DOMAINES

Le système d'information identifie de façon unique et authentifie les points source et destination par [Sélection (un ou plusieurs) : organisation, système, application, personne] à des fins de transfert d'information.

Conseils supplémentaires sur l'amélioration : L'attribution est une composante essentielle d'un concept d'opération de la sécurité. La capacité d'identifier les points source et destination de l'information circulant dans des systèmes d'information permet, le cas échéant, de reconstruire les événements à des fins judiciaires et d'encourager le respect des politiques en attribuant à des organisations ou à des personnes précises les infractions à la politique. Pour que l'authentification du domaine réussisse, les étiquettes du système d'information doivent faire la distinction entre les systèmes, les organisations et les personnes qui participent à la préparation, à l'envoi, à la réception ou à la diffusion de l'information. Contrôles connexes : IA-2, IA-3, IA-4 et IA-5.

(18) APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION | LIAISON D'ATTRIBUT DE SÉCURITÉ

Le système d'information lie des attributs de sécurité à l'information au moyen de [*Affectation : techniques de liaison définies par l'organisation*] pour faciliter l'application de la politique sur le flux d'information.

Conseils supplémentaires sur l'amélioration : Les techniques de liaison que les systèmes d'information mettent en œuvre nuisent à la force de la liaison entre les attributs de sécurité et l'information. La force de la liaison et l'assurance associée aux techniques de liaison jouent un rôle important dans la confiance qu'accordent les organisations au processus d'application du contrôle de flux d'information. Les techniques de liaison ont une incidence sur le nombre et le degré d'examens supplémentaires que devront exécuter les organisations. Contrôles connexes : AC-16 et SC-16.

(19) APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION | VALIDATION DES MÉTADONNÉES

Le système d'information, lors du transfert d'information entre différents domaines de sécurité, applique le même filtrage de politique de sécurité aux métadonnées qu'aux données utiles.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle exige la validation des métadonnées et des données auxquelles s'appliquent les métadonnées. Certaines organisations font une distinction entre les métadonnées et les données utiles (c.-à-d. seules les données auxquelles sont liées les métadonnées). D'autres organisations ne font pas cette distinction et considèrent plutôt que les métadonnées ainsi que les données auxquelles les métadonnées s'appliquent font partie des données utiles. Toute l'information (y compris les métadonnées de même que les données auxquelles les métadonnées s'appliquent) est assujettie au filtrage et à l'inspection.

(20) APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION | SOLUTIONS APPROUVÉES

Les organisations utilisent des [*Affectation : solutions définies par l'organisation dans les configurations approuvées*] pour contrôler le flux de [*Affectation : information définie par l'organisation*] dans les domaines de sécurité.

Conseils supplémentaires sur l'amélioration : Les organisations définissent les configurations et solutions approuvées dans les politiques et directives interdomaines conformément aux types de flux d'information dans les limites de la classification. Le CST fournit une liste de base des solutions interdomaines approuvées.

(21) APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION | SÉPARATION PHYSIQUE ET LOGIQUE DES FLUX D'INFORMATION

Le système d'information sépare les flux d'information de façon logique ou physique au moyen de [*Affectation : mécanismes et/ou techniques définis par l'organisation*] pour accomplir les [*Affectation : séparations requises par type d'information définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : L'application de la séparation des flux d'information par type peut augmenter la protection en garantissant que l'information n'est pas mélangée en transit et en permettant le contrôle de flux par chemin de transmission qui ne serait peut-être pas faisable autrement. Les types d'information séparable comprennent notamment le trafic de communication entrant et sortant, les demandes de services et les réponses, ainsi que l'information de catégories de sécurité différentes.

(22) APPLICATION DU CONTRÔLE DE FLUX D'INFORMATION | ACCÈS SEULEMENT

Le système d'information fournit à un seul dispositif l'accès aux plateformes informatiques, aux applications ou aux données contenues dans des domaines de sécurité différents tout en empêchant le flux d'information entre les différents domaines de sécurité.

Conseils supplémentaires sur l'amélioration : Le système d'information, par exemple, fournit un bureau afin que les utilisateurs puissent accéder à chaque domaine de sécurité connecté sans fournir de mécanismes de transfert d'information entre les différents domaines de sécurité.

Références :

CST, *ITSG-22, Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada* [référence 41].

AC-5 SÉPARATION DES TÂCHES

Contrôle :

(A) L'organisation :

(a) sépare les [*Affectation : tâches des personnes définies par l'organisation*];

(b) consigne la séparation des tâches des personnes;

(c) définit les autorisations d'accès au système d'information pour appuyer la séparation des tâches.

Conseils supplémentaires : La séparation des tâches gère l'abus possible des droits d'accès autorisés et aide à réduire le risque d'activités malveillantes sans collusion. Elle comprend notamment : (i) la division des fonctions liées à la mission et des fonctions de soutien liées au système d'information entre les personnes et/ou rôles; (ii) l'exécution de fonctions de soutien lié au système d'information par différentes personnes (p. ex. la gestion du système, la programmation, la gestion de la configuration, les tests et l'assurance de la qualité, et la sécurité réseau); (iii) l'assurance que le personnel de sécurité administrant les fonctions de contrôle d'accès n'administre pas également les fonctions de vérification. Contrôles connexes : AC-3, AC-6, PE-3, PE-4 et PS-2.

Améliorations du contrôle :

Aucune

Références :

Aucune

AC-6 DROIT D'ACCÈS MINIMAL

Contrôle :

(A) L'organisation utilise le principe du droit d'accès minimal, ce qui autorise l'accès uniquement aux utilisateurs (ou aux processus exécutés en leur nom) qui en ont besoin pour accomplir les tâches qui leur ont été assignées conformément aux missions et aux fonctions opérationnelles de l'organisation.

Conseils supplémentaires : Les organisations font appel au principe du droit d'accès minimal pour des tâches et systèmes d'information précis. Ce principe est également appliqué aux processus de système d'information et assure que les processus fonctionnent aux niveaux de droits d'accès appropriés pour la réalisation des fonctions opérationnelles et des missions organisationnelles. Les organisations considèrent la création de processus, de rôles et de comptes de système d'information additionnels, au besoin, pour adhérer au principe du droit d'accès minimal. Elles appliquent également ce principe au développement, à la mise en œuvre et à l'exploitation de leurs systèmes d'information. Contrôles connexes : AC-2, AC-3, AC-5, CM-6, CM-7 et PL-2.

Améliorations du contrôle :

(1) DROIT D'ACCÈS MINIMAL | AUTORISATION DE L'ACCÈS AUX FONCTIONS DE SÉCURITÉ

L'organisation autorise l'accès explicitement aux [*Affectation : fonctions de sécurité (déployées dans le matériel, les logiciels et les micrologiciels) et information liée à la sécurité définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les fonctions de sécurité comprennent notamment l'établissement des comptes système, la configuration des autorisations d'accès (c.-à-d. permissions et droits d'accès), la définition des événements à vérifier et le réglage des paramètres de détection d'intrusion. L'information pertinente en matière de sécurité comprend notamment les règles de filtrage des routeurs et des coupe-feux, l'information de gestion des clés cryptographiques, les paramètres de configuration des services de sécurité et les listes de contrôle d'accès. Le personnel explicitement autorisé comprend notamment les administrateurs de la sécurité, les administrateurs de système et de réseau, les agents de sécurité de système, le personnel de maintenance de système, les programmeurs de système et d'autres utilisateurs privilégiés. Contrôles connexes : AC-17, AC-18 et AC-19.

(2) DROIT D'ACCÈS MINIMAL | ACCÈS NON PRIVILÉGIÉ POUR LES FONCTIONS NON LIÉES À LA SÉCURITÉ

L'organisation exige des utilisateurs de comptes ou de rôles de système d'information qui ont accès aux [*Affectation : fonctions de sécurité et information sur la sécurité définies par l'organisation*] qu'ils utilisent des comptes ou des rôles non privilégiés pour accéder à des fonctions qui ne sont pas liées à la sécurité.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle limite l'exposition d'un système d'information aux menaces lors de l'utilisation de comptes ou de rôles privilégiés. Les rôles sont inclus pour tenir compte des situations où les organisations mettent en œuvre des politiques de contrôle d'accès, comme le RBAC, et où un changement de rôle fournit le même degré d'assurance, dans le changement des autorisations d'accès de l'utilisateur et de tous les processus exécutés en son nom, que celui qui serait fourni dans un changement apporté entre un compte privilégié et un compte non privilégié. Contrôle connexe : PL-4.

(3) DROIT D'ACCÈS MINIMAL | ACCÈS RÉSEAU AUX COMMANDES PRIVILÉGIÉES

L'organisation autorise l'accès réseau aux [*Affectation : commandes privilégiées définies par l'organisation*] seulement pour les [*Affectation : besoins opérationnels urgents définis par l'organisation*] et consigne les motifs d'un tel accès dans le plan de sécurité des opérations pour le système d'information.

Conseils supplémentaires sur l'amélioration : L'accès réseau désigne tout accès dans une connexion réseau par opposition à l'accès local (c.-à-d. utilisateur sur place). Contrôle connexe : AC-17.

(4) DROIT D'ACCÈS MINIMAL | DOMAINES DE TRAITEMENT SÉPARÉS

Le système d'information fournit des domaines de traitement séparés pour permettre une granularité plus fine dans l'attribution des droits d'accès utilisateur.

Conseils supplémentaires sur l'amélioration : Une granularité plus fine dans l'attribution des droits d'accès utilisateur comprend, par exemple : (i) l'utilisation de techniques de virtualisation pour accorder des droits d'accès additionnels dans une machine virtuelle tout en limitant ceux accordés à d'autres machines virtuelles ou à la machine réelle sous-jacente; (ii) l'utilisation de mécanismes de séparation des domaines logiciels et/ou matériels; (iii) la mise en œuvre de domaines physiques séparés. Contrôles connexes : AC-4, SC-3, SC-30 et SC-32.

(5) DROIT D'ACCÈS MINIMAL | COMPTES PRIVILÉGIÉS

L'organisation restreint les comptes privilégiés sur le système d'information aux [*Affectation : personnel ou rôles définis par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les comptes privilégiés, y compris les comptes de superutilisateur, sont habituellement décrits comme des administrateurs système dans les différents types de systèmes d'exploitation commerciaux sur étagère. La restriction des comptes privilégiés à des employés ou à des rôles précis empêche les utilisateurs normaux d'accéder aux fonctions et à l'information privilégiées. Lorsqu'elles appliquent cette amélioration de contrôle, les organisations peuvent faire une distinction entre les droits d'accès attribués aux comptes locaux et ceux attribués aux comptes de domaine pour autant qu'elles restent en mesure de contrôler les configurations des systèmes d'information en ce qui a trait aux paramètres clés de sécurité et, le cas échéant, d'atténuer suffisamment les risques. Contrôle connexe : CM-6.

(6) DROIT D'ACCÈS MINIMAL | ACCÈS PRIVILÉGIÉ INTERDIT AUX UTILISATEURS NON ORGANISATIONNELS

L'organisation interdit tout accès privilégié au système d'information aux utilisateurs ne faisant pas partie de l'organisation. Contrôle connexe : IA-8.

(7) DROIT D'ACCÈS MINIMAL | EXAMEN DES DROITS D'ACCÈS DES UTILISATEURS

L'organisation :

(a) examine les droits d'accès attribués aux [*Affectation : rôles ou classes d'utilisateur définis par l'organisation*] tous les [*Affectation : fréquence définie par l'organisation*] pour valider la nécessité de détenir ces droits d'accès;

(b) réattribue ou retire les droits d'accès, au besoin, pour bien refléter les besoins organisationnels liés à la mission et aux opérations.

Conseils supplémentaires sur l'amélioration : La nécessité de détenir certains droits d'accès utilisateur pourrait changer au fil du temps selon les changements aux fonctions opérationnelles et aux missions organisationnelles, selon les environnements d'opération, selon les technologies ou selon les menaces. L'examen périodique des droits d'accès attribués aux utilisateurs est essentiel afin de déterminer si la justification relative à l'attribution de ces droits d'accès est toujours valide. Si la nécessité ne peut être validée de nouveau, les organisations doivent prendre les mesures correctives appropriées. Contrôle connexe : CA-7.

(8) DROIT D'ACCÈS MINIMAL | NIVEAUX DE DROIT D'ACCÈS POUR L'EXÉCUTION DE CODE

Le système d'information empêche les [*Affectation : logiciels définis par l'organisation*] d'être exécutés à des niveaux de droits d'accès plus élevés que ceux des utilisateurs qui exécutent les logiciels.

Conseils supplémentaires sur l'amélioration : Dans certains cas, les applications et programmes logiciels doivent être exécutés avec des droits d'accès élevés pour effectuer les fonctions requises. Toutefois, si les droits d'accès requis pour l'exécution sont à un niveau plus élevé que les droits d'accès attribués aux utilisateurs de ces applications et programmes, les utilisateurs reçoivent indirectement des droits d'accès plus élevés que deux qui leur ont été attribués par l'organisation.

(9) DROIT D'ACCÈS MINIMAL | UTILISATION VÉRIFIÉE DES FONCTIONS PRIVILÉGIÉES

Le système d'information vérifie l'exécution de fonctions privilégiées.

Conseils supplémentaires sur l'amélioration : L'utilisation inappropriée, intentionnellement ou non, des fonctions privilégiées par des utilisateurs autorisés, ou par des entités externes non autorisées qui ont compromis les comptes du système d'information, est une préoccupation sérieuse et permanente qui peut avoir des répercussions négatives importantes sur les organisations. La vérification de l'utilisation des fonctions privilégiées est une façon de détecter l'utilisation inappropriée et d'aider à atténuer les risques liés aux menaces internes et aux menaces persistantes sophistiquées (APT pour *Advanced Persistent Threat*). Contrôle connexe : AU-2.

(10) DROIT D'ACCÈS MINIMAL | INTERDICTION AUX UTILISATEURS NON PRIVILÉGIÉS D'EXÉCUTER DES FONCTIONS PRIVILÉGIÉES

Le système d'information empêche les utilisateurs non privilégiés d'exécuter des fonctions privilégiées, y compris la désactivation, le contournement ou la modification des mesures de protection et contremesures de sécurité mises en œuvre.

Conseils supplémentaires sur l'amélioration : Les fonctions privilégiées comprennent notamment l'établissement de comptes du système d'information, la vérification de l'intégrité du système et l'administration des activités de gestion des clés cryptographiques. Les utilisateurs non privilégiés ne détiennent pas les autorisations appropriées. Les mécanismes de détection et de prévention d'intrusions et les mécanismes de protection contre les programmes malveillants sont des exemples de fonctions privilégiées qui doivent être protégées contre les utilisateurs non privilégiés.

Références :

Aucune

AC-7 TENTATIVES D'OUVERTURE DE SESSION INFRUCTUEUSES

Contrôle :

(A) Le système d'information applique une limite de [*Affectation : nombre défini par l'organisation*] tentatives d'ouverture de session invalides consécutives par l'utilisateur sur une période de [*Affectation : durée définie par l'organisation*].

(B) Le système d'information [*Sélection : verrouille le compte ou le nœud pendant [Affectation : durée définie par l'organisation*]; *verrouille le compte ou le nœud jusqu'à ce qu'un administrateur le libère; reporte l'invite d'ouverture de session suivante selon* [*Affectation : algorithme de temporisation défini par l'organisation*]] automatiquement lorsque le nombre maximal de tentatives infructueuses est dépassé.

Conseils supplémentaires : En raison des risques de déni de service, les verrouillages automatiques effectués par le système d'information sont habituellement temporaires et annulés automatiquement après une période prédéterminée établie par l'organisation. Dans le cas où l'on choisit un algorithme de temporisation, l'organisation peut utiliser différents algorithmes pour différents composants du système d'information, selon les capacités de ces composants. La réponse aux tentatives d'ouverture de session infructueuses peut être mise en œuvre tant au niveau du système d'exploitation qu'au niveau des applications. Ce contrôle s'applique à tous les accès autres que ceux explicitement identifiés et consignés par l'organisation dans le contrôle AC-14.

Améliorations du contrôle :

(1) TENTATIVES D'OUVERTURE DE SESSION INFRUCTUEUSES | VERROUILLAGE AUTOMATIQUE DU COMPTE

[Annulée : Intégrée au contrôle AC-7]

(2) TENTATIVES D'OUVERTURE DE SESSION INFRUCTUEUSES | PURGE ET NETTOYAGE DES DISPOSITIFS MOBILES

Le système d'information purge ou nettoie l'information des [*Affectation : dispositifs mobiles définis par l'organisation*] en fonction des [*Affectation : techniques ou exigences en matière de purge ou de nettoyage définies par l'organisation*] après [*Affectation : nombre défini par l'organisation*] tentatives infructueuses d'ouverture de session consécutives sur les dispositifs.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle s'applique seulement aux dispositifs mobiles (p. ex. assistants numériques, téléphones intelligents et tablettes) auxquels l'accès se fait par ouverture de session. L'ouverture de session concerne le dispositif mobile lui-même et non les comptes qui y ont été établis, le cas échéant. Les ouvertures de session réussies dans les comptes des dispositifs mobiles remettent à zéro le compteur de tentatives d'ouvertures de session infructueuses. Les organisations définissent l'information devant faire l'objet d'une purge ou d'un nettoyage attentif afin d'éviter que les dispositifs deviennent inutilisables en cas de purge ou de nettoyage excessif. Il se peut que la purge ou le nettoyage ne soit pas nécessaire si l'information sur le dispositif est protégée à l'aide de mécanismes de chiffrement suffisamment robustes. Contrôles connexes : AC-19, MP-5, MP-6 et SC-13.

Références :

Aucune

AC-8 AVIS D'UTILISATION SYSTÈME

Contrôle :

(A) Le système d'information, avant d'accorder l'accès, affiche aux utilisateurs [*Affectation : message ou bannière d'avis d'utilisation du système défini par l'organisation*], qui comprend des énoncés de confidentialité et de sécurité conformément à la *Politique sur l'utilisation acceptable des dispositifs et des réseaux* du SCT [référence 5].

(B) Le système d'information continue d'afficher le message ou la bannière d'avis jusqu'à ce que l'utilisateur accepte les modalités d'utilisation et opte d'ouvrir une session ou d'accéder au système.

(C) Le système d'information, dans le cas d'un système auquel peut accéder le public :

(a) affiche l'information sur l'utilisation du système selon les [*Affectation : modalités définies par l'organisation*] avant d'accorder l'accès;

(b) affiche, au besoin, des mises en garde concernant la surveillance, l'enregistrement et la vérification conformes aux dispositions sur la protection des renseignements personnels pour de tels systèmes qui interdisent généralement ces activités;

(c) comprend une description des utilisations autorisées du système.

Conseils supplémentaires : Les avis concernant l'utilisation du système peuvent être mis en œuvre au moyen de messages ou de bannières d'avertissement qui s'affichent avant qu'un utilisateur ouvre une session sur le système d'information. Ils sont utilisés uniquement pour l'accès au moyen des interfaces d'ouverture de session avec utilisateurs humains et ne sont pas requis lorsque de telles interfaces humaines n'existent pas. Les organisations considèrent l'affichage des messages et des bannières d'avis d'utilisation système en plusieurs langues selon les besoins organisationnels précis et la démographie des utilisateurs du système d'information. Elles peuvent également consulter les services juridiques de leur ministère à des fins de révision juridique et d'approbation du contenu des bannières d'avertissement.

Améliorations du contrôle :

Aucune

Références :

SCT, *Politique sur l'utilisation acceptable des dispositifs et des réseaux* [référence 5].

AC-9 AVIS D'OUVERTURE DE SESSION PRÉCÉDENTE (ACCÈS)

Contrôle :

(A) Le système d'information indique à l'utilisateur qui vient d'ouvrir une session sur le système la date et l'heure de sa dernière ouverture de session (dernier accès).

Conseils supplémentaires : Ce contrôle s'applique aux ouvertures de session sur les systèmes d'information au moyen des interfaces des utilisateurs humains et aux ouvertures de session sur les systèmes offerts par d'autres types d'architecture (p. ex. architectures orientées services). Contrôles connexes : AC-7 et PL-4.

Améliorations du contrôle :

(1) AVIS D'OUVERTURE DE SESSION PRÉCÉDENTE | OUVERTURES DE SESSION INFRUCTUEUSES

Le système d'information indique à l'utilisateur qui vient d'ouvrir une session le nombre de tentatives d'ouverture de session infructueuses depuis sa dernière tentative réussie.

(2) AVIS D'OUVERTURE DE SESSION PRÉCÉDENTE | OUVERTURES DE SESSION INFRUCTUEUSES ET RÉUSSIES

Le système d'information indique à l'utilisateur le nombre de [*Sélection : ouvertures de session/accès réussis; ouvertures de session/accès infructueux; les deux*] pendant [*Affectation : durée définie par l'organisation*].

(3) AVIS D'OUVERTURE DE SESSION PRÉCÉDENTE | AVIS DE CHANGEMENTS AU COMPTE

Le système d'information indique à l'utilisateur les changements à [*Affectation : caractéristiques ou paramètres liés à la sécurité appliqués au compte de l'utilisateur définis par l'organisation*] pendant [*Affectation : durée définie par l'organisation*].

(4) AVIS D'OUVERTURE DE SESSION PRÉCÉDENTE | INFORMATION ADDITIONNELLE SUR L'OUVERTURE DE SESSION

Le système d'information indique à l'utilisateur qui vient d'ouvrir une session sur le système l'information additionnelle suivante : [*Affectation : information définie par l'organisation à indiquer en plus de la date et de l'heure de la dernière ouverture de session (dernier accès)*].

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle permet aux organisations d'ajouter de l'information additionnelle qui sera fournie aux utilisateurs lors de l'ouverture de session, comme l'emplacement de la dernière ouverture de session. L'emplacement de l'utilisateur est défini comme l'information que les systèmes d'information peuvent établir (p. ex. les adresses IP à partir desquelles les ouvertures de session réseau ont eu lieu, les identificateurs de dispositif et les avis d'ouvertures de session locales).

Références :

Aucune

AC-10 CONTRÔLE DE SESSIONS SIMULTANÉES

Contrôle :

(A) Le système d'information limite le nombre de sessions simultanées pour chaque [*Affectation : type de compte et/ou compte défini par l'organisation*] à [*Affectation : nombre défini par l'organisation*].

Conseils supplémentaires : Les organisations peuvent définir le nombre maximal de sessions simultanées pour les comptes de système d'information globalement, par type de compte (p. ex. utilisateur privilégié, utilisateur non privilégié, domaine, application précise), par compte ou selon une combinaison. Par exemple, les organisations peuvent limiter le nombre de sessions simultanées pour les administrateurs système ou les utilisateurs travaillant dans des domaines particulièrement sensibles ou avec des applications essentielles à la mission. Ce contrôle concerne les sessions simultanées de comptes de système d'information et non celles effectuées par un seul utilisateur se servant de plusieurs comptes système.

Améliorations du contrôle :

Aucune

Références :

Aucune

AC-11 VERROUILLAGE DE SESSION

Contrôle :

(A) Le système d'information empêche tout autre accès au système en verrouillant la session après [*Affectation : délai défini par l'organisation*] d'inactivité ou à la réception d'une demande d'un utilisateur.

(B) Le système d'information maintient le verrouillage de la session jusqu'à ce que l'utilisateur rétablisse l'accès en exécutant les procédures établies d'identification et d'authentification.

Conseils supplémentaires : Les verrouillages de session sont des mesures temporaires prises lorsque des utilisateurs cessent de travailler sur leur poste et s'éloignent de l'environnement immédiat où se trouvent les systèmes d'information et qu'ils ne souhaitent pas se déconnecter en raison de la nature temporaire de leur absence. Les verrouillages de session sont mis en œuvre où les activités de session peuvent être déterminées. Cet arrêt s'effectue normalement au niveau du système d'exploitation, mais peut également se faire au niveau de l'application. Les verrouillages de session ne remplacent pas la fermeture de la session sur les systèmes d'information, par exemple, si les organisations exigent de leurs utilisateurs qu'ils ferment leur session à la fin de la journée de travail. Contrôle connexe : AC-7.

Améliorations du contrôle :

(1) VERROUILLAGE DE SESSION | MASQUAGE DE L'AFFICHAGE AU MOYEN D'UNE IMAGE

Au moyen du verrouillage de session, le système d'information utilise une image visible afin de masquer l'information qui était visible auparavant sur l'affichage.

Conseils supplémentaires sur l'amélioration : Les images visibles peuvent inclure des images statiques ou dynamiques, comme des formes que l'on retrouve dans les économiseurs d'écran, des photographies, des couleurs solides, une horloge, un indicateur de la charge de la pile ou un écran vide, ainsi qu'une mise en garde supplémentaire indiquant que les images ne comportent pas d'information sensible.

Références :

Aucune

AC-12 FIN DE SESSION

Contrôle :

(A) Le système d'information met automatiquement fin à une session utilisateur après [*Affectation : modalités ou événements déclenchant une déconnexion définis par l'organisation*].

Conseils supplémentaires : Ce contrôle porte sur l'interruption des sessions logiques ouvertes par les utilisateurs, par opposition au contrôle SC-10 qui porte sur l'interruption des connexions réseau associées à des sessions de communication (c.-à-d. déconnexion réseau). Une session logique (pour l'accès local, réseau et distant) est lancée quand un utilisateur (ou un processus exécuté en son nom) accède à un système d'information organisationnel. De telles sessions utilisateur peuvent être interrompues (ce qui met fin à l'accès de l'utilisateur) sans interrompre les sessions réseau. L'interruption de la session met fin à tous les processus liés à la session logique de l'utilisateur, à l'exception des processus créés précisément par l'utilisateur (c.-à-d. propriétaire de la session) pour continuer après l'interruption de la session. Les conditions ou les événements déclenchant l'interruption automatique de la session comprennent notamment la durée d'inactivité de l'utilisateur (définie par l'organisation), des réponses ciblées à certains types d'incidents et des restrictions liées à l'heure de la journée pour l'utilisation du système d'information. Contrôles connexes : SC-10 et SC-23.

Améliorations du contrôle :

(1) FIN DE SESSION | FERMETURES DE SESSION EXÉCUTÉES PAR LES UTILISATEURS ET AFFICHAGE DE MESSAGES

(a) Le système d'information fournit une capacité de fermeture de session pour les sessions de communication lancées par les utilisateurs lorsque l'authentification est utilisée pour accéder aux [*Affectation : ressources d'information définies par l'organisation*].

(b) Le système d'information affiche un message explicite de fermeture de session pour indiquer aux utilisateurs l'interruption des sessions de communication authentifiées.

Conseils supplémentaires sur l'amélioration : Les ressources d'information auxquelles les utilisateurs accèdent par authentification comprennent notamment les postes de travail locaux, les bases de données ainsi que les services Web et sites Web protégés par mot de passe. Les messages de fermeture de session pour l'accès aux pages Web peuvent par exemple être affichés après l'interruption des sessions authentifiées. Cependant, pour certains types de sessions interactives comme les sessions FTP, les systèmes d'information envoient habituellement des messages de fermeture de session à titre de dernier message avant de mettre fin à la session.

Références :

Aucune

AC-13 SURVEILLANCE ET EXAMEN — CONTRÔLE D'ACCÈS

[Annulé : Intégré aux contrôles AC-2 et AU-6]

AC-14 OPÉRATIONS PERMISES SANS IDENTIFICATION NI AUTHENTIFICATION

Contrôle :

(A) L'organisation identifie les [*Affectation : opérations de l'utilisateur définies par l'organisation*] que l'utilisateur peut exécuter dans le système d'information sans devoir s'identifier ni s'authentifier, conformément aux fonctions opérationnelles et aux missions de l'organisation.

(B) L'organisation consigne et explique dans le plan de sécurité du système d'information la logique sous-jacente qui permet à l'utilisateur d'effectuer des opérations qui ne nécessitent ni identification ni authentification.

Conseils supplémentaires : Ce contrôle porte sur les situations où les organisations déterminent que l'identification et l'authentification ne sont pas requises dans les systèmes d'information organisationnels. Les organisations peuvent autoriser un nombre limité d'opérations sans identification ni authentification, par exemple lorsque des personnes accèdent à des sites Web publics ou à des systèmes d'information fédéraux accessibles au public, lorsque des personnes utilisent des téléphones mobiles pour recevoir des appels ou lorsque des télécopies sont reçues. Les organisations identifient également les opérations nécessitant normalement une identification ou une authentification, mais permettent une dérogation à ces mécanismes dans certaines circonstances (p. ex. situations d'urgence). Ces dérogations peuvent s'effectuer, par exemple, par un commutateur physique, lisible par logiciel, qui permet de contourner la procédure d'ouverture de session et qui est protégé contre toute utilisation accidentelle ou non surveillée. Ce contrôle ne s'applique pas aux situations où l'identification et l'authentification ont déjà été effectuées et ne sont pas répétées. Il s'applique plutôt aux situations où les mécanismes d'identification et d'authentification n'ont pas encore eu lieu. Les organisations peuvent décider que les opérations de l'utilisateur doivent être effectuées dans les systèmes d'information organisationnels uniquement à l'aide de mécanismes d'identification et d'authentification. Par conséquent, les valeurs pour les énoncés d'attribution peuvent être « *aucun* ». Contrôles connexes : CP-2 et IA-2.

Améliorations du contrôle :

Aucune

Références :

Aucune

AC-15 MARQUAGE AUTOMATIQUE

[Annulé : Intégré au contrôle MP-3]

AC-16 ATTRIBUTS DE SÉCURITÉ

Contrôle :

(A) L'organisation fournit les moyens permettant d'associer les [*Affectation : types d'attribut de sécurité définis par l'organisation*] qui ont [*Affectation : valeurs des attributs de sécurité définies par l'organisation*] à l'information pendant qu'elle est stockée, traitée et/ou transmise.

(B) L'organisation s'assure que toutes les associations d'attribut de sécurité sont effectuées et conservées avec l'information.

(C) L'organisation établit les [*Affectation : attributs de sécurité définis par l'organisation*] permis pour les [*Affectation : systèmes d'information définis par l'organisation*].

(D) L'organisation détermine les [*Affectation : valeurs ou intervalles définis par l'organisation*] permis pour chacun des attributs de sécurité établis.

Conseils supplémentaires : L'information est représentée à l'interne dans les systèmes d'information au moyen d'abstractions également appelées structures de données. Les structures de données internes peuvent représenter différents types d'entités actives et passives. Les entités actives, également appelées sujets, sont habituellement associées à des personnes, à des dispositifs ou à des processus exécutés au nom des personnes. Les entités passives, également appelées objets, sont habituellement associées à des structures de données comme des dossiers, des tampons, des fichiers, des canaux interprocessus et des ports de communications. Les attributs de sécurité (une forme de métadonnées) sont des abstractions des propriétés ou des caractéristiques d'entités actives et passives qui concernent la protection de l'information. Ces attributs peuvent être associés à des entités actives (c.-à-d. des sujets) qui ont le potentiel d'envoyer ou de recevoir de l'information, de faire circuler l'information entre des objets ou de changer l'état du système d'information. Ils peuvent également être associés à des entités passives (c.-à-d. des objets) qui contiennent ou reçoivent de l'information. L'association d'attribut de sécurité à des sujets et objets s'appelle une *liaison* et fait habituellement partie de l'établissement de la valeur de l'attribut et du type de l'attribut. Les attributs de sécurité, lorsqu'ils sont liés à des données ou à de l'information, permettent d'appliquer les politiques de sécurité de l'information relatives au contrôle d'accès et au contrôle de flux d'information, soit au moyen de processus organisationnels, soit au moyen de fonctions ou de mécanismes du système d'information. Le contenu ou les valeurs attribuées aux attributs de sécurité peuvent avoir une incidence directe sur la capacité des personnes d'accéder à l'information de l'organisation.

Les organisations peuvent définir les types d'attribut requis pour des systèmes d'information particuliers afin d'appuyer les fonctions opérationnelles et les missions. Une vaste gamme de valeurs peut être attribuée à un attribut de sécurité. Le marquage aux fins de diffusion peut inclure SECRET//Rel to CAN, USA, NATO ou CONFIDENTIEL//Réservé aux Canadiens (ne peut être diffusé à des gouvernements étrangers). En précisant les valeurs et les intervalles d'attribut permis, les organisations s'assurent que les valeurs d'attribut de sécurité sont pertinentes et importantes. L'expression « étiquetage de sécurité » désigne l'association d'attribut de sécurité à des sujets et objets représentés par des structures de données internes dans les systèmes d'information organisationnels, pour permettre l'application des politiques de sécurité de l'information selon les systèmes d'information. Les étiquettes de sécurité comprennent notamment les autorisations d'accès, la protection du cycle de vie des données (c.-à-d. le chiffrement et l'expiration des données), la nationalité, l'affiliation à titre d'entrepreneur et la classification de l'information conformément aux exigences juridiques et aux exigences en matière de conformité. L'expression « marquage de sécurité » désigne l'association d'attribut de sécurité à des objets sous forme lisible, pour permettre l'application des politiques de sécurité de l'information selon les processus de l'organisation. Le contrôle AC-16 de base porte sur l'exigence d'effectuer des associations d'attribut selon les utilisateurs (marquage). Les améliorations au contrôle AC-16 portent sur les exigences supplémentaires, y compris les associations d'attribut selon les systèmes d'information (étiquetage). Les types d'attribut comprennent notamment le niveau de classification pour les objets et le niveau d'habilitation de sécurité (autorisation d'accès) pour les sujets. Contrôles connexes : AC-3, AC-4, AC-6, AC-21, AU-2, AU-10, SC-16 et MP-3.

Améliorations du contrôle :

(1) ATTRIBUTS DE SÉCURITÉ | ASSOCIATION DYNAMIQUE D'ATTRIBUT

Le système d'information associe de manière dynamique des attributs de sécurité aux [*Affectation : sujets et objets définis par l'organisation*] conformément aux [*Affectation : politiques de sécurité définies par l'organisation*] au moment où l'information est créée et combinée.

Conseils supplémentaires sur l'amélioration : L'organisation peut faire appel à l'association dynamique d'attribut de sécurité lorsque les caractéristiques de sécurité de l'information changent au fil du temps. Les attributs de sécurité peuvent changer, par exemple, en raison de problèmes relatifs au regroupement de l'information (c.-à-d. les caractéristiques de sécurité des éléments individuels d'information sont différentes des éléments combinés), ainsi qu'en raison de changements liés aux autorisations d'accès individuels (c.-à-d. les droits d'accès) et à la catégorie de sécurité de l'information. Contrôle connexe : AC-4.

(2) ATTRIBUTS DE SÉCURITÉ | CHANGEMENTS AUX VALEURS D'ATTRIBUT PAR DES PERSONNES AUTORISÉES

Le système d'information fournit aux personnes autorisées (ou aux processus exécutés en leur nom) la capacité de définir ou de changer la valeur des attributs de sécurité connexes.

Conseils supplémentaires sur l'amélioration : Le contenu des attributs de sécurité ou les valeurs qui leur ont été attribuées peuvent avoir une incidence directe sur la capacité des personnes d'accéder à l'information de l'organisation. Par conséquent, il est important que les systèmes d'information soient capables de fournir uniquement aux personnes autorisées la capacité de créer ou de modifier des attributs de sécurité. Contrôles connexes : AC-6 et AU-2.

(3) ATTRIBUTS DE SÉCURITÉ | MAINTIEN DES ASSOCIATIONS D'ATTRIBUT PAR LE SYSTÈME D'INFORMATION

Le système d'information maintient l'intégrité des [*Affectation : attributs de sécurité définis par l'organisation*] et l'association de ceux-ci aux [*Affectation : sujets et objets définis par l'organisation*].

Conseils supplémentaires sur l'amélioration : Le maintien de l'intégrité des attributs de sécurité et de leur association à des sujets et à des objets avec un degré d'assurance suffisant aide à garantir que les associations d'attribut peuvent servir de base aux opérations automatisées liées aux politiques. Les exemples d'opérations automatisées liées aux politiques incluent les décisions automatisées de contrôle d'accès et les décisions de contrôle de flux d'information.

(4) ATTRIBUTS DE SÉCURITÉ | ASSOCIATION D'ATTRIBUT PAR DES PERSONNES AUTORISÉES

Le système d'information prend en charge l'association des [*Affectation : attributs de sécurité définis par l'organisation*] aux [*Affectation : sujets et objets définis par l'organisation*] effectuée par des personnes autorisées (ou par des processus exécutés en leur nom).

Conseils supplémentaires sur l'amélioration : Le soutien que les systèmes d'information fournissent à cet égard peut varier : (i) inviter les utilisateurs à sélectionner des attributs de sécurité précis à associer à des objets d'information particuliers; (ii) employer des mécanismes automatisés pour catégoriser l'information avec les attributs appropriés en fonction des politiques définies; (iii) veiller à ce que la combinaison d'attributs de sécurité sélectionnée soit valide. Les organisations considèrent la création, la suppression ou la modification d'attributs de sécurité lorsqu'elles définissent les événements vérifiables.

(5) ATTRIBUTS DE SÉCURITÉ | AFFICHAGE D'ATTRIBUT POUR LES DISPOSITIFS DE SORTIE

Le système d'information affiche sous forme lisible les attributs de sécurité de chaque objet que le système transmet à des dispositifs de sortie afin d'identifier les [*Affectation : instructions spéciales de diffusion, de traitement ou de distribution définies par l'organisation*] conformément aux [*Affectation : conventions d'appellation standard, en langage lisible, définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les sorties du système d'information comprennent notamment des pages, des écrans et des objets équivalents. Les dispositifs de sortie du système d'information comprennent notamment les imprimantes et les affichages vidéo sur les postes de travail, les ordinateurs bloc-notes et les assistants numériques.

(6) ATTRIBUTS DE SÉCURITÉ | MAINTIEN DES ASSOCIATIONS D'ATTRIBUT PAR L'ORGANISATION

L'organisation permet au personnel d'associer les [*Affectation : attributs de sécurité définis par l'organisation*] aux [*Affectation : sujets et objets définis par l'organisation*] et de maintenir cette association, conformément aux [*Affectation : politiques de sécurité définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle exige que l'utilisateur (par opposition au système d'information) maintienne les associations d'attribut de sécurité aux sujets et objets.

(7) ATTRIBUTS DE SÉCURITÉ | INTERPRÉTATION UNIFORME DES ATTRIBUTS

L'organisation fournit une interprétation uniforme des attributs de sécurité transmis entre les composants du système d'information.

Conseils supplémentaires sur l'amélioration : Afin d'appliquer les politiques de sécurité dans de multiples composants de systèmes d'information distribués (p. ex. systèmes distribués de gestion des bases de données, systèmes infonuagiques et architectures orientées services), les organisations fournissent une interprétation uniforme des attributs de sécurité qui sont utilisés dans les décisions d'application de flux et de l'accès. Les organisations établissent des ententes et des processus pour veiller à ce que tous les composants de systèmes d'information distribués mettent en œuvre des attributs de sécurité avec des interprétations uniformes dans les opérations automatisées d'application de flux et de l'accès.

(8) ATTRIBUTS DE SÉCURITÉ | TECHNIQUES ET TECHNOLOGIES D'ASSOCIATION

Le système d'information met en œuvre les [*Affectation : techniques ou technologies définies par l'organisation*] avec le [*Affectation : niveau d'assurance défini par l'organisation*] lors de l'association d'attribut de sécurité à l'information.

Conseils supplémentaires sur l'amélioration : L'association (c.-à-d. la liaison) d'attributs de sécurité à de l'information dans les systèmes d'information est très importante en ce qui a trait à l'exécution des opérations automatisées d'application de flux et d'accès. L'association de tels attributs de sécurité peut être accomplie au moyen de technologies ou de techniques offrant différents niveaux d'assurance. Par exemple, les systèmes d'information peuvent établir des liaisons cryptographiques entre des attributs de sécurité et de l'information au moyen de signatures numériques et des clés cryptographiques connexes protégées par des dispositifs matériels (également appelés base matérielle sécurisée).

(9) ATTRIBUTS DE SÉCURITÉ | RÉATTRIBUTION DES ATTRIBUTS

L'organisation veille à ce que les attributs de sécurité associés à de l'information soient réattribués seulement à l'aide de mécanismes remaniés validés au moyen de [*Affectation : techniques ou procédures définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les organisations emploient des mécanismes remaniés validés afin de fournir les niveaux d'assurance requis pour les activités de réattribution d'attribut de sécurité. La validation est facilitée si les mécanismes remaniés sont monofonctions et ont des fonctions limitées. Comme les réattributions d'attribut de sécurité peuvent avoir une incidence sur les opérations d'application des politiques de sécurité (p. ex. décisions d'application de flux et d'accès), l'utilisation de mécanismes remaniés fiables est nécessaire afin de s'assurer que ces mécanismes fonctionnent correctement et uniformément.

(10) ATTRIBUTS DE SÉCURITÉ | CONFIGURATION D'ATTRIBUT PAR DES PERSONNES AUTORISÉES

Le système d'information fournit aux personnes autorisées la capacité de définir ou de changer le type et la valeur d'attributs de sécurité pouvant être associés à des sujets et à des objets.

Conseils supplémentaires sur l'amélioration : Le contenu des attributs de sécurité ou les valeurs qui leur ont été attribuées peuvent avoir une incidence directe sur la capacité des personnes d'accéder à l'information de l'organisation. Par conséquent, il est important que les systèmes d'information soient capables de fournir uniquement aux personnes autorisées la capacité de créer ou de modifier des attributs de sécurité.

Références :

SCT, *Politique sur la sécurité du gouvernement* (PSG) [référence 63].
SCT, *Norme de sécurité relative à l'organisation et l'administration* [référence 73].

AC-17 ACCÈS À DISTANCE

Contrôle :

(A) L'organisation définit et consigne les restrictions d'utilisation, les exigences en matière de configuration et de connexion, ainsi que les directives de mise en œuvre de chaque type d'accès à distance autorisé.

(B) L'organisation autorise l'accès à distance au système d'information avant d'autoriser de telles connexions.

(AA) L'organisation s'assure que tous les employés qui travaillent à l'extérieur de ses locaux protègent l'information conformément aux exigences minimales précisées dans la *Norme opérationnelle sur la sécurité matérielle* du SCT [référence 6].

Conseils supplémentaires : Un accès distant est l'accès des utilisateurs (ou des processus exécutés en leur nom) aux systèmes d'information organisationnels à l'aide de réseaux externes (p. ex. Internet). Les méthodes d'accès à distance comprennent notamment l'accès par ligne commutée, à large bande et sans fil. Les organisations utilisent souvent des réseaux privés virtuels (RPV) chiffrés pour augmenter la confidentialité et l'intégrité des connexions à distance. Cette utilisation ne rend pas l'accès non distant; toutefois, lorsque les RPV sont dotés des contrôles de sécurité appropriés (p. ex. employant des techniques de chiffrement pour la protection de la confidentialité et de l'intégrité), leur utilisation peut assurer à l'organisation qu'elle peut traiter ce type de connexion efficacement comme des réseaux internes. Néanmoins, les connexions RPV traversent des réseaux externes, et les RPV chiffrés n'augmentent pas la disponibilité des connexions distantes. Par ailleurs, les RPV dotés de tunnels chiffrés peuvent avoir une incidence sur la capacité de l'organisation de surveiller adéquatement le trafic de communication réseau à des fins de détection de programmes malveillants. Les contrôles d'accès à distance s'appliquent aux systèmes d'information autres que les serveurs Web publics ou les systèmes conçus pour l'accès public. Ce contrôle porte sur l'autorisation avant de permettre l'accès distant, sans préciser les formats de cette autorisation. Bien que les organisations puissent utiliser des ententes sur la sécurité des interconnexions pour autoriser les connexions d'accès à distance, ce contrôle ne requiert pas de telles ententes. Le contrôle AC-3 porte sur l'application des restrictions d'accès pour les connexions à distance.
Contrôles connexes : AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10 et SI-4.

Améliorations du contrôle :

(1) ACCÈS À DISTANCE | SURVEILLANCE ET CONTRÔLE AUTOMATISÉS

Le système d'information surveille et contrôle les méthodes d'accès à distance.

Conseils supplémentaires sur l'amélioration : La surveillance et le contrôle automatisés des sessions d'accès à distance permettent aux organisations de détecter les cyberattaques et de s'assurer du respect constant des politiques d'accès à distance grâce à la vérification des activités de connexion des utilisateurs distants sur une variété de composants du système d'information (p. ex. les serveurs, les postes de travail, les ordinateurs bloc-notes, les téléphones intelligents et les tablettes). Contrôles connexes : AU-2 et AU-12.

(2) ACCÈS À DISTANCE | PROTECTION DE LA CONFIDENTIALITÉ ET DE L'INTÉGRITÉ AU MOYEN DU CHIFFREMENT

Le système d'information met en œuvre des mécanismes cryptographiques pour protéger la confidentialité et l'intégrité des sessions d'accès à distance. La cryptographie doit être conforme aux exigences du contrôle SC-13.

Conseils supplémentaires sur l'amélioration : Le CST peut fournir, sur demande, des conseils sur la force du mécanisme de chiffrement.. Contrôles connexes : SC-8, SC-12 et SC-13.

(3) ACCÈS À DISTANCE | POINTS DE CONTRÔLE D'ACCÈS GÉRÉS

Le système d'information achemine tous les accès à distance au moyen de [*Affectation : nombre défini par l'organisation*] points de contrôle d'accès réseau gérés.

Conseils supplémentaires sur l'amélioration : La limitation du nombre de points de contrôle d'accès pour les accès à distance réduit la superficie d'attaque des organisations. Les organisations considèrent les exigences de l'initiative des connexions Internet fiables (TIC) pour les connexions réseau externes. Contrôle connexe : SC-7.

(4) ACCÈS À DISTANCE | ACCÈS ET COMMANDES PRIVILÉGIÉES

(a) L'organisation autorise l'exécution de commandes privilégiées et de l'accès à l'information liée à la sécurité au moyen de l'accès à distance seulement pour répondre aux [*Affectation : besoins définis par l'organisation*].

(b) L'organisation consigne la justification pour cet accès dans le plan de sécurité du système d'information.

Conseils supplémentaires sur l'amélioration : Contrôle connexe : AC-6.

(5) ACCÈS À DISTANCE | SURVEILLANCE DES CONNEXIONS NON AUTORISÉES

[Annulée : Intégrée au contrôle SI-4]

(6) ACCÈS À DISTANCE | PROTECTION DE L'INFORMATION

L'organisation veille à ce que les utilisateurs protègent l'information sur les mécanismes d'accès à distance contre toute utilisation et divulgation non autorisées.

Conseils supplémentaires sur l'amélioration : Contrôles connexes : AT-2, AT-3 et PS-6.

(7) ACCÈS À DISTANCE | PROTECTION SUPPLÉMENTAIRE POUR L'ACCÈS AUX FONCTIONS DE SÉCURITÉ

[Annulée : Intégrée au contrôle AC-3 (10)]

(8) ACCÈS À DISTANCE | DÉSACTIVATION DES PROTOCOLES RÉSEAU NON SÉCURISÉS

[Annulée : Intégrée au contrôle CM-7]

(9) ACCÈS À DISTANCE | DÉCONNEXION ET DÉSACTIVATION DE L'ACCÈS

L'organisation fournit la capacité de déconnecter ou de désactiver rapidement l'accès à distance au système d'information dans un délai de [*Affectation : délai défini par l'organisation*].

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle exige que les organisations aient la capacité de déconnecter rapidement à distance les utilisateurs ayant accès au système d'information et/ou de désactiver l'accès distant. La vitesse de la déconnexion ou de la désactivation dépend de la criticité des fonctions opérationnelles et des missions, ainsi que de la nécessité d'éliminer l'accès distant immédiat ou futur aux systèmes d'information organisationnels.

(100) L'accès à distance à des comptes privilégiés s'effectue à partir de consoles de gestion spécialisées régies entièrement par les politiques de sécurité du système et utilisées exclusivement à cette fin (p. ex. l'accès à Internet n'est pas autorisé).

Références :

SCT, *Norme opérationnelle sur la sécurité matérielle* [référence 6].
SCT, *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* [référence 7].

AC-18 ACCÈS SANS FIL

Contrôle :

(A) L'organisation établit les restrictions d'utilisation, les exigences en matière de configuration et de connexion, ainsi que les directives de mise en œuvre de l'accès sans fil.

(B) L'organisation autorise l'accès sans fil au système d'information avant d'autoriser de telles connexions.

Conseils supplémentaires : Les technologies sans fil incluent notamment les hyperfréquences, la radiocommunication à commutation de paquets (UHF/VHF), 802.11 et Bluetooth. Les réseaux sans fil utilisent des protocoles d'authentification (p. ex. Extensible Authentication Protocol [EAP]/Transport Layer Security [TLS], EAP protégé [PEAP]) qui assurent la protection des justificatifs d'identité et l'authentification mutuelle. Contrôles connexes : AC-2, AC-3, AC-17, AC-19, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, PL-4, SI-4 et SC-9.

Améliorations du contrôle :

(1) ACCÈS SANS FIL | AUTHENTIFICATION ET CHIFFREMENT

Le système d'information protège l'accès sans fil au moyen de l'authentification des [*Sélection (un ou les deux) : utilisateurs; dispositifs*] et du chiffrement.

Conseils supplémentaires sur l'amélioration : Contrôles connexes : SC-8 et SC-13.

(2) ACCÈS SANS FIL | SURVEILLANCE DES CONNEXIONS NON AUTORISÉES

[Annulée : Intégrée au contrôle SI-4]

(3) ACCÈS SANS FIL | DÉSACTIVATION DU RÉSEAUTAGE SANS FIL

L'organisation désactive, lorsqu'elle n'envisage pas de les utiliser, les capacités de réseautage sans fil intégrées aux composants du système d'information avant leur remise et leur déploiement.

Conseils supplémentaires sur l'amélioration : Contrôle connexe : AC-19.

(4) ACCÈS SANS FIL | RESTRICTION DES CONFIGURATIONS PAR LES UTILISATEURS

L'organisation identifie les utilisateurs et les autorise explicitement à configurer eux-mêmes les capacités de réseautage sans fil.

Conseils supplémentaires sur l'amélioration : Les autorisations organisationnelles permettant aux utilisateurs sélectionnés de configurer les capacités de réseautage sans fil sont appliquées en partie par les mécanismes d'application de l'accès employés dans les systèmes d'information organisationnels. Contrôles connexes : AC-3 et SC-15.

(5) ACCÈS SANS FIL | ANTENNES ET PUISSANCE DE TRANSMISSION

L'organisation sélectionne des antennes radio et calibre la puissance de transmission afin de réduire la probabilité que les signaux utilisables puissent être reçus en dehors des frontières que contrôle l'organisation.

Conseils supplémentaires sur l'amélioration : Les mesures que peut prendre l'organisation pour limiter l'utilisation non autorisée de communications sans fil en dehors des frontières qu'elle contrôle comprennent, par exemple : (i) la réduction de la puissance des transmissions sans fil pour qu'elles risquent moins d'émettre un signal que pourraient utiliser des adversaires à l'extérieur du périmètre physique de l'organisation; (ii) l'utilisation de mesures telles que TEMPEST pour contrôler les émissions sans fil; (iii) l'utilisation d'antennes directionnelles ou de mise en forme de faisceaux qui réduisent la probabilité que des personnes non prévues réussissent à intercepter les signaux. Avant de prendre de telles mesures, l'organisation peut mener des enquêtes sans fil périodiques pour comprendre le profil de radiofréquence des systèmes d'information organisationnels ainsi que d'autres systèmes qui pourraient être en fonction dans le secteur. Contrôle connexe : PE-19.

Références :

CST, *ITSPSR-21A, Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11* [référence 27].
CST, *ITSB-57B, Sécurité de la messagerie BlackBerry NIP à NIP* [référence 33].
CST, *ITSB-60, Conseils sur l'utilisation du protocole TLS (Transport Layer Security) au sein du gouvernement du Canada* [référence 34].
CST, *ITSG-02, Critères pour la conception, la fabrication, l'approvisionnement, l'installation et les essais de réception des enceintes blindées contre les radiofréquences* [référence 35].

AC-19 CONTRÔLE D'ACCÈS POUR LES DISPOSITIFS MOBILES

Contrôle :

(A) L'organisation établit les restrictions d'utilisation, les exigences en matière de configuration et de connexion, ainsi que les directives de mise en œuvre des dispositifs mobiles qu'elle contrôle.

(B) L'organisation autorise la connexion des dispositifs mobiles à ses systèmes d'information.

Conseils supplémentaires : Un dispositif mobile est un appareil informatique qui : (i) est de petite taille, afin qu'il soit facile à transporter par une seule personne; (ii) est conçu pour fonctionner sans connexion physique (p. ex. il peut transmettre ou recevoir de l'information sans fil); (iii) possède un stockage de données local et amovible ou non; (iv) comprend une source d'alimentation autonome. Les dispositifs mobiles peuvent également inclure les capacités de communication vocale, les capteurs internes qui permettent au dispositif d'acquérir de l'information et/ou les fonctions intégrées de synchronisation des données locales et des emplacements éloignés. Les téléphones intelligents, les tablettes et les liseuses sont des exemples de dispositifs mobiles. Ces dispositifs sont habituellement associés à une seule personne et restent habituellement à proximité de cette personne. Le degré de proximité peut toutefois varier selon la taille et la forme du dispositif. Les capacités de traitement, de stockage et de transmission du dispositif mobile sont comparables à un sous-ensemble de postes de travail, selon la nature et l'utilisation prévue du dispositif. En raison de la vaste gamme de dispositifs mobiles et des différentes caractéristiques et capacités techniques, les restrictions organisationnelles peuvent varier d'une classe ou d'un type de dispositif à l'autre. Les restrictions d'utilisation et les directives de mise en œuvre précises pour les dispositifs mobiles comprennent notamment la gestion des configurations, l'identification et l'authentification du dispositif, la mise en œuvre de logiciels de protection obligatoires (p. ex. détecteur de code malveillant, coupe-feu), le balayage aux fins de détection de code malveillant, la mise à jour du logiciel antivirus, la recherche des mises à jour et des correctifs critiques, l'exécution des contrôles d'intégrité du système d'exploitation principal (et d'autres logiciels résidents, le cas échéant) et la désactivation de tout matériel inutile (p. ex. sans fil, infrarouge). Les organisations doivent prendre note que la nécessité de fournir une sécurité adéquate pour les dispositifs mobiles va au-delà des exigences énoncées dans ce contrôle. Un grand nombre de mesures de protection et de contremesures pour les dispositifs mobiles sont reflétées dans d'autres contrôles de sécurité du catalogue, alloués dans le contrôle initial de base à titre de points de départ pour l'élaboration de plans de sécurité et de compléments à l'aide du processus d'adaptation. Il pourrait également y avoir un certain chevauchement des exigences énoncées dans les contrôles de sécurité au sein des différentes familles de contrôles. Le contrôle AC-20 porte sur les dispositifs mobiles qui ne sont pas contrôlés par les organisations. Contrôles connexes : AC-3, AC-7, AC-18, AC-20, CA-9, CM-2, IA-2, IA-3, MP-2, MP-4, MP-5, PL-4, SC-7, SC-43, SI-3 et SI-4.

Améliorations du contrôle :

(1) CONTRÔLE D'ACCÈS POUR LES DISPOSITIFS MOBILES | UTILISATION DE DISPOSITIFS MOBILES

[Annulée : Intégrée au contrôle MP-7]

(2) CONTRÔLE D'ACCÈS POUR LES DISPOSITIFS MOBILES | UTILISATION DE DISPOSITIFS MOBILES PERSONNELS

[Annulée : Intégrée au contrôle MP-7]

(3) CONTRÔLE D'ACCÈS POUR LES DISPOSITIFS MOBILES | UTILISATION DE DISPOSITIFS MOBILES SANS PROPRIÉTAIRE IDENTIFIABLE

[Annulée : Intégrée au contrôle MP-7]

(4) CONTRÔLE D'ACCÈS POUR LES DISPOSITIFS MOBILES | RESTRICTIONS LIÉES À L'INFORMATION CLASSIFIÉE

(a) L'organisation interdit l'utilisation de dispositifs mobiles non classifiés dans les installations hébergeant des systèmes d'information qui traitent, stockent ou transmettent de l'information classifiée, sauf si l'autorité responsable le permet.

(b) L'organisation applique les restrictions ci-après aux personnes autorisées par l'autorisé responsable à utiliser des dispositifs mobiles non classifiés dans les installations hébergeant des systèmes d'information qui traitent, stockent ou transmettent de l'information classifiée :

- il est interdit de connecter des dispositifs mobiles non classifiés à des systèmes d'information classifiés;
- la connexion de dispositifs mobiles non classifiés à des systèmes d'information classifiés requiert l'approbation de l'autorité responsable;
- il est interdit d'utiliser des modems internes ou externes, ou des interfaces sans fil, avec les dispositifs mobiles non classifiés (c.-à-d. ces dispositifs ou interfaces doivent être mis hors tension);
- les dispositifs mobiles non classifiés et l'information qui y est stockée peuvent faire l'objet d'examens et d'inspections aléatoires par les [*Affectation : agents de sécurité définis par l'organisation*]; si l'inspection confirme la présence d'information classifiée, la politique de traitement des incidents est appliquée;
- la connexion de dispositifs mobiles classifiés à des systèmes d'information classifiés doit être limitée conformément aux [*Affectation : politiques de sécurité définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Contrôles connexes : CA-6 et IR -4.

(5) CONTRÔLE D'ACCÈS POUR LES DISPOSITIFS MOBILES | CHIFFREMENT COMPLET DE DISPOSITIFS ET DE CONTENANTS

L'organisation emploie le [*Sélection : chiffrement complet des dispositifs; chiffrement des contenants*] pour protéger la confidentialité et l'intégrité de l'information sur les [*Affectation : dispositifs mobiles définis par l'organisation*].

Conseils supplémentaires sur l'amélioration : Le chiffrement des contenants fournit une approche à granularité fine au chiffrement des données et de l'information sur les dispositifs mobiles, y compris le chiffrement des structures de données sélectionnées, telles que les fichiers, les dossiers et les champs. Contrôles connexes : MP-5, SC-13 et SC-28.

(100) L'organisation veille à ce que les utilisateurs éteignent les dispositifs sans fil capables de transmettre la voix, ou qu'ils en désactivent manuellement le microphone, lorsqu'ils assistent à une réunion où de l'information classifiée, PROTÉGÉ B ou PROTÉGÉ C est communiquée, conformément à la *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* du SCT [référence 7].

Références :

SCT, *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* [référence 7].
CST, *ITSPSR-21A, Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11* [référence 27].
CST, *ITSB-57B, Sécurité de la messagerie BlackBerry NIP à NIP* [référence 33].
CST, *ITSB-104, Répercussions sur la sécurité de l'exposition de systèmes TI classifiés à des dispositifs mobiles et à des signaux sans fil* [référence 64].

AC-20 UTILISATION DE SYSTÈMES D'INFORMATION EXTERNES

Contrôle :

(A) L'organisation, conformément aux relations de confiance établies avec d'autres organisations qui possèdent, exploitent ou maintiennent des systèmes d'information externes, définit les modalités permettant aux personnes autorisées d'accéder au système d'information à partir de systèmes d'information externes.

(B) L'organisation, conformément aux relations de confiance établies avec d'autres organisations qui possèdent, exploitent ou maintiennent des systèmes d'information externes, définit les modalités permettant

aux personnes autorisées de traiter, de stocker ou de transmettre de l'information contrôlée par l'organisation à l'aide de systèmes d'information externes.

Conseils supplémentaires : Les systèmes d'information externes sont des systèmes d'information ou des composants de système d'information qui sont en-dehors des limites d'autorisation établies par les organisations et pour lesquels les organisations n'exercent normalement aucune supervision ou autorité directe sur le plan de l'application des contrôles de sécurité nécessaires ou de l'évaluation de l'efficacité de ces contrôles. Ils incluent, notamment : (i) les systèmes d'information et les dispositifs personnels (p. ex. ordinateurs bloc-notes, téléphones intelligents, tablettes et assistants numériques); (ii) les dispositifs de traitement et de communication privés hébergés dans des installations commerciales ou publiques (p. ex. hôtels, gares de train, centres de congrès, centres commerciaux ou aéroports); (iii) les systèmes d'information appartenant à des organisations non gouvernementales ou dont le contrôle relève de ces organisations; (iv) les systèmes d'information du GC qui ne sont ni la propriété des organisations, ni exploités ou contrôlés sous leur supervision directe et leur autorité. Ce contrôle porte également sur l'utilisation des systèmes d'information externes à des fins de traitement, de stockage ou de transmission de l'information organisationnelle, y compris l'accès aux services infonuagiques (p. ex. infrastructure, plateforme ou logiciel en tant que service) à partir des systèmes d'information organisationnels.

Dans le cas de certains systèmes d'information externes (c.-à-d. ceux exploités par d'autres organisations du GC, y compris les organisations qui leur sont subordonnées), les relations de confiance établies entre ces organisations et l'organisation concernée peuvent être telles qu'aucune modalité explicite n'est requise. Les systèmes d'information dans ces organisations ne sont pas considérés comme des systèmes externes. Ces situations se produisent, par exemple, lorsque des partages existaient déjà ou que des ententes de confiance (implicites ou explicites) avaient été établies entre les organisations subordonnées de ces organisations du GC, ou lorsque de telles ententes sont stipulées dans les lois du GC et les politiques, directives et normes applicables du SCT. Les personnes autorisées comprennent les employés de l'organisation, les entrepreneurs ou d'autres personnes autorisées à accéder aux systèmes d'information de l'organisation et auxquelles l'organisation est en droit d'imposer des règles de conduite en matière d'accès aux systèmes. Les restrictions que les organisations imposent aux personnes autorisées n'ont pas besoin d'être uniformes puisqu'elles peuvent varier selon les relations de confiance entre les organisations. Par conséquent, les organisations peuvent choisir d'imposer différentes restrictions de sécurité aux entrepreneurs qu'à un gouvernement fédéral, provincial ou municipal.

Ce contrôle ne concerne pas l'utilisation de systèmes d'information externes pour accéder à des interfaces publiques permettant d'utiliser les systèmes d'information de l'organisation. Les organisations établissent les modalités d'utilisation des systèmes d'information externes conformément à leurs politiques et procédures en matière de sécurité. Les modalités définissent, au minimum : les types d'application accessibles sur les systèmes d'information organisationnels à partir des systèmes d'information externes, et la catégorie de sécurité la plus élevée de l'information qui peut être traitée, stockée ou transmise dans des systèmes d'information externes. Si les organisations ne peuvent pas établir des modalités avec les propriétaires des systèmes d'information externes, elles peuvent imposer des restrictions à leur personnel au moyen de ces systèmes externes. Contrôles connexes : AC-3, AC-17, AC-19, CA-3, PL-4 et SA-9.

Améliorations du contrôle :

(1) UTILISATION DE SYSTÈMES D'INFORMATION EXTERNES | LIMITES RELATIVES À L'UTILISATION AUTORISÉE

L'organisation permet à des personnes autorisées d'utiliser un système d'information externe pour accéder à son système d'information ou pour traiter, stocker ou transmettre de l'information sous son contrôle seulement lorsqu'elle :

(a) vérifie si les contrôles de sécurité requis ont été mis en œuvre dans le système externe, tel qu'il est stipulé dans la politique de sécurité et dans le plan de sécurité de l'organisation liés à l'information;

ou

(b) conserve les ententes approuvées de connexion au système d'information ou de traitement avec l'entité organisationnelle qui héberge le système d'information externe.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle reconnaît que dans certaines circonstances, des utilisateurs de systèmes d'information externes (p. ex. entrepreneurs et partenaires de la coalition) ont besoin d'accéder aux systèmes d'information organisationnels. Dans ces situations, les organisations doivent être certaines que les systèmes d'information externes contiennent les mesures de protection de sécurité nécessaires (c.-à-d. contrôles de sécurité), de manière à ne pas compromettre ni endommager les systèmes d'information organisationnels. La vérification visant à s'assurer que les contrôles de sécurité requis ont été mis en œuvre peut être réalisée, par exemple, par un tiers, des évaluations indépendantes, des attestations ou d'autres moyens, selon le degré de certitude dont ont besoin les organisations. Contrôle connexe : CA-2.

(2) UTILISATION DE SYSTÈMES D'INFORMATION EXTERNES | DISPOSITIFS DE STOCKAGE PORTATIFS

L'organisation [*Sélection : limite; interdit*] l'utilisation de dispositifs mobiles qu'elle contrôle par des personnes autorisées sur les systèmes d'information externes.

Conseils supplémentaires sur l'amélioration : Les limites d'utilisation, dans les systèmes d'information externes, des dispositifs mobiles contrôlés par l'organisation par des personnes autorisées comprennent, par exemple, l'interdiction absolue d'utiliser ces dispositifs ou des restrictions et des modalités sur la façon de les utiliser.

(3) UTILISATION DE SYSTÈMES D'INFORMATION EXTERNES | SYSTÈMES, COMPOSANTS ET DISPOSITIFS N'APPARTENANT PAS À L'ORGANISATION

L'organisation [*Sélection : limite; interdit*] l'utilisation de systèmes d'information, de composants système et de dispositifs ne lui appartenant pas, à des fins de traitement, de stockage ou de transmission d'information organisationnelle.

Conseils supplémentaires sur l'amélioration : Les dispositifs n'appartenant pas à l'organisation comprennent les dispositifs personnels ainsi que les dispositifs appartenant à d'autres organisations (p. ex. organisations non gouvernementales et entrepreneurs). L'utilisation de tels dispositifs comporte des risques. Dans certains cas, le risque est suffisamment élevé pour en interdire l'utilisation. Dans d'autres cas, l'utilisation de dispositifs n'appartenant pas à l'organisation peut être permise, mais limitée dans une certaine mesure. Les restrictions peuvent comprendre : (i) l'exigence de mettre en œuvre des contrôles de sécurité approuvés par l'organisation avant d'autoriser de telles connexions; (ii) la limitation de l'accès à certains types d'information, de services ou d'applications; (iii) l'utilisation de techniques de virtualisation pour limiter le traitement et le stockage d'activités sur des serveurs ou d'autres composants système fournis par l'organisation; (iv) l'acceptation des modalités d'utilisation. En ce qui concerne les dispositifs personnels, les organisations devraient consulter leurs services juridiques au sujet des enjeux juridiques associés à l'utilisation de ces dispositifs dans des environnements opérationnels, y compris les exigences relatives à l'analyse judiciaire dans le cadre d'enquêtes à la suite d'un incident.

(4) UTILISATION DE SYSTÈMES D'INFORMATION EXTERNES | DISPOSITIFS DE STOCKAGE ACCESSIBLES PAR RÉSEAU

L'organisation interdit l'utilisation de [*Affectation : dispositifs de stockage accessibles par réseau, définis par l'organisation*] dans des systèmes d'information externes.

Conseils supplémentaires sur l'amélioration : Les dispositifs de stockage accessibles par réseau dans des systèmes d'information externes comprennent, par exemple, les dispositifs de stockage en ligne dans des systèmes infonuagiques publics, hybrides ou communautaires.

Références :

Aucune

AC-21 COLLABORATION ET ÉCHANGE D'INFORMATION ENTRE UTILISATEURS

Contrôle :

(A) L'organisation facilite l'échange d'information en permettant aux utilisateurs autorisés de déterminer si les autorisations d'accès accordées aux partenaires d'échange respectent les restrictions d'accès à l'information en question, en tenant compte des [*Affectation : circonstances d'échange d'information définies par l'organisation où l'utilisateur doit faire preuve de discrétion*].

(B) L'organisation utilise des [*Affectation : mécanismes automatisés ou processus manuels définis par l'organisation*] pour aider les utilisateurs à prendre des décisions concernant l'échange d'information et la collaboration.

Conseils supplémentaires : Ce contrôle s'applique à l'information susceptible de faire l'objet de restrictions (p. ex. renseignements médicaux, information relative à un contrat, information exclusive ou permettant d'identifier une personne et information classifiée relative à des programmes ou à des compartiments à accès spéciaux) en fonction d'un mode quelconque de détermination officielle ou administrative. Selon les circonstances de l'échange d'information, les partenaires d'échange peuvent être définis comme des personnes, des groupes ou des organisations. L'information peut être définie par contenu, type, catégorie de sécurité, ou programme ou compartiment à accès spécial. Contrôle connexe : AC-3.

Améliorations du contrôle :

(1) ÉCHANGE D'INFORMATION | APPLICATION DES DÉCISIONS AUTOMATISÉES

Le système d'information applique des décisions sur l'échange d'information par utilisateur autorisé en fonction des autorisations d'accès des partenaires d'échange et des restrictions d'accès à l'information à échanger.

(2) ÉCHANGE D'INFORMATION | RECHERCHE ET RÉCUPÉRATION D'INFORMATION

Le système d'information met en œuvre des services de recherche et de récupération de l'information qui appliquent des [*Affectation : restrictions liées à l'échange d'information définies par l'organisation*].

(100) L'ORGANISATION, SUITE À DES ENTENTES ÉCRITES, VEILLE À PRENDRE LES MESURES DE PROTECTION APPROPRIÉES DE L'INFORMATION SENSIBLE ÉCHANGÉE AVEC D'AUTRES GOUVERNEMENTS ET ORGANISATIONS.

Références :

SCT, *Norme de sécurité relative à l'organisation et l'administration* [référence 13].

AC-22 CONTENU ACCESSIBLE AU PUBLIC

Contrôle :

(A) L'organisation désigne les personnes autorisées à afficher de l'information dans un système d'information accessible au public.

(B) L'organisation forme les personnes autorisées afin de s'assurer que l'information accessible au public ne contient aucune information sensible confidentielle.

(C) L'organisation examine le contenu d'information proposé avant de l'afficher sur le système d'information accessible au public pour s'assurer qu'il ne contient aucune information sensible confidentielle.

(D) L'organisation examine tous les [*Affectation : fréquence définie par l'organisation*] le contenu du système d'information accessible au public pour vérifier s'il contient de l'information sensible confidentielle et pour la supprimer le cas échéant.

Conseils supplémentaires : Conformément aux lois du GC et aux politiques, directives et normes du SCT, le grand public n'est pas autorisé à accéder à de l'information sensible confidentielle (p. ex. l'information protégée en vertu de la *Loi sur la protection des renseignements personnels* et les renseignements propriétaires). Ce contrôle concerne les systèmes d'information contrôlés par l'organisation et accessibles au public, généralement sans l'application de mesures d'identification ou d'authentification. L'affichage d'information dans les systèmes d'information non organisationnels est assujetti à une politique de l'organisation. Contrôles connexes : AC-3, AC-4, AT-2, AT-3 et AU-13.

Améliorations du contrôle :

Aucune

Références :

Aucune

AC-23 PROTECTION CONTRE L'EXPLORATION DE DONNÉES

Contrôle :

(A) L'organisation emploie des [*Affectation : techniques de détection et de prévention de l'exploration de données définies par l'organisation*] pour les [*Affectation : objets de stockage de données définis par l'organisation*] pour détecter l'exploration de données et protéger correctement les systèmes d'information contre celle-ci.

Conseils supplémentaires : Les objets de stockage de données comprennent notamment les bases de données, les enregistrements de base de données et les champs de base de données. Les techniques de détection et de prévention de l'exploration de données comprennent, par exemple : (i) limiter les types de réponse fournis aux requêtes de base de données; (ii) limiter le nombre et la fréquence des requêtes de base de données afin d'augmenter le facteur de travail requis pour déterminer le contenu de telles bases de données; (iii) aviser le personnel organisationnel lorsque des requêtes de base de données ou des accès irréguliers ont lieu. Ce contrôle met l'accent sur la protection de l'information de l'organisation contre l'exploration de données lorsque l'information est conservée dans des magasins de données. Au contraire, le contrôle AU-13 porte sur la surveillance de l'information organisationnelle qui pourrait avoir été explorée ou obtenue de magasins de données et qui est maintenant offerte comme de l'information de sources ouvertes dans des sites externes, notamment par l'intermédiaire de sites Web de réseautage social ou de médias sociaux.

Améliorations du contrôle :

Aucune

Références :

Aucune

AC-24 DÉCISIONS DE CONTRÔLE D'ACCÈS

Contrôle :

(A) L'organisation établit les procédures pour s'assurer que les [*Affectation : décisions de contrôle d'accès définies par l'organisation*] sont appliquées à chacune des demandes d'accès avant l'application de l'accès.

Conseils supplémentaires : Les décisions de contrôle d'accès (également appelées décisions d'autorisation) ont lieu lorsque l'information d'autorisation est appliquée à des accès précis. Par contre, l'application de l'accès se produit lorsque les systèmes d'information appliquent les décisions de contrôle d'accès. Bien qu'il arrive

couramment qu'une même entité mette en œuvre les décisions de contrôle d'accès et l'application de l'accès, il n'est pas nécessaire ni toujours optimal qu'une seule entité soit responsable de ces deux mises en œuvre. Pour certains systèmes d'information distribués et certaines architectures, des entités différentes peuvent effectuer les décisions de contrôle d'accès et l'application de l'accès.

Améliorations du contrôle :

(1) DÉCISIONS DE CONTRÔLE D'ACCÈS | TRANSMISSION DE L'INFORMATION SUR L'AUTORISATION D'ACCÈS

Le système d'information transmet [*Affectation : information sur l'autorisation d'accès définie par l'organisation*] au moyen des [*Affectation : mesures de protection de sécurité définies par l'organisation*] aux [*Affectation : systèmes d'information définis par l'organisation*] qui appliquent les décisions de contrôle d'accès.

Conseils supplémentaires sur l'amélioration : Dans les systèmes d'information distribués, les processus d'autorisation et les décisions de contrôle d'accès peuvent avoir lieu dans des parties distinctes des systèmes. Dans ce cas, l'information sur l'autorisation est transmise de façon sécurisée afin que les décisions de contrôle d'accès puissent être appliquées aux emplacements appropriés. Afin d'appuyer les décisions de contrôle d'accès, il pourrait s'avérer nécessaire de transmettre les attributs de sécurité connexes avec l'information sur l'autorisation d'accès, parce que dans les systèmes d'information distribués, diverses décisions de contrôle d'accès doivent être prises en série par différentes entités (p. ex. services) qui ont toutes besoin de certains attributs de sécurité pour prendre les décisions. La protection de l'information sur l'autorisation d'accès (c.-à-d. les décisions de contrôle d'accès) permet d'empêcher que cette information soit modifiée, mystifiée ou compromise au cours de la transmission.

(2) DÉCISIONS DE CONTRÔLE D'ACCÈS | AUCUNE IDENTITÉ D'UTILISATEUR OU PROCESSUS

Le système d'information applique les décisions de contrôle d'accès en fonction des [*Affectation : attributs de sécurité définis par l'organisation*] qui ne contiennent pas l'identité d'utilisateur ni le processus exécuté en leur nom.

Conseils supplémentaires sur l'amélioration : Dans certaines situations, il est important que les décisions de contrôle d'accès soient prises sans information concernant l'identité des utilisateurs présentant les demandes. La protection de la vie privée des personnes est alors de la plus haute importance. Dans d'autres situations, l'information d'identification des utilisateurs n'est pas nécessaire pour les décisions de contrôle d'accès et, surtout dans le cas des systèmes d'information distribués, la transmission de cette information avec le degré d'assurance requis pourrait être très coûteuse ou difficile à accomplir.

Références :

Aucune

AC-25 MONITEUR DE RÉFÉRENCE

Contrôle :

(A) Le système d'information met en œuvre un moniteur de référence pour les [Affectation : politiques de contrôle d'accès définies par l'organisation] qui est résistant aux intrusions, systématiquement appelé et suffisamment simple pour faire l'objet d'une analyse et de tests dont l'exhaustivité peut être assurée.

Conseils supplémentaires : L'information est représentée à l'interne dans les systèmes d'information au moyen d'abstractions également appelées structures de données. Les structures de données internes peuvent représenter différents types d'entités actives et passives. Les entités actives, également appelées sujets, sont habituellement associées à des personnes, à des dispositifs ou à des processus exécutés au nom des personnes. Les entités passives, également appelées objets, sont habituellement associées à des structures de données comme des dossiers, des tampons, des fichiers, des canaux interprocessus et des ports de communications. Les moniteurs de référence appliquent habituellement les politiques de contrôle d'accès non discrétionnaire, c'est-à-dire un type de

contrôle d'accès limitant l'accès aux objets en fonction de l'identité des sujets ou des groupes auxquels les sujets appartiennent. Les contrôles d'accès sont obligatoires puisque les sujets détenant certains privilèges (c.-à-d. droits d'accès) ne peuvent pas transmettre ces droits d'accès à d'autres sujets, que ce soit directement ou indirectement. Le système d'information applique donc la politique de contrôle d'accès rigoureusement en fonction des règles établies par la politique. La propriété de *résistance aux intrusions* du moniteur de référence empêche les adversaires de compromettre le fonctionnement du mécanisme. La propriété *systématiquement appelé* empêche les adversaires de contourner le mécanisme et ainsi d'enfreindre la politique de sécurité. La propriété de *simplicité* aide à assurer l'exhaustivité de l'analyse et des tests des mécanismes pour détecter les faiblesses (c.-à-d. les lacunes latentes) qui empêcheraient l'application de la politique de sécurité. Contrôles connexes : AC-3, AC-16, SC-3 et SC-39.

Améliorations du contrôle :

Aucune

Références :

Aucune

3.2 FAMILLE : SENSIBILISATION ET FORMATION

CLASSE : OPÉRATIONNELLE

AT-1 POLITIQUE ET PROCÉDURES DE FORMATION ET DE SENSIBILISATION À LA SÉCURITÉ

Contrôle :

(A) L'organisation élabore, document et diffuse à *[Affectation : liste des employés et des rôles définie par l'organisation]* :

(a) une politique de sensibilisation et de formation à la sécurité qui définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et le respect;

(b) des procédures pour faciliter la mise en œuvre de la politique de sensibilisation et de formation à la sécurité ainsi que des contrôles connexes.

(B) L'organisation examine et met à jour ce qui suit :

(a) la politique de sensibilisation et de formation à la sécurité *[Affectation : fréquence définie par l'organisation]*;

(b) les procédures de sensibilisation et de formation à la sécurité *[Affectation : fréquence définie par l'organisation]*.

Conseils supplémentaires : Ce contrôle permet de mettre en place la politique et les procédures nécessaires à la mise en œuvre efficace de certains contrôles de sécurité et de certaines améliorations de la famille AT. Les politiques et les procédures rendent compte des lois du GC ainsi que des politiques, des directives et des normes du SCT qui s'appliquent. Les politiques et les procédures du programme de sécurité de l'organisation peuvent rendre facultatives les politiques et les procédures propres au système. La politique peut être intégrée à la politique générale sur la sécurité de l'information de l'organisation ou, inversement, elle peut être représentée par de multiples politiques compte tenu de la nature complexe de certaines organisations. Les procédures peuvent être établies pour le programme de sécurité général et pour des systèmes d'information particuliers, au besoin. La stratégie organisationnelle de gestion des risques est un facteur clé dans l'établissement de la politique et des procédures.

Amélioration du contrôle :

Aucune

Référence :

SCT, *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* [Référence 7].

AT-2 SENSIBILISATION À LA SÉCURITÉ

Contrôle :

(A) L'organisation dispense une formation de base sur la sensibilisation à la sécurité aux utilisateurs du système d'information (y compris les gestionnaires, les cadres supérieurs et les entrepreneurs) :

(a) dans le cadre de la formation initiale à l'intention des nouveaux utilisateurs;

(b) au besoin, lorsque des changements apportés au système d'information l'exigent;

(c) *[Affectation : fréquence définie par l'organisation]* par la suite.

Conseils supplémentaires : Les organisations déterminent le contenu des cours sur la sensibilisation à la sécurité et les techniques connexes en tenant compte des besoins précis de l'organisation et des systèmes d'information auxquels le personnel est autorisé à accéder. Le contenu comprend entre autres de l'information de base sur le besoin de sécuriser l'information et des mesures que doivent prendre les utilisateurs pour maintenir la sécurité et intervenir en cas d'incidents de sécurité suspects. Il porte également sur la sensibilisation au besoin de sécuriser les opérations. Les techniques de sensibilisation peuvent compter l'installation d'affiches, la distribution de fournitures de bureau sur lesquelles sont inscrits des rappels en matière de sécurité, l'envoi par courriel d'avis ou de notifications par des cadres supérieurs de l'organisation, l'affichage de messages lors de l'ouverture de session et la tenue d'activités de sensibilisation à la sécurité de l'information. Contrôles connexes : AT-3, AT-4, PL-4.

Améliorations du contrôle :

(1) SENSIBILISATION À LA SÉCURITÉ | EXERCICES PRATIQUES

L'organisation inclut dans la formation des exercices pratiques de sensibilisation à la sécurité qui simulent des cyberattaques.

Conseils supplémentaires : Les exercices pratiques peuvent par exemple comprendre des tentatives sans préavis de collecte d'information par des mécanismes d'ingénierie sociale, des accès non autorisés ou des simulations de conséquences négatives associées à l'ouverture de pièces jointes malveillantes ou à l'utilisation de liens vers des sites Web malveillants découlant d'attaques de harponnage. Contrôles connexes : CA-2, CA-7, CP-4, IR-3.

(2) SENSIBILISATION À LA SÉCURITÉ | MENACE INTERNE

L'organisation inclut dans la formation des exercices pratiques de sensibilisation à la sécurité pour que le personnel sache reconnaître les indicateurs potentiels d'une menace interne et pour qu'il les signale.

Conseils supplémentaires : Les indicateurs potentiels et les possibles signes précurseurs d'une menace interne peuvent comprendre des comportements comme les suivants : des comportements excessifs, de l'insatisfaction de longue durée en ce qui a trait à son travail, des tentatives d'accès à de l'information inutile dans le cadre de ses tâches, des accès inexpliqués à des ressources financières, de l'intimidation ou du harcèlement sexuel envers des collègues, de la violence en milieu de travail et d'autres manquements graves aux politiques, aux procédures, aux directives, aux règles ou aux pratiques de l'organisation. La formation sur la sensibilisation à la sécurité porte notamment sur la communication par le personnel ou la direction de préoccupations concernant des indicateurs potentiels d'une menace interne au moyen des voies de communication de l'organisation, conformément aux politiques et aux procédures organisationnelles. Contrôles connexes : PL-4, PS-3, PS-6.

Référence :

SCT, *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* [Référence 7].

AT-3 FORMATION À LA SÉCURITÉ AXÉE SUR LES RÔLES

Contrôle :

(A) L'organisation offre de la formation à la sécurité axée sur les rôles aux employés qui assument des rôles et des responsabilités en matière de sécurité :

(a) Avant d'autoriser leur accès au système d'information ou avant qu'ils commencent leurs tâches;

(b) au besoin, lorsque des changements apportés au système d'information l'exigent;

(c) *[Affectation : fréquence définie par l'organisation]* par la suite.

Conseils supplémentaires : Les organisations déterminent le contenu de la formation à la sécurité en tenant compte des rôles et des responsabilités des personnes, des besoins précis en matière de sécurité de l'organisation et des systèmes d'information auxquels le personnel est autorisé à accéder. De plus, elles offrent aux architectes d'entreprise, aux développeurs de systèmes d'information, aux développeurs de logiciels, aux

responsables de l'approvisionnement, aux gestionnaires de système d'information, aux administrateurs de système et de réseau, au personnel chargé des activités de gestion de la configuration et de vérification, au personnel effectuant des activités indépendantes de vérification et de validation, aux évaluateurs de contrôle de sécurité et à d'autres employés qui ont accès aux logiciels au niveau du système une formation technique spécialisée en sécurité pour leur permettre de s'acquitter de leurs tâches. La formation complète axée sur les rôles concerne les rôles et les responsabilités techniques, opérationnels et de gestion qui sont associés aux contrôles de sécurité physiques, techniques et du personnel. Cette formation peut par exemple porter sur les politiques, les procédures, les outils et les produits liés aux rôles de sécurité de l'organisation. Dans le cadre de leur programme de sécurité de l'information, les organisations dispensent également la formation nécessaire pour que les personnes puissent s'acquitter de leurs responsabilités qui sont liées à la sécurité des opérations et de la chaîne d'approvisionnement. La formation à la sécurité axée sur les rôles comprend aussi les entrepreneurs qui offrent des services aux ministères et aux organismes du GC. Contrôles connexes : AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16.

Améliorations du contrôle :

(1) FORMATION À LA SÉCURITÉ | CONTRÔLES ENVIRONNEMENTAUX

L'organisation offre à *[Affectation : liste des employés et des rôles définie par l'organisation]* la formation initiale sur l'utilisation et le fonctionnement des contrôles environnementaux *[Affectation : fréquence définie par l'organisation].*

Conseils supplémentaires : Les contrôles environnementaux comprennent notamment les dispositifs ou les systèmes de suppression et de détection des incendies, les systèmes de gicleurs, les extincteurs manuels, les boyaux d'arrosage fixes, les détecteurs de fumée, les dispositifs de contrôle de la température et de l'humidité, le chauffage, la ventilation et la climatisation de même que l'alimentation dans les installations de l'organisation. Les organisations désignent les employés qui assument des rôles et des responsabilités précises liés aux contrôles environnementaux et qui doivent suivre une formation spécialisée. Contrôles connexes : PE-1, PE-13, PE-14, PE-15.

(2) FORMATION À LA SÉCURITÉ | CONTRÔLES DE SÉCURITÉ PHYSIQUE

L'organisation offre à *[Affectation : liste des employés et des rôles définie par l'organisation]* la formation initiale sur l'utilisation et le fonctionnement des contrôles environnementaux *[Affectation : fréquence définie par l'organisation]*.

Conseils supplémentaires : Les contrôles de sécurité physique comprennent notamment les dispositifs de contrôle d'accès physique, les avertisseurs d'intrusion physique, l'équipement de contrôle et de surveillance ainsi que les gardiens de sécurité (procédures de déploiement et d'exploitation). Les organisations désignent les employés qui assument des rôles et des responsabilités précises liés aux contrôles de sécurité physique et qui doivent suivre une formation spécialisée. Contrôles connexes : PE-2, PE-3, PE-4, PE-5.

(3) FORMATION À LA SÉCURITÉ | EXERCICES PRATIQUES

L'organisation inclut dans la formation à la sécurité des exercices pratiques qui renforcent les objectifs de formation.

Conseils supplémentaires : Les exercices pratiques peuvent comprendre de la formation à la sécurité pour les développeurs de logiciels, comportant des simulations de cyberattaques qui exploitent les vulnérabilités les plus courantes des logiciels (p. ex. le débordement de la mémoire tampon) et d'attaques par harponnage visant des cadres supérieurs. Ces exercices pratiques permettent aux développeurs d'accroître leur compréhension des conséquences de ces vulnérabilités et de voir l'importance des normes et des processus de codage aux fins de sécurité.

(4) FORMATION À LA SÉCURITÉ | COMMUNICATIONS SUSPECTES ET COMPORTEMENTS ANORMAUX DE SYSTÈMES

L'organisation offre à son personnel une formation sur *[Affectation : indicateurs de programmes malveillants définis par l'organisation]* pour qu'il sache reconnaître les communications suspectes et les comportements anormaux dans les systèmes d'information de l'organisation.

Conseils supplémentaires : Un effectif bien formé représente une autre mesure de protection pour les organisations, car il joue un rôle dans le cadre d'une stratégie de défense en profondeur en protégeant les organisations contre des programmes malveillants qui tentent d'infiltrer les systèmes organisationnels par des courriels ou des applications Web. Le personnel est formé pour détecter les courriels potentiellement suspects (p. ex. réception de courriels inattendus, drôlement rédigés ou contenant des fautes de grammaire, ou provenant d'un expéditeur inconnu, qui semble être associé à un partenaire ou à un entrepreneur connu). Il détient également la formation nécessaire pour savoir quoi faire lorsqu'il reçoit ce type de courriels ou de communications Web suspects (p. ex. ne pas ouvrir les pièces jointes, ne pas cliquer sur les liens Web contenus dans un courriel et vérifier l'origine des adresses courriel). Pour veiller au bon fonctionnement du processus, le personnel de l'organisation est bien formé et est mis au courant des caractéristiques des communications suspectes. Grâce à la formation qu'il reçoit pour détecter les comportements anormaux dans les systèmes d'information de l'organisation, le personnel peut avertir rapidement l'organisation de la présence de programmes malveillants. En reconnaissant ces comportements anormaux, le personnel de l'organisation peut servir de complément aux outils et aux systèmes automatisés que les organisations utilisent pour détecter les programmes malveillants et s'en protéger.

Référence :

SCT, *Politique sur la sécurité du gouvernement* (PSG) [Référence 63]

AT-4 DOSSIERS DE FORMATION À LA SÉCURITÉ

Contrôle :

(A) L'organisation consigne et surveille les activités de formation individuelles sur la sécurité des systèmes d'information, y compris la formation de base sur la sensibilisation à la sécurité et la formation sur la sécurité propre aux systèmes d'information.

(B) L'organisation conserve les dossiers de formation individuels pendant *[Affectation : durée définie par l'organisation]*.

Conseils supplémentaires : À la discrétion de l'organisation, chaque superviseur peut consigner les cours spécialisés que suit son personnel. Contrôles connexes : AT-2, AT-3.

Améliorations du contrôle :

Aucune

Référence :

Aucune

AT-5 CONTACTS AVEC LES GROUPES ET LES ASSOCIATIONS DE SÉCURITÉ

[Annulée]

3.3 FAMILLE : VÉRIFICATION ET RESPONSABILITÉ

CLASSE : TECHNIQUE

AU-1 POLITIQUE ET PROCÉDURES DE VÉRIFICATION ET DE RESPONSABILITÉ

Contrôle :

(A) L'organisation élabore, documente et diffuse *à [Affectation : liste des employés et des rôles définie par l'organisation]* :

(a) une politique de vérification et de responsabilité qui définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et le respect;

(b) des procédures pour faciliter la mise en œuvre de la politique de vérification et de responsabilité ainsi que des contrôles connexes.

(B) L'organisation examine et met à jour :

(a) la politique de vérification et de responsabilité *[Affectation : fréquence définie par l'organisation]*;

(b) les procédures de vérification et de responsabilité *[Affectation : fréquence définie par l'organisation]*.

Conseils supplémentaires : Ce contrôle permet de mettre en place la politique et les procédures nécessaires à la mise en œuvre efficace de certains contrôles de sécurité et de certaines améliorations de la famille AU. Les politiques et les procédures rendent compte des lois du GC ainsi que des politiques, des directives et des normes du SCT qui s'appliquent. Les politique et les procédures du programme de sécurité de l'organisation peuvent rendre facultatives les politiques et les procédures propres au système. La politique peut être intégrée à la politique générale sur la sécurité de l'information de l'organisation ou, inversement, elle peut être représentée par de multiples politiques compte tenu de la nature complexe de certaines organisations. Les procédures peuvent être établies pour le programme de sécurité général et pour des systèmes d'information particuliers, au besoin. La stratégie organisationnelle de gestion des risques est un facteur clé dans l'établissement de la politique et des procédures.

Améliorations du contrôle :

Aucune

Références :

SCT, *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* [Référence 7].
CST, *ITSD-03A, Directive sur le contrôle du matériel COMSEC au sein du gouvernement du Canada* [Référence 36].

AU-2 ÉVÉNEMENTS VÉRIFIABLES

Contrôle :

(A) L'organisation détermine la capacité du système d'information de vérifier les événements suivants : *[Affectation : liste des événements vérifiables définie par l'organisation]*.

(B) L'organisation coordonne la fonction de vérification de la sécurité avec d'autres entités organisationnelles qui nécessitent de l'information en matière de vérification pour favoriser le soutien mutuel et faciliter la sélection des événements vérifiables.

(C) L'organisation explique pourquoi les événements vérifiables sont jugés adéquats pour soutenir les enquêtes après coup sur les incidents de sécurité.

(D) L'organisation détermine s'il faut vérifier les événements suivants dans le système d'information : *[Affectation : événements vérifiables (sous-ensemble d'événements vérifiables défini dans le contrôle AU-2 a) et fréquence de vérification (ou la situation qui justifie la vérification) de chacun des événements]*.

Conseils supplémentaires : On entend par *événement* tout fait observable dans un système d'information organisationnel. Pour les organisations, les événements vérifiables représentent des événements importants et pertinents pour la sécurité des systèmes et des environnements d'information dans lesquels ces systèmes sont exploités, car ils permettent de répondre à certains besoins de vérification continue. Les événements vérifiables comptent par exemple les changements de mot de passe, les échecs d'ouverture de session, les tentatives infructueuses d'accès liées aux systèmes d'information, le recours à des droits d'accès administratifs, l'utilisation de justificatifs d'identité de vérification d'identification personnelle ou de justificatifs d'identité d'organismes de troisième part. En définissant le sous-ensemble d'événements vérifiables, les organisations étudient la mise en place d'une vérification adaptée à chacun des contrôles de sécurité. Dans le but d'établir un équilibre entre les besoins en vérification et les autres besoins du système d'information, ce contrôle exige également que soit déterminé le sous-ensemble des événements *vérifiables* qui feront l'objet d'une *vérification* à un moment précis. Par exemple, les organisations peuvent déterminer que les systèmes d'information doivent pouvoir journaliser tous les accès aux fichiers, réussis ou non, mais ne pas activer cette capacité – sauf dans certaines circonstances – en raison de la charge potentielle qu'elle représente envers le rendement du système. D'autres contrôles de sécurité et améliorations de contrôle peuvent faire référence aux besoins en vérification, dont le besoin d'avoir des événements vérifiables. Les organisations incluent également des événements vérifiables qui sont exigés en vertu des lois du GC et des politiques, des directives et des normes du SCT qui s'appliquent. Les enregistrements de vérification peuvent être créés à différents niveaux d'abstraction, y compris au niveau des paquets, lorsque l'information traverse le réseau. La sélection du bon niveau d'abstraction est un aspect essentiel de la capacité de vérification et peut aider à déterminer les causes profondes des problèmes. Les organisations prennent en compte dans la définition des événements vérifiables le besoin de vérifier des événements connexes, comme les étapes liées aux processus diffusés axés sur les transactions (p. ex. processus diffusés dans de multiples organisations) et les opérations qui se produisent dans les architectures orientées services. Contrôles connexes : AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, MP-4, SI-4.

Améliorations du contrôle :

(1) ÉVÉNEMENTS VÉRIFIABLES | COMPILATION DES ENREGISTREMENTS DE VÉRIFICATION PROVENANT DE SOURCES MULTIPLES

[Annulé : intégré au contrôle AU-12]

(2) ÉVÉNEMENTS VÉRIFIABLES | SÉLECTION D'ÉVÉNEMENTS VÉRIFIABLES PAR COMPOSANT DE SYSTÈME D'INFORMATION

[Annulé : intégré au contrôle AU-12]

(3) ÉVÉNEMENTS VÉRIFIABLES | RÉVISIONS ET MISES À JOUR

L'organisation examine et met à jour les événements vérifiables *[Affectation : fréquence définie par l'organisation]*.

Conseils supplémentaires sur l'amélioration : Il se peut que les événements vérifiables de l'organisation changent avec le temps. Il faut réviser et mettre à jour le sous-ensemble d'événements vérifiables régulièrement pour s'assurer qu'il est toujours nécessaire et suffisant.

(4) ÉVÉNEMENTS VÉRIFIABLES | FONCTIONS PRIVILÉGIÉES

[Annulé : intégré au contrôle AC-6(9)]

Référence :

Aucune

AU-3 CONTENU DES ENREGISTREMENTS DE VÉRIFICATION

Contrôle :

(A) Le système d'information génère des enregistrements de vérification qui contiennent de l'information permettant d'établir le type d'événement qui s'est produit, le moment où il s'est produit, l'endroit où il s'est produit, sa source, son résultat ainsi que l'identité de toutes les personnes ou de tous les sujets qui lui sont associés.

Conseils supplémentaires : Le contenu de l'enregistrement de vérification qui peut être jugé nécessaire pour satisfaire aux exigences de ce contrôle comprend notamment les timbres horodateurs, les adresses source et de destination, les identificateurs d'utilisateur ou de processus, les descriptions d'événement, les indications de réussite ou d'échec, les noms des fichiers concernés et les règles de contrôle d'accès ou de flux invoquées. Les résultats de l'événement peuvent comprendre des indicateurs de réussite ou d'échec de l'événement et des résultats propres à l'événement (p. ex. l'état de sécurité du système d'information à la suite de l'événement). Contrôles connexes : AU-2, AU-8, AU-12, SI-11.

Améliorations du contrôle :

(1) CONTENU DES ENREGISTREMENTS DE VÉRIFICATION | INFORMATION DE VÉRIFICATION SUPPLÉMENTAIRE

Le système d'information génère des enregistrements de vérification qui contiennent l'information supplémentaire qui suit : *[Affectation : information supplémentaire et approfondie définie par l'organisation].*

Conseils supplémentaires sur l'amélioration : L'enregistrement plein texte des commandes privilégiées ou les identités individuelles des utilisateurs d'un compte de groupe sont des exemples d'information détaillée dont peuvent tenir compte les organisations dans les enregistrements de vérification. Les organisations pensent à limiter l'information de vérification supplémentaire pour n'avoir que l'information explicitement requise pour répondre aux besoins de vérification précis. Ainsi, l'utilisation des pistes de vérification et des journaux de vérification serait simplifiée, car on ne tiendrait pas compte de l'information qui pourrait être trompeuse ou rendre difficile la localisation de l'information pertinente.

(2) CONTENU DES ENREGISTREMENTS DE VÉRIFICATION | GESTION CENTRALISÉE DU CONTENU DE L'ENREGISTREMENT DE VÉRIFICATION PRÉVU

Le système d'information centralise la gestion et la configuration du contenu des enregistrements de vérification générés par *[Affectation : composants de système d'information définis par l'organisation]*.

Conseils supplémentaires sur l'amélioration : Cette amélioration exige la configuration centralisée du contenu des enregistrements de vérifications (automatisation nécessaire). Les organisations coordonnent la sélection du contenu d'enregistrement requis pour appuyer la capacité de gestion et de configuration centralisée qu'offre le système d'information. Contrôles connexes : AU-6, AU-7.

Référence :

Aucune

AU-4 CAPACITÉ DE STOCKAGE DES VÉRIFICATIONS

Contrôle :

(A) L'organisation attribue la capacité de stockage des enregistrements de vérification selon *[Affectation : besoins de stockage d'enregistrement de vérification définis par l'organisation]*.

Conseils supplémentaires : Les organisations tiennent compte des types de vérification à effectuer et des exigences de traitement pour attribuer la capacité de stockage des vérifications. En attribuant une capacité de stockage des vérifications suffisante, on réduit les risques de dépassement de cette capacité, qui engendrait possiblement l'interruption ou la réduction de cette capacité de vérification. Contrôles connexes : AU-2, AU-5, AU-6, AU-7, AU-11, SI-4.

Améliorations du contrôle :

(1) CAPACITÉ DE STOCKAGE DES VÉRIFICATIONS | TRANSFERT D'ENREGISTREMENTS DANS UNE AUTRE CAPACITÉ DE STOCKAGE

Le système d'information transfère les enregistrements de vérification *[Affectation : fréquence définie par l'organisation]* dans un système ou un support qui est différent du système faisant l'objet de la vérification.

Conseils supplémentaires sur l'amélioration : On entend par *transfert* un processus visant à conserver la confidentialité et l'intégrité des enregistrements de vérification par le déplacement des enregistrements d'un système d'information principal à un système d'information secondaire ou de substitution. Il s'agit d'un processus souvent utilisé dans le cas des systèmes d'information dont la capacité de stockage est limitée. Le stockage de vérification n'est alors qu'une solution temporaire jusqu'à ce que le système puisse communiquer avec le système d'information secondaire ou de substitution mis en place pour stocker les enregistrements de vérification. Lorsque la communication est possible, on procède au transfert de l'information.

Référence :

Aucune

AU-5 INTERVENTION EN CAS D'ÉCHECS DE VÉRIFICATION

Contrôle :

(A) Le système d'information avertit *[Affectation : liste des employés définie par l'organisation]* en cas d'échecs de vérification;

(B) Le système d'information prend les mesures supplémentaires suivantes : *[Affectation : mesures à prendre définies par l'organisation (p. ex. interruption du système, écrasement des enregistrements de vérification les plus anciens, interruption de la génération des enregistrements de vérification)]*.

Conseils supplémentaires : Les échecs de vérification comprennent notamment les erreurs logicielles ou matérielles, la défaillance des mécanismes de saisie des vérifications ainsi que l'atteinte ou le dépassement de la capacité de stockage des vérifications. Les organisations peuvent choisir de mettre en place des mesures supplémentaires en fonction des différents échecs de vérification (p. ex. selon le type, l'emplacement, la gravité ou une combinaison de ces facteurs). Ce contrôle s'applique à tous les dépôts de stockage de données de vérification (chacun des composants du système d'information dans lesquels sont stockés des enregistrements de vérification), à la capacité de stockage de vérifications d'ensemble des organisations (tous les dépôts de données de vérification combinés) ou aux deux options. Contrôles connexes : AU-4, SI-12.

Améliorations du contrôle :

(1) INTERVENTION EN CAS D'ÉCHECS DE VÉRIFICATION | CAPACITÉ DE STOCKAGE DES VÉRIFICATIONS

Le système d'information avertit *[Affectation : liste des employés, des fonctions ou des emplacements définie par l'organisation]* dans un délai de *[Affectation : délai défini par l'organisation]* lorsque le volume de stockage attribué aux enregistrements de vérification atteint *[Affectation : pourcentage défini par l'organisation]* de sa capacité maximale.

Conseils supplémentaires sur l'amélioration : Les organisations peuvent se voir attribuer plusieurs dépôts de stockage de données de vérification se trouvant dans de multiples composants de système d'information; chacun des dépôts a une capacité de volume de stockage différente.

(2) INTERVENTION EN CAS D'ÉCHEC DE VÉRIFICATION | ALERTES EN TEMPS RÉEL

Le système d'information avertit *[Affectation : liste des employés, des fonctions ou des emplacements définie par l'organisation]* en *[Affectation : période en temps réel définie par l'organisation]* lorsque les événements d'échec de vérification suivants se produisent : *[Affectation : événements d'échec de vérification définis par l'organisation qui nécessitent une alerte en temps réel]*.

Conseils supplémentaires sur l'amélioration : Les alertes génèrent des messages d'urgence pour les organisations. La vitesse à laquelle ces messages sont générés à la suite des alertes en temps réel dépend de la technologie de l'information utilisée (le temps qui s'écoule entre la détection de l'événement et de l'alerte est inférieur à quelques secondes).

(3) INTERVENTION EN CAS D'ÉCHEC DE VÉRIFICATION | SEUILS DE VOLUME DE TRAFIC CONFIGURABLES

Le système d'information applique des seuils de volume de trafic configurable aux communications réseau, qui représentent les limites de la capacité de vérification et *[Sélection : rejette ou retarde]* tout trafic réseau supérieur à ces seuils.

Conseils supplémentaires sur l'amélioration : Les organisations peuvent rejeter ou retarder le traitement du trafic des communications réseau si elles jugent que le trafic dépasse la capacité de stockage de la fonction de vérification du système d'information. Le choix de rejeter ou de retarder le trafic dépend des seuils de volume de trafic établis par l'organisation, qui peuvent être adaptés en fonction des changements apportés à la capacité de stockage des vérifications.

(4) INTERVENTION EN CAS D'ÉCHEC DE VÉRIFICATION | INTERRUPTION EN CAS D'ÉCHEC

Le système d'information procède à *[Sélection : l'interruption complète du système; l'interruption partielle du système; la détérioration des opérations en limitant les fonctions associées à la mission et aux activités] en cas de [Affectation : échecs de vérification définis par l'organisation]*, sauf s'il existe une capacité de vérification de substitution.

Conseils supplémentaires sur l'amélioration : Les organisations déterminent les types d'échecs de vérification qui peuvent engendrer automatiquement l'interruption ou la détérioration des opérations du système d'information. Étant donné l'importance de veiller à la continuité de leur mission et de leurs activités, les organisations peuvent déterminer que la nature de l'échec de vérification n'est pas assez grave pour justifier l'interruption complète du système d'information qui permet de mener les activités principales associées à la mission. Le cas échéant, l'interruption partielle du système d'information ou la dégradation des opérations réduisant les capacités peuvent constituer des solutions viables. Contrôle connexe : AU-15.

Référence :

Aucune

AU-6 EXAMEN, ANALYSE ET RAPPORTS DE VÉRIFICATION

Contrôle :

(A) L'organisation examine et analyse les enregistrements de vérification du système d'information *[Affectation : fréquence définie par l'organisation]* pour déceler toute indication de *[Affectation : activités inappropriées ou inhabituelles définies par l'organisation]*.

(B) L'organisation fait part de ses constatations à *[Affectation : liste des employés ou des rôles définie par l'organisation]*.

Conseils supplémentaires : L'examen, l'analyse et les rapports de vérification connexes portent sur les vérifications en matière de sécurité de l'information qu'effectuent les organisations, par exemple, les vérifications qui découlent de la surveillance de l'utilisation d'un compte, de l'accès à distance, de la connectivité sans fil, de la connexion de dispositifs mobiles, de paramètres de configuration, de l'inventaire des composants de système d'information, de l'utilisation d'outils de maintenance et de télémaintenance, de l'accès physique, de la température et de l'humidité, de la livraison et du retrait d'équipement, de communications aux frontières du système d'information et de l'utilisation de code mobile et de voix sur protocole Internet (VoIP pour *Voice over Internet Protocol*). Les constatations peuvent être communiquées à des entités de l'organisation, dont l'équipe de réaction aux incidents, l'équipe des services de dépannage et le groupe chargé de la sécurité de l'information. Si des organisations n'ont pas l'autorisation d'examiner et d'analyser l'information de vérification ou si elles ne sont pas en mesure de mener de telles activités (p. ex. dans certaines applications ou certains systèmes de sécurité

nationale), d'autres organisations détenant ce pouvoir peuvent le faire pour elles. Contrôles connexes : AC-2, AC-3, AC-6, AC-17, AT-3, AU-7, AU-16, CA-7, CM-5, CM-10, CM-11, IA-3, IA-5, IR-5, IR-6, MA-4, MP-4, PE-3, PE-6, PE-14, PE-16, RA-5, SC-7, SC-18, SC-19, SI-3, SI-4, SI-7.

Améliorations du contrôle :

(1) EXAMEN, ANALYSE ET RAPPORTS DE VÉRIFICATION | INTÉGRATION DES PROCESSUS

L'organisation utilise des mécanismes automatisés pour intégrer les processus d'examen, d'analyse et de rapports de vérification afin de soutenir les processus organisationnels d'enquête et d'intervention en cas d'activités suspectes.

Conseils supplémentaires sur l'amélioration : Les processus organisationnels qui tirent profit de l'intégration des processus d'examen, d'analyse et de rapports de vérification comprennent les processus de réaction aux incidents, de surveillance continue, de planification d'urgence et de surveillance par l'inspecteur général. Contrôle connexe : AU-12.

(2) EXAMEN, ANALYSE ET RAPPORTS DE VÉRIFICATION | ALERTES DE SÉCURITÉ AUTOMATISÉES

[Annulé : Intégré au contrôle SI-4]

(3) EXAMEN, ANALYSE ET RAPPORTS DE VÉRIFICATION | DÉPÔTS DE VÉRIFICATION CORRESPONDANTS

L'organisation analyse et fait correspondre les enregistrements de vérification des différents dépôts afin d'acquérir une connaissance globale de la situation.

Conseils supplémentaires sur l'amélioration : La connaissance globale de la situation de l'organisation comprend la connaissance des trois niveaux de gestion des risques (organisation, mission et processus opérationnel ainsi que système d'information) et aide avoir une connaissance interorganisationnelle. Contrôles connexes : AU-12, IR-4.

(4) EXAMEN, ANALYSE ET RAPPORTS DE VÉRIFICATION | ANALYSES ET EXAMENS CENTRALISÉS

Le système d'information permet de centraliser les examens et les analyses des enregistrements de vérification provenant de plusieurs composants du système d'information.

Conseils supplémentaires sur l'amélioration : On compte parmi les mécanismes automatisés liés aux examens et aux analyses centralisés les produits de gestion de l'information de sécurité. Contrôles connexes : AU-2, AU-12.

(5) EXAMEN, ANALYSE ET RAPPORTS DE VÉRIFICATION | INTÉGRATION DES CAPACITÉS D'ANALYSE ET DE SURVEILLANCE

L'organisation intègre l'analyse des enregistrements de vérification et l'analyse de *[Sélection (un choix ou plus) : l'information liée au balayage des vulnérabilités; les données de rendement; l'information sur la surveillance du système d'information; [Affectation : données ou information recueillies par d'autres sources définies par l'organisation]]* pour accroître sa capacité de détecter les activités inappropriées ou inhabituelles.

Conseils supplémentaires sur l'amélioration : Le balayage des vulnérabilités, la génération de données de rendement et la surveillance du système d'information ne sont pas nécessaires pour cette amélioration. Dans le cadre de cette amélioration, il faut plutôt intégrer l'analyse de l'information liée aux activités susmentionnées que l'on obtient autrement et l'analyse de l'information de vérification. Des outils de gestion de l'information et d'événements de sécurité peuvent faciliter l'intégration et la consolidation des enregistrements de vérification que produisent les nombreux composants du système d'information, de même que leur analyse et leurs associations. L'utilisation de scripts normalisés d'analyse des enregistrements de vérification développés par les organisations (complétés par des scripts localisés, au besoin) offre une approche plus rentable de l'analyse de l'information liée aux enregistrements de vérification recueillie. La corrélation entre l'information contenue dans les enregistrements de vérification et celle produite par le balayage des vulnérabilités est importante, car elle permet d'établir la justesse des balayages de vulnérabilités et d'établir des liens entre les événements de détection d'attaques et les résultats des balayages. Les liens avec les données de rendement peuvent contribuer à la découverte

d'attaques par déni de service ou de cyberattaques ayant mené à l'utilisation non autorisée de ressources. Les associations avec l'information sur la surveillance du système peuvent contribuer à détecter des attaques et à établir un lien accru entre l'information de vérification et les situations opérationnelles. Contrôles connexes : AU-12, IR-4, RA-5.

(6) EXAMEN, ANALYSE ET RAPPORTS DE VÉRIFICATION | CORRÉLATION AVEC L'INFORMATION LIÉE À LA SURVEILLANCE PHYSIQUE

L'organisation met en corrélation l'information des enregistrements de vérification avec celle découlant de la surveillance de l'accès physique pour accroître sa capacité à détecter des activités suspectes, inappropriées, inhabituelles ou malveillantes.

Conseils supplémentaires sur l'amélioration : En mettant en corrélation l'information de vérification liée à la surveillance physique et les journaux de vérification des systèmes d'information, les organisations peuvent détecter des comportements suspects ou des signes associés à ce type de comportement. Par exemple, la corrélation entre l'identité d'un individu qui permet l'accès logique à certains systèmes d'information et l'information liée à la sécurité physique supplémentaire qui révèle la présence de l'individu sur place lorsque l'accès logique a eu lieu peut s'avérer utile dans le cadre d'enquêtes.

(7) EXAMEN, ANALYSE ET RAPPORTS DE VÉRIFICATION | OPÉRATIONS AUTORISÉES

L'organisation précise les opérations qui sont autorisées concernant chaque *[Sélection (un choix ou plus) : processus, rôle ou utilisateur]* associé à l'examen, à l'analyse et aux rapports de l'information de vérification.

Conseils supplémentaires sur l'amélioration : Les organisations précisent les opérations autorisées concernant les processus, les rôles et les utilisateurs du système d'information en ce qui a trait à l'examen, à l'analyse et aux rapports des enregistrements de vérification en recourant à des techniques de gestion des comptes. Il s'agit d'une façon d'appliquer le principe des droits d'accès minimaux. Le système d'information veille au respect des opérations autorisées, dont la lecture, l'écriture, l'exécution, l'annexion et la suppression.

(8) EXAMEN, ANALYSE ET RAPPORTS DE VÉRIFICATION | ANALYSE PLEIN TEXTE DES COMMANDES PRIVILÉGIÉES

L'organisation mène une analyse plein texte des commandes privilégiées vérifiées dans un composant de système d'information ou un sous-système physiquement distinct du système d'information ou dans un autre système d'information conçu pour mener cette analyse.

Conseils supplémentaires sur l'amélioration : Cette amélioration exige l'utilisation d'un environnement distinct pour analyser l'information de vérification concernant les utilisateurs qui détiennent des droits d'accès privilégiés afin de ne pas compromettre l'information dans le système d'information dans lequel les utilisateurs ont des privilèges élevés, dont la capacité d'exécuter des commandes privilégiées. On entend par *analyse plein texte* l'analyse qui prend en compte le texte intégral associé aux commandes privilégiées (c.-à-d. les commandes et tous les paramètres) contrairement aux analyses qui ne tiennent compte que du nom de la commande. L'analyse plein texte comprend le recours au filtrage et à l'heuristique. Contrôles connexes : AU-3, AU-9, AU-11, AU-12.

(9) EXAMEN, ANALYSE ET RAPPORTS DE VÉRIFICATION | CORRÉLATION AVEC L'INFORMATION PROVENANT DE SOURCES NON TECHNIQUES

L'organisation met en corrélation l'information provenant de sources non techniques et l'information de vérification afin d'acquérir une connaissance globale de sa situation.

Conseils supplémentaires sur l'amélioration : On compte parmi les sources non techniques les données liées aux ressources humaines qui répertorient les manquements aux politiques organisationnelles (p. ex. le harcèlement sexuel et l'utilisation inappropriée d'actifs d'information organisationnels). Grâce à ce type d'information, les efforts d'analyse des organisations sont plus ciblés et permettent de détecter les possibles activités malveillantes provenant de l'interne. En raison de la nature sensible de l'information provenant de sources non techniques, les organisations limitent l'accès à cette information pour minimiser les risques de divulgation par inadvertance d'information liée à la vie privée à des personnes qui ne répondent pas au besoin de connaître. Ainsi, on établit généralement des liens entre l'information provenant de sources non

techniques et l'information de vérification uniquement lorsque l'on soupçonne l'implication d'un individu dans un incident de sécurité. Les organisations sollicitent des conseils juridiques avant de prendre des mesures. Contrôle connexe : AT-2.

(10) EXAMEN, ANALYSE ET RAPPORTS DE VÉRIFICATION | AJUSTEMENT DU NIVEAU D'EXAMEN

L'organisation ajuste le niveau d'examen, d'analyse et de rapports de vérification dans le système d'information lorsqu'un changement fondé sur des renseignements relatifs au maintien de l'ordre, du renseignement brut ou d'autres sources crédibles d'information est apporté au risque.

Conseils supplémentaires sur l'amélioration : Il est possible d'ajuster la fréquence, la portée ou la profondeur de l'examen, de l'analyse ou des rapports de vérification pour répondre aux besoins organisationnels lorsqu'une nouvelle information est reçue.

Référence :

SCT, *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* [Référence 7].

AU-7 RÉDUCTION DES VÉRIFICATIONS ET GÉNÉRATION DE RAPPORTS

Contrôle :

(A) Le système d'information permet de réduire les vérifications et de générer des rapports pour répondre aux besoins d'examen, d'analyse et de rapports de vérification sur demande ainsi qu'aux enquêtes après coup sur les incidents de sécurité.

(B) Le système d'information offre une capacité qui permet de réduire les vérifications et de générer des rapports et qui ne change pas le contenu original ni le classement chronologique des enregistrements de vérification.

Conseils supplémentaires : La réduction des vérifications consiste en un processus permettant de manipuler l'information de vérification recueillie et de la condenser afin d'en accroître la valeur pour les analystes. Les capacités de réduction des vérifications et de génération de rapports ne proviennent pas toujours du même système d'information ou des mêmes entités organisationnelles qui mènent les activités de vérification. La capacité de réduction des vérifications peut entre autres comprendre des techniques modernes d'exploration de données comportant des filtres de données avancés qui permettent de détecter des comportements anormaux dans les enregistrements de vérification. La capacité de génération de rapports qu'offre le système d'information peut générer des rapports spécialisés. Le classement chronologique des enregistrements de vérification peut représenter un enjeu important si la granularité de l'estampille temporelle de l'enregistrement est insuffisante. Contrôle connexe : AU-6.

Améliorations du contrôle :

(1) RÉDUCTION DES VÉRIFICATIONS ET GÉNÉRATION DE RAPPORTS | TRAITEMENT AUTOMATISÉ

Le système d'information permet de traiter des enregistrements de vérification liés à des événements d'intérêt selon *[Affectation : champs d'enregistrements de vérification définis par l'organisation]*.

Conseils supplémentaires sur l'amélioration : Il est possible de déterminer les événements d'intérêt selon le contenu de certains champs d'enregistrement de vérification, dont l'identité des individus, les types d'événements, les emplacements, les heures et les dates des événements, les ressources système et les adresses IP concernées, ou les objets d'information auxquels on a accédé. Les organisations peuvent définir les critères d'événements de vérification selon le degré de granularité requis, par exemple, les emplacements choisis par l'emplacement du réseau général (p. ex. le réseau ou le sous-réseau) ou par un composant du système d'information précis. Contrôles connexes : AU-2, AU-12.

(2) RÉDUCTION DES VÉRIFICATIONS ET GÉNÉRATION DE RAPPORTS | TRIAGE ET RECHERCHE AUTOMATISÉS

Le système d'information permet de trier et de rechercher des enregistrements de vérification liés à des événements d'intérêt selon le contenu de *[Affectation : champs des enregistrements de vérification définis par l'organisation]*.

Conseils supplémentaires sur l'amélioration : Le triage et la recherche d'enregistrements de vérification peut reposer sur le contenu des champs d'enregistrement de vérification, dont ce qui suit : (i) la date et l'heure des événements, (ii) les identificateurs d'utilisateur, (iii) les adresses de protocole Internet associées à l'événement, (iv) le type d'événement ou (v) la réussite ou l'échec de l'événement.

Référence :

Aucune

AU-8 ESTAMPILLES TEMPORELLES

Contrôle :

(A) Le système d'information utilise des horloges de système internes afin de générer des estampilles temporelles pour les enregistrements de vérification.

(B) Le système d'information consigne les estampilles temporelles des enregistrements de vérification que l'on peut faire correspondre au temps universel coordonné (UTC) ou au temps moyen de Greenwich (UT), et respecte *[Affectation : granularité de la mesure du temps définie par l'organisation]*.

Conseils supplémentaires : Les estampilles temporelles que génère le système d'information comportent la date et l'heure. L'heure est souvent exprimée selon l'UTC, un prolongement moderne du TMG, ou selon l'heure locale qui est décalée par rapport à l'UTC. On entend par *granularité des mesures de temps* le degré de synchronisation entre les horloges du système d'information et les horloges de référence, par exemple les horloges qui sont synchronisées à des centaines ou à des dizaines de millisecondes. Les organisations peuvent définir des granularités de temps différentes pour les divers composants de système d'information. Le service lié au temps peut aussi s'avérer essentiel dans le cas d'autres capacités de sécurité comme le contrôle d'accès ainsi que l'identification et l'authentification, selon la nature des mécanismes employés pour soutenir ces capacités. Contrôles connexes : AU-3, AU-12.

Améliorations du contrôle :

(1) ESTAMPILLES TEMPORELLES | SYNCHRONISATION AVEC LA SOURCE DE TEMPS QUI FAIT AUTORITÉ

(a) Le système d'information compare ses horloges internes *[Affectation : fréquence définie par l'organisation]* en utilisant *[Affectation : source de temps faisant autorité définie par l'organisation]*.

(b) Le système d'information synchronise ses horloges internes avec la source de temps qui fait autorité lorsque la différence de temps est supérieure à *[Affectation : temps défini par l'organisation]*.

Conseils supplémentaires sur l'amélioration : Cette amélioration permet de synchroniser les estampilles temporelles des systèmes d'information ayant de multiples horloges systèmes de même que des systèmes connectés à un réseau.

(2) ESTAMPILLES TEMPORELLES | DEUXIÈME SOURCE DE TEMPS QUI FAIT AUTORITÉ

Le système d'information choisit une deuxième source de temps qui fait autorité, laquelle se trouve dans une région géographique différente de celle de la première source de temps qui fait autorité.

Référence :

Aucune

AU-9 PROTECTION DE L'INFORMATION DE VÉRIFICATION

Contrôle :

(A) Le système d'information protège l'information de vérification et les outils de vérification contre l'accès, la modification et la suppression non autorisés.

Conseils supplémentaires : L'information de vérification comprend toute information (p. ex. enregistrements de vérification, paramètres de vérification et rapports de vérification) nécessaire à la réussite de l'activité de vérification du système d'information. Ce contrôle est axé sur la protection technique de l'information de vérification. Les contrôles de protection des supports ainsi que les contrôles de protection physiques et environnementaux protègent physiquement l'information de vérification. Contrôles connexes : AC-3, AC-6, MP-2, MP-4, PE-2, PE-3, PE-6.

Améliorations du contrôle :

(1) PROTECTION DE L'INFORMATION DE VÉRIFICATION | SUPPORTS MATÉRIELS NON RÉINSCRIPTIBLES

Le système d'information consigne les enregistrements de vérification sur des supports matériels non réinscriptibles.

Conseils supplémentaires sur l'amélioration : Cette amélioration s'applique aux pistes de vérification de première génération (c.-à-d. les enregistrements de vérification qui constituent l'information de vérification qu'il faut utiliser à des fins de détection, d'analyse et d'élaboration de rapports) ainsi qu'aux pistes de vérification sauvegardées. Elle ne s'applique pas aux enregistrements de vérification de première génération avant qu'elles ne soient consignées dans une piste de vérification. On compte entre autres parmi les supports non réinscriptibles les disques compacts inscriptibles et les DVD inscriptibles. À l'inverse, le recours à des supports de protection d'écriture commutables, comme des cartouches de bande magnétique ou des bus série universel (USB pour *Universal Serial Bus*), entraîne l'utilisation de supports de protection d'écriture, pas l'utilisation de supports non réinscriptibles. Contrôles connexes : AU-4, AU-5.

(2) PROTECTION DE L'INFORMATION DE VÉRIFICATION | SAUVEGARDE DES VÉRIFICATIONS SUR DES SYSTÈMES D'INFORMATION OU DES COMPOSANTS DE SYSTÈME D'INFORMATION PHYSIQUES DISTINCTS

Le système d'information sauvegarde les enregistrements de vérification *[Affectation : fréquence définie par l'organisation]* sur un système d'information ou un composant de système d'information qui est physiquement différent du système ou du composant faisant l'objet de la vérification.

Conseils supplémentaires sur l'amélioration : Cette amélioration permet de veiller à ce qu'une compromission du système d'information qui fait l'objet d'une vérification n'engendre pas la compromission des enregistrements de vérification. Contrôles connexes : AU-4, AU-5, AU-11.

(3) PROTECTION DE L'INFORMATION DE VÉRIFICATION | PROTECTION CRYPTOGRAPHIQUE

Le système d'information met en place des mécanismes cryptographiques pour protéger l'intégrité de l'information de vérification et des outils de vérification.

Conseils supplémentaires sur l'amélioration : Les mécanismes cryptographiques servant à protéger l'intégrité de l'information de vérification comprennent des fonctions de hachage signé au moyen de cryptographie asymétrique qui permettent de diffuser la clé publique pour vérifier l'information de hachage tout en préservant la confidentialité de la clé secrète ayant servi à générer l'algorithme de hachage. Contrôles connexes : AU-10, SC-12, SC-13.

(4) PROTECTION DE L'INFORMATION DE VÉRIFICATION | ACCÈS PAR UN SOUS-ENSEMBLE D'UTILISATEURS PRIVILÉGIÉS

L'organisation autorise l'accès à la fonction de gestion de la vérification uniquement à *[Affectation : sous-ensemble d'utilisateurs privilégiés défini par l'organisation]*.

Conseils supplémentaires sur l'amélioration : Les personnes qui détiennent des droits d'accès privilégiés à un système d'information et qui font aussi l'objet de vérifications par ce système peuvent influencer la fiabilité de l'information de vérification en entravant les activités de vérification ou en modifiant les enregistrements de vérification. Cette amélioration exige que les accès privilégiés liés à la vérification diffèrent des autres accès privilégiés, permettant ainsi de réduire le nombre d'utilisateurs possédant des privilèges de vérification. Contrôle connexe : AC-5.

(5) PROTECTION DE L'INFORMATION DE VÉRIFICATION | DOUBLE AUTORISATION

L'organisation applique le principe de double autorisation pour *[Sélection (un choix ou plus) : déplacement, suppression]* de *[Affectation : mesures définies par l'organisation]*.

Conseils supplémentaires sur l'amélioration : Les organisations peuvent choisir différentes options pour les divers types d'information de vérification. Les mécanismes de double autorisation exigent l'approbation de deux personnes autorisées pour permettre la prise d'une mesure. La double autorisation est également appelée le contrôle par deux personnes. Contrôles connexes : AC-3, MP-2.

(6) PROTECTION DE L'INFORMATION DE VÉRIFICATION | LECTURE SEULE

L'organisation accorde un accès « lecture seule » à l'information de vérification à *[Affectation : sous-ensemble d'utilisateurs privilégiés défini par l'organisation]*.

Conseils supplémentaires sur l'amélioration : En restreignant les droits d'accès aux utilisateurs privilégiés pour qu'ils n'aient qu'un accès « lecture seule », on limite les possibles dommages qu'ils pourraient causer à l'organisation (p. ex. supprimer les enregistrements de vérification pour dissimuler des activités malveillantes).

Référence :

Aucune

AU-10 NON-RÉPUDIATION

Contrôle :

(A) Le système d'information offre une protection contre quiconque (ou contre tout processus exécuté en son nom) nie faussement avoir effectué *[Affectation : opérations de non-répudiation définies par l'organisation]*.

Conseils supplémentaires : La création d'information, l'envoi et la réception de messages et l'approbation d'information (p. ex. confirmation d'un accord ou signature d'un contrat) sont des exemples d'opérations de non-répudiation effectuées par des personnes. La non-répudiation protège les personnes contre toute déclaration ultérieure (i) d'un auteur qui nie être le créateur d'un document particulier, (ii) d'un émetteur qui nie avoir transmis un message, (iii) d'un destinataire qui nie avoir reçu un message ou (iv) d'un signataire qui nie avoir signé un document. Les services de non-répudiation peuvent servir à déterminer si l'information provient d'une personne en particulier, si une personne a pris des mesures particulières (p. ex. envoi d'un courriel, signature d'un contrat, approbation d'une demande d'approvisionnement) ou si elle a reçu certains renseignements. Les organisations obtiennent des services de non-répudiation grâce à plusieurs techniques ou mécanismes (p. ex. signatures numériques, reçus numériques de message). Contrôles connexes : SC-12, SC-8, SC-13, SC-16, SC-17, SC-23.

Améliorations du contrôle :

(1) NON-RÉPUDIATION | ASSOCIATION AVEC LES IDENTITÉS

(a) Le système d'information associe l'identité de l'auteur d'une information avec l'information de *[Affectation : robustesse du lien définie par l'organisation]*.

(b) Le système d'information permet aux personnes autorisées de déterminer l'identité de l'auteur de l'information.

Conseils supplémentaires sur l'amélioration : Cette amélioration satisfait aux exigences de vérification selon lesquelles le personnel de l'organisation doit pouvoir identifier l'auteur d'une information particulière

dans l'éventualité d'un transfert d'information. Les organisations déterminent et approuvent la robustesse du lien entre l'auteur de l'information et l'information en fonction de la catégorie de sécurité de l'information et des facteurs de risque pertinents. Contrôles connexes : AC-4, AC-16.

(2) NON-RÉPUDIATION | VALIDITÉ DU LIEN AVEC L'IDENTITÉ DE L'AUTEUR DE L'INFORMATION

(a) Le système d'information valide le lien entre l'identité de l'auteur de l'information et l'information *[Affectation : fréquence définie par l'organisation]*.

(b) Le système d'information effectue *[Affectation : opérations définies par l'organisation]* en cas d'erreur de validation.

Conseils supplémentaires sur l'amélioration : Cette amélioration permet de prévenir toute modification de l'information entre sa production et son examen. La validation des liens peut être effectuée, par exemple, par l'utilisation des totaux des contrôles cryptographiques. Les organisations déterminent si les validations découlent des demandes d'utilisateurs ou si elles sont générées automatiquement. Contrôles connexes : AC-3, AC-4, AC-16.

(3) NON-RÉPUDIATION | CHAÎNE DE POSSESSION

Le système d'information conserve, dans la chaîne de possession établie, l'identité et les justificatifs d'identité de l'examinateur ou de l'émetteur pour toute l'information examinée ou diffusée.

Conseils supplémentaires sur l'amélioration : La chaîne de possession est un processus qui permet de faire le suivi des transferts de l'information lors de sa collecte, de sa protection et de son cycle de vie en consignant le nom de chaque personne l'ayant traité, la date et l'heure de sa collecte et de son transfert ainsi que l'objectif de son transfert. Si l'examinateur est une personne ou si la fonction d'examen est automatisée mais distincte de la fonction de diffusion ou de transfert, le système d'information associe à l'information et à l'étiquette de l'information l'identité de l'examinateur de l'information à diffuser. Dans le cas d'un examen effectué par une personne, l'amélioration de contrôle fournit aux responsables de l'organisation le moyen d'identifier l'examinateur et le diffuseur de l'information. Dans le cas d'un examen automatisé, elle permet d'assurer que seules des fonctions d'examen approuvées ont été utilisées. Contrôles connexes : AC-4, AC-16.

(4) NON-RÉPUDIATION | VALIDITÉ DU LIEN AVEC L'IDENTITÉ DE L'EXAMINATEUR DE L'INFORMATION

(a) Le système d'information valide le lien entre l'identité de l'examinateur et l'information au point de transfert ou de diffusion, avant que l'information ne soit transférée ou diffusée *[Affectation : d'un domaine de sécurité à un autre définis par l'organisation]*.

(b) Le système d'information effectue *[Affectation : opérations définies par l'organisation]* en cas d'erreur de validation.

Conseils supplémentaires sur l'amélioration : Cette amélioration permet de prévenir toute modification de l'information entre son examen et son transfert ou sa diffusion. La validation des liens peut être effectuée, par exemple, par l'utilisation de totaux de contrôle cryptographiques. Les organisations déterminent si les validations découlent des demandes d'utilisateurs ou si elles sont générées automatiquement. Contrôles connexes : AC-4, AC-16.

(5) NON-RÉPUDIATION | SIGNATURES NUMÉRIQUES

[Annulé : Intégré au contrôle SI-7]

Référence :

CST, ITSG-31, *Guide sur l'authentification des utilisateurs pour les systèmes TI* [Référence 18].

AU-11 CONSERVATION DES ENREGISTREMENTS DE VÉRIFICATION

Contrôle :

(A) L'organisation conserve les enregistrements de vérification pendant *[Affectation : durée définie par l'organisation et conforme à la politique de conservation des dossiers]* pour appuyer les enquêtes après coup sur les incidents de sécurité et satisfaire aux exigences réglementaires et organisationnelles de conservation de l'information.

Conseils supplémentaires sur l'amélioration : Les organisations conservent les enregistrements de vérification jusqu'à ce qu'on détermine qu'ils ne sont plus requis à des fins administratives, juridiques ou de vérification, ou encore à d'autres fins opérationnelles, ce qui comprend la conservation et la disponibilité des enregistrements de vérification pour répondre à des demandes de nature juridique, des assignations à témoigner et des mesures d'application de la loi. Les organisations créent des catégories pour les enregistrements de vérification en fonction de ces types de mesures de même que des processus d'intervention pour chacun des types de mesure. Contrôles connexes : AU-4, AU-5, AU-9, MP-6.

Améliorations du contrôle :

(1) CONSERVATION DES ENREGISTREMENTS DE VÉRIFICATION | CAPACITÉ DE RÉCUPÉRATION À LONG TERME

L'organisation a recours à *[Affectation : mesures définies par l'organisation]* pour s'assurer que les enregistrements de vérification à long terme que génère le système d'information sont récupérables.

Conseils supplémentaires sur l'amélioration : On compte parmi les mesures que prennent les organisations pour faciliter la récupération des enregistrements de vérification la conversion des enregistrements dans de nouveaux formats, la conservation de l'équipement pouvant lire les enregistrements ainsi que la conservation de documents nécessaires pour aider le personnel de l'organisation à comprendre comment interpréter les enregistrements.

Référence :

Aucune

AU-12 GÉNÉRATION D'ENREGISTREMENTS DE VÉRIFICATION

Contrôle :

(A) Le système d'information permet de générer des enregistrements de vérification liés à des événements vérifiables qui sont définis au contrôle AU-2a au *[Affectation : composants du système d'information définis par l'organisation]*.

(B) Le système d'information permet à *[Affectation : liste des employés ou des rôles définis par l'organisation]* de sélectionner les événements vérifiables qui doivent être vérifiés par des composants de système d'information particuliers.

(C) Le système d'information génère des enregistrements de vérification pour les événements vérifiés qui sont définis au contrôle AU-2d et dont le contenu est défini au contrôle AU-3.

Conseils supplémentaires : Les enregistrements de vérification peuvent provenir de nombreux différents composants de système d'information. La liste des événements vérifiés constitue l'ensemble des événements pour lesquels il faut produire un enregistrement de vérification. Ces événements sont habituellement un sous-ensemble de tous les événements pour lesquels le système d'information peut générer des enregistrements de vérification. Contrôles connexes : AC-3, AU-2, AU-3, AU-6, AU-7.

Améliorations du contrôle :

(1) GÉNÉRATION D'ENREGISTREMENTS DE VÉRIFICATION | PISTE DE VÉRIFICATION GLOBALE CORRÉLÉE DANS LE TEMPS

Le système d'information compile les enregistrements de vérification provenant de *[Affectation : composants du système d'information définis par l'organisation]* dans une piste de vérification (logique ou physique) globale qui est corrélée dans le temps, à l'intérieur de *[Affectation : niveau de tolérance défini par l'organisation pour les relations entre les estampilles temporelles des enregistrements individuels de la piste de vérification]*.

Conseils supplémentaires sur l'amélioration : Les pistes de vérification sont corrélées dans le temps lorsque les estampilles temporelles des enregistrements de vérification individuels peuvent être associées de manière fiable aux estampilles temporelles d'autres enregistrements pour permettre un classement chronologique des enregistrements à l'intérieur des limites de tolérance définies par l'organisation. Contrôles connexes : AU-8, AU-12.

(2) GÉNÉRATION D'ENREGISTREMENTS DE VÉRIFICATION | FORMATS NORMALISÉS

Le système d'information produit une piste de vérification (logique ou physique) globale composée d'enregistrements de vérification dans un format normalisé.

Conseils supplémentaires sur l'amélioration : La normalisation de l'information de vérification en un format commun facilite l'interopérabilité et l'échange de l'information entre des dispositifs et des systèmes d'information différents. Elle permet la production d'information sur les événements plus faciles à analyser et à mettre en corrélation. Les formats normalisés d'enregistrements de vérification comprennent les enregistrements des journaux système et les enregistrements de vérification conformes à la norme CEE (CEE pour *Common Event Expression*). Dans le cas des mécanismes de journalisation des systèmes d'information qui ne sont pas conformes aux les formats normalisés, les systèmes peuvent convertir chacun des enregistrements de vérification en un format normalisé au moment de compiler les pistes de vérification globales.

(3) GÉNÉRATION D'ENREGISTREMENTS DE VÉRIFICATION | MODIFICATIONS PAR DES PERSONNES AUTORISÉES

Le système d'information permet à *[Affectation : liste des personnes ou des rôles définie par l'organisation]* de modifier la vérification à effectuer sur *[Affectation : composants de système d'information définis par l'organisation]* en fonction de *[Affectation : critères d'événement sélectionnables définis par l'organisation]* en dedans de *[Affectation : laps de temps défini par l'organisation]*.

Conseils supplémentaires sur l'amélioration : Cette amélioration permet aux organisations d'accroître ou de limiter leurs activités de vérification au besoin pour répondre aux exigences organisationnelles. Il est possible d'accroître les activités de vérification qui sont limitées pour préserver les ressources du système d'information afin de répondre à certaines situations de menace. Les activités de vérification peuvent aussi au contraire être limitées à un ensemble précis d'événements afin de faciliter la réduction des vérifications ainsi que l'analyse et les rapports de vérification. Les organisations peuvent déterminer la durée pendant laquelle les opérations de vérification sont modifiées, par exemple en temps quasi réel, en quelques minutes ou en quelques heures. Contrôle connexe : AU-7

Référence :

Aucune

AU-13 SURVEILLANCE DE LA DIVULGATION D'INFORMATION

Contrôle :

(A) L'organisation surveille *[Affectation : sites d'information ou sites d'information de source ouverte définis par l'organisation] [Affectation : fréquence définie par l'organisation]* pour veiller à ce qu'il n'y ait aucune divulgation non autorisée d'information liée à l'organisation.

Conseils supplémentaires : L'information de source ouverte comprend celle se trouvant sur les sites de réseautage social. Contrôles connexes : PE-3, SC-7.

Améliorations du contrôle :

(1) SURVEILLANCE DE LA DIVULGATION D'INFORMATION | UTILISATION D'OUTILS AUTOMATISÉS

L'organisation a recours à des mécanismes automatisés pour déterminer si de l'information organisationnelle a fait l'objet d'une divulgation non autorisée.

Conseils supplémentaires sur l'amélioration : Des scripts automatisés visant à surveiller les nouveaux messages affichés sur certains sites Web ainsi que des services commerciaux qui envoient des avis et des alertes aux organisations représentent des exemples de mécanismes automatisés.

(2) SURVEILLANCE DE LA DIVULGATION D'INFORMATION | EXAMEN DES SITES SURVEILLÉS

L'organisation examine les sites d'information de source ouverte qui sont surveillés *[Affectation : fréquence définie par l'organisation]*.

Référence :

Aucune

AU-14 VÉRIFICATION DES SESSIONS

Contrôle :

(A) Le système d'information permet aux utilisateurs autorisés de sélectionner une session utilisateur pour saisir, enregistrer, visualiser ou écouter son contenu.

Conseils supplémentaires sur l'amélioration : Les vérifications de session comprennent entre autres la surveillance des frappes et des sites Web consultés de même que l'enregistrement de l'information ou des transferts de dossiers. Les activités de vérification des sessions sont mises au point, intégrées et utilisées après consultation avec des conseillers juridiques, conformément aux lois du GC ainsi qu'aux politiques, aux directives et aux normes applicables du SCT. Contrôles connexes : AC-3, AU-4, AU-5, AU-9, AU-11.

Améliorations du contrôle :

(1) VÉRIFICATION DES SESSIONS | DÉMARRAGE DU SYSTÈME

Le système d'information lance les vérifications de session au démarrage du système.

(2) VÉRIFICATION DES SESSIONS | SAISI OU ENREGISTREMENT ET JOURNALISATION DU CONTENU

Le système d'information permet aux utilisateurs autorisés de saisir ou d'enregistrer et de journaliser tout le contenu d'une session utilisateur.

(3) VÉRIFICATION DES SESSIONS | VISUALISATION OU ÉCOUTE À DISTANCE

Le système d'information permet aux utilisateurs autorisés de visualiser ou d'écouter à distance et en temps réel tout le contenu d'une session utilisateur établie.

Référence :

Aucune

AU-15 CAPACITÉ DE VÉRIFICATION SECONDAIRE

Contrôle :

(A) L'organisation prévoit une capacité de vérification secondaire en vue de parer à l'impossibilité d'avoir recours à la capacité de vérification principale, et d'offrir [*Affectation : autres fonctions de vérification définies par l'organisation*].

Conseils supplémentaires : Une capacité de vérification secondaire n'est, par définition, qu'une protection à court terme à laquelle l'organisation fait appel jusqu'au rétablissement de la capacité de vérification principale. À ce titre, l'organisation peut décider de n'offrir qu'un sous-ensemble de la fonction de vérification principale touchée par cette inexécution. Contrôle connexe : AU-5.

Améliorations du contrôle :

Aucune

Références :

Aucune

AU-16 VÉRIFICATION TRANS-ORGANISATIONNELLE

Contrôle :

(A) L'organisation utilise [*Affectation : méthodes définies par l'organisation*] pour coordonner [*Affectation : information de contrôle définie par l'organisation*] avec d'autres organisations lorsque l'information de contrôle est transmise au-delà des frontières organisationnelles.

Conseils supplémentaires : La capacité de vérification nécessite une approche trans-organisationnelle coordonnée dans la mesure où l'organisation utilise les systèmes d'information et/ou les services d'autres organisations. Par exemple, le maintien de l'identité des utilisateurs qui font appel à des services offerts au-delà des frontières de l'organisation peut s'avérer fort difficile et toute tentative en ce sens risque de donner lieu à des ramifications importantes sur le plan du rendement. C'est pourquoi la vérification trans-organisationnelle (p. ex. le type de capacité de vérification fournie par les architectures axées sur le service) ne capture souvent que l'identité des utilisateurs à l'origine des demandes d'accès au système d'information initial, tandis que les systèmes subséquents enregistrent si ces demandes proviennent de personnes autorisées. Contrôle connexe : AU-6.

Améliorations du contrôle :

(1) VÉRIFICATION TRANS-ORGANISATIONNELLE | PRÉSERVATION DE L'IDENTITÉ

L'organisation exige que l'identité des utilisateurs soit préservée dans des pistes de vérification trans-organisationnelles.

Conseils supplémentaires sur l'amélioration : Cette amélioration du contrôle s'applique dans les cas où il est nécessaire de faire le suivi des actions menées par un utilisateur particulier au-delà des frontières de l'organisation.

(2) VÉRIFICATION TRANS-ORGANISATIONNELLE | ÉCHANGE D'INFORMATION DE VÉRIFICATION

L'organisation fournit de l'information de vérification trans-organisationnelle aux [*Affectation : organisations définies par l'organisation*] en vertu des [*Affectation : accords liés à l'échange trans-organisationnel définis par l'organisation*].

Conseils supplémentaires sur l'amélioration : L'échange d'information de vérification trans-organisationnel peut s'avérer essentiel à l'analyse de la vérification effectuée en raison de l'étalement de l'information de vérification. Par exemple, les enregistrements de vérification appartenant à l'une des organisations peuvent ne pas fournir suffisamment d'information pour déterminer si les utilisateurs d'autres organisations ont employé des ressources informationnelles de façon appropriée ou inappropriée. Dans certains cas, seule l'organisation où travaillent les employés possèdent les connaissances nécessaires pour établir de tels faits, d'où l'importance d'échanger l'information de vérification entre organisations.

Références :

Aucune

3.4 FAMILLE : ÉVALUATION DE SÉCURITÉ ET AUTORISATION

CLASSE : GESTION

CA-1 POLITIQUES ET PROCÉDURES D'ÉVALUATION DE SÉCURITÉ ET D'AUTORISATION

Contrôle :

(A) L'organisation élabore, consigne et diffuse à *[Affectation : liste des employés ou des rôles définie par l'organisation]* :

(a) une politique d'évaluation de sécurité et d'autorisation qui définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et le respect;

(b) des procédures pour faciliter la mise en œuvre de la politique d'évaluation de sécurité et d'autorisation ainsi que des contrôles connexes.

(B) L'organisation examine et met à jour :

(a) la politique d'évaluation de sécurité et d'autorisation *[Affectation : fréquence définie par l'organisation]*;

(b) les procédures d'évaluation de sécurité et d'autorisation *[Affectation : fréquence définie par l'organisation]*.

Conseils supplémentaires : Ce contrôle permet de mettre en place la politique et les procédures nécessaires à la mise en œuvre efficace de certains contrôles de sécurité et de certaines améliorations de la famille CA. La politique et les procédures d'évaluation de sécurité et d'autorisation rendent compte des lois du GC ainsi que des politiques, des directives et des normes applicables du SCT. Les politiques et les procédures du programme de sécurité de l'organisation peuvent rendre facultatives les politiques et les procédures propres au système. La politique peut être intégrée à la politique générale sur la sécurité de l'information de l'organisation ou, inversement, elle peut être représentée par de multiples politiques compte tenu de la nature complexe de certaines organisations. Les procédures peuvent être établies pour le programme de sécurité général et pour des systèmes d'information particuliers, au besoin. La stratégie organisationnelle de gestion des risques est un facteur clé dans l'établissement des politiques et des procédures.

Amélioration du contrôle :

Aucune

Références :

SCT, *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* [Référence 7].
SCT, *Directive sur la gestion de la sécurité ministérielle* [Référence 10].

CA-2 ÉVALUATIONS DE SÉCURITÉ

Contrôle :

(A) L'organisation met en place un plan d'évaluation de sécurité qui définit la portée de l'évaluation, notamment ce qui suit :

(a) les contrôles de sécurité et les améliorations de contrôle faisant l'objet d'une évaluation;

(b) les procédures d'évaluation servent à déterminer l'efficacité des contrôles de sécurité;

(c) l'environnement d'évaluation, l'équipe d'évaluation ainsi que les rôles et les responsabilités liés à l'évaluation.

(B) L'organisation évalue les contrôles de sécurité du système d'information et l'environnement dans lequel il est exploité *[Affectation : fréquence définie par l'organisation]* pour déterminer dans quelle mesure les contrôles ont été mis en œuvre correctement, s'ils fonctionnent comme prévu et s'ils produisent les résultats escomptés tout en respectant les exigences relatives à la sécurité.

(C) L'organisation produit un rapport d'évaluation de sécurité qui consigne les résultats de l'évaluation.

(D) L'organisation remet les résultats de l'évaluation des contrôles de sécurité à *[Affectation : liste des personnes et des rôles définie par l'organisation]*.

Conseils supplémentaires : Les organisations évaluent les contrôles de sécurité des systèmes d'information organisationnels de même que les environnements dans lesquels ces systèmes sont exploités dans le cadre (i) des autorisations de sécurité initiales et continues, (ii) des exigences du SCT relativement aux évaluations périodiques stipulées dans la *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* [Référence 7], (iii) de la surveillance continue et (iv) des activités de cycle de vie de développement de systèmes. Les évaluations de sécurité permettent de : (i) veiller à l'intégration de la sécurité de l'information dans les systèmes d'information de l'organisation, (ii) cerner les faiblesses et les lacunes au début du processus de développement, (iii) fournir l'information essentielle pour prendre des décisions relatives aux risques dans le cadre des processus d'autorisation de sécurité et (iv) veiller au respect des procédures d'atténuation des vulnérabilités. On procède à l'évaluation des contrôles de sécurité mentionnés à l'annexe F (catalogue principal) et à l'annexe G (contrôles de gestion du programme) qui sont en place, comme le stipulent les plans de sécurité des systèmes et du programme de sécurité de l'information. Les organisations peuvent mener d'autres types d'activités d'évaluation, comme l'analyse des vulnérabilités et la surveillance du système, pour maintenir la posture de sécurité des systèmes d'information durant tout leur cycle de vie. Les rapports d'évaluation de sécurité consignent les résultats à un niveau que les organisations jugent suffisamment détaillé pour leur permettre d'en déterminer l'exactitude et l'exhaustivité et d'établir dans quelle mesure les contrôles de sécurité sont mis en œuvre correctement, fonctionnent comme prévu et produisent les résultats escomptés tout en respectant les exigences relatives aux contrôles de sécurité. L'exigence du SCT concernant les évaluations de sécurité régulières ne signifie pas qu'il faut mener d'autres activités d'évaluation en plus de celles mises de l'avant dans les processus d'autorisation de sécurité de l'organisation. Les résultats des évaluations de sécurité sont remis aux personnes qui occupent des fonctions liées aux types d'évaluations menées. Par exemple, les résultats des évaluations qui visent à appuyer les décisions en matière d'autorisation de sécurité sont remises à l'autorité responsable ou au représentant désigné.

Pour répondre au besoin de mener régulièrement des évaluations du SCT, les organisations peuvent se servir des résultats d'évaluation provenant des sources suivantes : (i) des autorisations initiales ou continues du système d'information, (ii) de la surveillance continue ou (iii) des activités de cycle de vie du développement du système. Les organisations s'assurent que les résultats d'évaluation de sécurité sont actuels et pertinents afin de déterminer l'efficacité des contrôles de sécurité et qu'ils sont obtenus conformément au niveau requis d'indépendance de l'évaluateur. On peut réutiliser les résultats d'évaluation d'un contrôle de sécurité dans la mesure où ils demeurent valables et qu'ils peuvent être complétés par d'autres évaluations, au besoin. Après avoir obtenu les autorisations initiales et en conformité avec aux politiques du SCT, les organisations évaluent périodiquement les contrôles de sécurité dans le cadre des activités de surveillance continue. Elles établissent la fréquence des évaluations de contrôle de sécurité permanentes conformément aux stratégies de surveillance continue des organisations. Les vérifications externes (p. ex. celles effectuées par des entités externes, comme les organismes réglementaires) sont hors de la portée de ce contrôle. Contrôles connexes : CA-5, CA-6, CA-7, RA-5, SA-11, SA-12, SI-4.

Améliorations du contrôle :

(1) ÉVALUATIONS DE SÉCURITÉ | ÉVALUATEURS INDÉPENDANTS

L'organisation fait appel à des évaluateurs ou à des équipes d'évaluateurs ayant *[Affectation : niveau d'indépendance défini par l'organisation]* pour mener des évaluations de contrôle de sécurité.

Conseils supplémentaires sur l'amélioration : Les évaluateurs ou les équipes d'évaluateurs indépendants sont des personnes ou des groupes chargés de mener des évaluations impartiales des systèmes d'information organisationnels. L'impartialité sous-entend que les évaluateurs ne doivent en aucun cas se trouver en conflit d'intérêts, subjectif ou réel, en ce qui a trait au développement, aux opérations ou à

la gestion des systèmes d'information organisationnels qui font l'objet d'évaluations ou en ce qui a trait à l'établissement de l'efficacité du contrôle de sécurité. Pour s'assurer de leur impartialité, les évaluateurs ne doivent pas : (i) avoir un intérêt commun ou concurrentiel avec les organisations pour lesquelles ils mènent des évaluations, (ii) évaluer leur propre travail, (iii) être gestionnaires ou employés des organisations pour lesquelles ils mènent les évaluations ou (iv) agir à titre de conseillers pour les organisations qui ont recours à leurs services. Les évaluations indépendantes peuvent être menées par des éléments des organisations ou par des sous-traitants provenant d'entités publiques ou privées extérieures aux organisations concernées. Les autorités responsables déterminent le niveau d'indépendance requis en fonction des catégories de sécurité liées aux systèmes d'information ou au risque ultime associé aux opérations, aux actifs et aux personnes de l'organisation. Elles décident également si le niveau d'indépendance des évaluateurs permet de garantir de façon suffisante que les résultats sont valables et qu'il permet de prendre des décisions crédibles fondées sur les risques, ce qui comprend déterminer si les sous-traitants qui offrent les services d'évaluation de sécurité sont assez indépendants, par exemple lorsque les détenteurs de systèmes d'information ne participent pas directement aux processus contractuels ou qu'ils ne peuvent pas influencer indûment l'objectivité des évaluateurs. Dans des situations spéciales, par exemple lorsque les organisations qui détiennent les systèmes d'information sont de petite taille ou lorsque les structures organisationnelles exigent que les évaluations soient menées par des personnes qui font partie de la chaîne de développement, des opérations ou de gestion des détenteurs des systèmes, on peut s'assurer de l'indépendance des processus d'évaluation en examinant minutieusement les résultats des évaluations et en veillant à ce que des équipes de spécialistes indépendants mènent des analyses pour valider le caractère exhaustif, l'exactitude, l'intégrité et la fiabilité des résultats. Les organisations reconnaissent que les évaluations menées autrement que pour appuyer directement les décisions liées aux autorisations – si elles sont menées par des évaluateurs suffisamment indépendants – risquent d'être davantage utiles pour prendre ce genre de décisions, ce qui permet de réduire le besoin de répéter les évaluations.

(2) ÉVALUATIONS DE SÉCURITÉ | ÉVALUATIONS SPÉCIALISÉES

Les évaluations de contrôle de sécurité organisationnelles comprennent ce qui suit : *[Sélection : (un choix ou plus) : une surveillance approfondie; une analyse des vulnérabilités; des tests liés aux utilisateurs malveillants; une évaluation des menaces internes; des tests de charge et de performance] [Affectation : autres formes d'évaluation de sécurité définies par l'organisation] [Sélection : annoncé; non annoncé] [Affectation : fréquence définie par l'organisation]*.

Conseils supplémentaires sur l'amélioration : Les organisations peuvent surveiller les systèmes d'information, évaluer les menaces internes, mener des tests concernant les utilisateurs malveillants ou tout autre test (p. ex. des vérifications et des validations) pour mieux se préparer en mettant en œuvre des capacités organisationnelles et en indiquant les niveaux de performance actuels afin d'orienter les efforts et d'accroître ainsi la sécurité. Les organisations mènent des activités d'évaluation en conformité avec les directives, les politiques, les règles et les normes qui s'appliquent. Les autorités responsables approuvent les méthodes d'évaluation parallèlement à la stratégie de gestion des risques organisationnels. Les organisations peuvent intégrer les vulnérabilités découvertes durant les évaluations aux processus d'atténuation des vulnérabilités. Contrôles connexes : PE-3, SI-2.

(3) ÉVALUATIONS DE SÉCURITÉ | ORGANISATIONS EXTERNES

L'organisation accepte les résultats d'une évaluation de *[Affectation : système d'information défini par l'organisation]* que mène *[Affectation : organisation externe définie par l'organisation]* lorsque l'évaluation respecte *[Affectation : exigences définies par l'organisation]*.

Conseils supplémentaires sur l'amélioration : Les organisations peuvent souvent s'appuyer sur les évaluations que mènent d'autres organisations (externes) sur certains systèmes d'information. En recourant à ces évaluations (c.-à-d. en réutilisant l'information provenant d'évaluations déjà menées), les organisations diminuent de façon importante le temps et les ressources nécessaires aux activités d'évaluation en limitant le nombre d'activités d'évaluation indépendante qu'elles doivent mener. Les facteurs dont elles peuvent tenir compte pour déterminer si les résultats d'évaluation provenant d'organisations externes sont acceptables peuvent varier. Elles peuvent par exemple tenir compte d'expériences d'évaluation antérieures qu'a vécues une organisation concernant une autre organisation, de la réputation que détiennent les organisations en ce qui a trait aux évaluations, du niveau de détails que fournit la documentation appuyant l'évaluation, ou les

mandats que confèrent les lois du GC ainsi que les politiques, les directives et les normes du SCT aux organisations.

Références :

SCT, *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* [Référence 7].
SCT, *Directive sur la gestion de la sécurité ministérielle* [Référence 10].

CA-3 CONNEXIONS DES SYSTÈMES D'INFORMATION

Contrôle :

(A) L'organisation autorise les connexions du système d'information à d'autres systèmes conformément aux ententes sur la sécurité des interconnexions.

(B) L'organisation consigne, pour chaque interconnexion, les caractéristiques d'interface, les exigences des contrôles de sécurité et la nature de l'information communiquée.

(C) L'organisation examine et met à jour les ententes sur la sécurité des interconnexions *[Affectation : fréquence définie par l'organisation]*.

Conseils supplémentaires : Ce contrôle s'applique aux connexions spécialisées entre les systèmes d'information (interconnexions de systèmes), et non aux connexions temporaires contrôlées par les utilisateurs, comme le courrier électronique et la navigation dans les sites Web. Les organisations étudient minutieusement les risques possibles liés à l'interconnexion de systèmes d'information, tant intérieurs qu'extérieurs, dont les exigences en matière de contrôle de sécurité et les contrôles eux-mêmes diffèrent. Les autorités responsables déterminent les risques associés à chaque connexion de système d'information ainsi que les contrôles qui doivent être en place. Si les systèmes interconnectés ont la même autorité responsable, aucune entente sur la sécurité des interconnexions n'est requise. Les organisations peuvent alors décrire les caractéristiques d'interface entre les systèmes interconnectés dans les plans de sécurité de chaque système. Si les systèmes interconnectés ont une autorité responsable différente, mais qu'elles appartiennent toutes à la même organisation, les organisations peuvent conclure des ententes sur la sécurité des interconnexions ou décrire les caractéristiques d'interface entre les systèmes dans les plans de sécurité de chaque système. Les organisations peuvent aussi ajouter l'information liée à l'entente sur la sécurité des interconnexions à des contrats officiels, surtout lorsque l'interconnexion se fait entre un ministère ou un organisme du GC et un organisme non gouvernemental (du secteur privé). Les risques concernent également les systèmes d'information qui partagent les mêmes réseaux. Dans le cas de certaines technologies (p. ex. des véhicules aériens spatiaux sans pilote ou des dispositifs médicaux), des connexions spécialisées peuvent être en place durant les essais préopérationnels. Ces connexions requièrent des ententes sur la sécurité des interconnexions et peuvent être assujetties à d'autres contrôles de sécurité. Contrôles connexes : AC-3, AC-4, AC 20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4.

Améliorations du contrôle :

(1) INTERCONNEXIONS DES SYSTÈMES | CONNEXIONS DE SYSTÈMES DE SÉCURITÉ NATIONAUX NON CLASSIFIÉS

L'organisation interdit toute connexion directe de *[Affectation : système de sécurité national non classifié défini par l'organisation]* à un réseau externe sans utiliser *[Affectation : dispositif de protection des frontières défini par l'organisation]*.

Conseils supplémentaires sur l'amélioration : Le contrôle de réseaux externes (Internet) échappe habituellement aux organisations. Les communications (flux d'information) entre les systèmes de sécurité nationaux non classifiés et les réseaux externes passent par des dispositifs approuvés de protection des frontières (comme des routeurs ou des coupe-feux). Cette amélioration est nécessaire afin que les organisations puissent traiter, stocker ou transmettre l'information protégée.

(2) INTERCONNEXIONS DES SYSTÈMES | CONNEXIONS DE SYSTÈMES DE SÉCURITÉ NATIONAUX CLASSIFIÉS

L'organisation interdit toute connexion directe d'un système de sécurité national classifié à un réseau externe sans utiliser *[Affectation : dispositif de protection des frontières défini par l'organisation]*.

Conseils supplémentaires sur l'amélioration : Le contrôle de réseaux externes (Internet) échappe habituellement aux organisations. Les communications (flux d'information) entre les systèmes de sécurité nationaux classifiés et les réseaux externes passent par des dispositifs approuvés de protection des frontières (comme des routeurs ou des coupe-feux). De plus, les dispositifs approuvés (habituellement des systèmes interdomaines ou des systèmes d'interface gérés) appliquent des règles de flux d'information entre les systèmes d'information et les réseaux externes.

(3) INTERCONNEXIONS DES SYSTÈMES | CONNEXIONS DE SYSTÈMES DE SÉCURITÉ NON NATIONAUX ET NON CLASSIFIÉS

L'organisation interdit toute connexion directe de *[Affectation : système de sécurité non national et non classifié défini par l'organisation]* à un réseau externe sans utiliser *[Affectation : dispositif de protection des frontières défini par l'organisation]*.

Conseils supplémentaires sur l'amélioration : Le contrôle des réseaux externes (Internet) échappe habituellement aux organisations. Les communications (flux d'information) entre les systèmes de sécurité non nationaux et non classifiés et les réseaux externes passent par des dispositifs approuvés de protection des frontières (comme des routeurs ou des coupe-feux). Cette amélioration est nécessaire afin que les organisations puissent traiter, stocker ou transmettre l'information protégée.

(4) INTERCONNEXIONS DES SYSTÈMES | CONNEXIONS À DES RÉSEAUX PUBLICS

L'organisation interdit toute connexion directe de *[Affectation : système d'information défini par l'organisation]* à un réseau public.

Conseils supplémentaires sur l'amélioration : On entend par *réseau public* tout réseau auquel peut accéder le public, par exemple Internet et les réseaux extranet d'accès public d'une organisation.

(5) INTERCONNEXIONS DES SYSTÈMES | CONNEXIONS RESTREINTES À DES SYSTÈMES EXTERNES

L'organisation applique une politique *[Sélection : tout permettre, interdire par exception; tout interdire, permettre par exception]* afin d'autoriser la connexion de *[Affectation : systèmes d'information définis par l'organisation]* à des systèmes d'information externes.

Conseils supplémentaires sur l'amélioration : Les organisations peuvent restreindre la connectivité d'un système d'information à des domaines externes (p. ex. des sites Web) en appliquant l'une des deux politiques associées à ce type de connectivité : (i) tout permettre, interdire par exception, ce que l'on appelle aussi une *liste noire* (la plus faible des deux politiques); ou (ii) interdire tout, permettre par exception, ce que l'on appelle aussi une *liste blanche* (la plus forte des deux politiques). Dans les deux cas, les organisations déterminent les exceptions qui sont acceptables, au besoin. Contrôle connexe : CM -7.

Références :

CST, ITSG-22, *Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada* [Référence 41].
CST, ITSG-38, *Établissement des zones de sécurité dans un réseau – Considérations en matière de positionnement des services au sein de zones spécifiques* [Référence 43].

CA-4 CERTIFICATION DE SÉCURITÉ

[Annulé : Intégré au contrôle CA-2]

CA-5 PLAN D'ACTION ET JALONS

Contrôle :

(A) L'organisation met en place un plan d'action et des jalons concernant le système d'information afin de consigner les mesures correctives qu'elle envisage de prendre pour corriger les faiblesses ou les lacunes relevées durant l'évaluation des contrôles de sécurité ainsi que pour réduire et éliminer les vulnérabilités du système.

(B) L'organisation met à jour le plan d'action et les jalons *[Affectation : fréquence définie par l'organisation]* en tenant compte des résultats des évaluations de contrôles de sécurité, des analyses concernant les répercussions sur la sécurité et des activités de surveillance continue.

Conseils supplémentaires : Les plans d'action et les jalons représentent des sections clés des plans de sécurité sur les opérations, qui sont des documents essentiels des trousses d'autorisation de sécurité et qui peuvent être assujettis à l'obligation de rendre des comptes de l'organisation et du GC. Contrôles connexes : CA-2, CA-7, CM-4.

Améliorations du contrôle :

(1) PLAN D'ACTION ET JALONS | AUTOMATISATION DU SOUTIEN AUX FINS D'EXACTITUDE ET D'ACTUALITÉ

L'organisation utilise des mécanismes automatisés pour s'assurer que le plan d'action et les jalons du système d'information sont exacts, à jour et facilement accessibles.

Références :

SCT, *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* [Référence 7].
CST, *ITSG-33, Annexe 2 – Activités de gestion des risques liés aux systèmes d'information* [Référence 58].

CA-6 AUTORISATION DE SÉCURITÉ

Contrôle :

(A) L'organisation attribue à un cadre supérieur ou à un gestionnaire le rôle d'autorité responsable du système d'information.

(B) L'organisation s'assure que l'autorité responsable autorise le système d'information aux fins de traitement avant d'en commencer l'exploitation.

(C) L'organisation met à jour l'autorisation de sécurité *[Affectation : fréquence définie par l'organisation].*

Conseils supplémentaires : Les autorisations de sécurité sont des décisions de gestion officielles qu'un cadre supérieur de l'organisation (l'autorité responsable) communique dans un document de décision d'autorisation. Elles visent à autoriser l'exploitation des systèmes d'information et à confirmer que les responsables acceptent explicitement les risques concernant les activités, les biens et les personnes liés à l'organisation ainsi que les autres organisations et le Canada, tant qu'un ensemble convenu de contrôles de sécurité est mis en œuvre. Les autorités responsables supervisent le budget lié aux systèmes d'information ou s'occupent des activités liées à la mission qui sont prises en charge par ces systèmes. Le processus d'autorisation de sécurité est essentiellement une responsabilité gouvernementale, et les autorités responsables doivent donc être des employés du gouvernement. Par ce processus d'autorisation, les autorités responsables doivent rendre des comptes en ce qui a trait aux risques de sécurité associés à l'exploitation des systèmes d'information organisationnels. Ils occupent donc des postes dont le niveau d'autorité correspond à la compréhension et à l'acceptation de tels risques de sécurité. Selon les politiques du SCT, les organisations doivent continuellement effectuer des contrôles d'autorisation des systèmes d'information en mettant en place des programmes de surveillance continue. Ces programmes permettent de répondre aux exigences de réautorisation des systèmes qui doit s'effectuer tous les trois ans; ainsi,

les processus de réautorisation distincts sont inutiles. En recourant à des processus de surveillance continue et exhaustive, les organisations peuvent continuellement mettre à jour l'information clé contenue dans les trousses d'autorisation (c.-à-d. les plans de sécurité, les rapports d'évaluation de la sécurité, ainsi que les plans d'action et les jalons) et ainsi fournir aux autorités responsables et aux détenteurs de systèmes d'information un aperçu de l'état de sécurité de leurs systèmes d'information et de leurs environnements d'exploitation. Pour réduire les coûts administratifs associés aux réautorisations de sécurité, les autorités responsables utilisent autant que possible les résultats du processus de surveillance continue pour prendre les décisions concernant ces réautorisations.
Contrôles connexes : CA-2, CA-7.

Amélioration du contrôle :
Aucune

Références :
SCT, *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* [Référence 7].
SCT, *Directive sur la gestion de la sécurité ministérielle* [Référence 10].

CA-7 SURVEILLANCE CONTINUE

Contrôle :

(A) L'organisation crée une stratégie de surveillance continue et met en place un programme connexe qui comprend l'établissement de *[Affectation : mesures définies par l'organisation]*.

(B) L'organisation crée une stratégie de surveillance continue et met en place un programme connexe qui comprend la mise en place d'activités de surveillance *[Affectation : fréquences définies par l'organisation]* et d'évaluations appuyant ces activités de surveillance *[Affectation : fréquences définies par l'organisation]*.

(C) L'organisation crée une stratégie de surveillance continue et met en œuvre un programme connexe qui comprend des évaluations de contrôle de sécurité permanentes, conformément à sa stratégie de surveillance continue.

(D) L'organisation crée une stratégie de surveillance continue et met en œuvre un programme connexe qui comprend des mesures définies par l'organisation qui visent à surveiller en permanence l'état de la sécurité, conformément à la stratégie de surveillance continue de l'organisation.

(E) L'organisation crée une stratégie de surveillance continue et met en place un programme connexe qui comprend une mise en corrélation et une analyse de l'information sur la sécurité découlant des évaluations et de la surveillance.

(F) L'organisation crée une stratégie de surveillance continue et met en place un programme connexe qui comprend des mesures d'intervention concernant les résultats qui découlent de l'analyse de l'information sur la sécurité.

(G) L'organisation crée une stratégie de surveillance continue et met en place un programme connexe qui comprend le besoin de rendre compte de l'état de sécurité de l'organisation et du système d'information à *[Affectation : liste des employés ou des rôles définie par l'organisation] [Affectation : fréquences définies par l'organisation]*.

Conseils supplémentaires : Les programmes de surveillance continue facilitent la sensibilisation permanente aux menaces, aux vulnérabilités et à la sécurité de l'information, et permettent d'appuyer les décisions que prend l'organisation au sujet de la gestion des risques. Les mots *continu* et *permanent* signifient que les organisations évaluent ou analysent les contrôles de sécurité et l'information liée aux risques de sécurité à une fréquence suffisante pour appuyer les décisions que prennent les organisations concernant les risques de sécurité. Les résultats associés aux programmes de surveillance continue sont à l'origine des mesures d'intervention liées aux risques que mettent en œuvre les organisations. Grâce aux programmes de surveillance continue, les

organisations peuvent aussi maintenir en permanence les autorisations de sécurité des systèmes d'information de même que les contrôles communs dans un environnement d'exploitation très dynamique où les menaces, les vulnérabilités, les technologies et les missions et les besoins opérationnels sont en constante évolution. En pouvant accéder en tout temps à de l'information sur la sécurité dans les rapports ou les tableaux de bord, les responsables des organisations peuvent prendre des décisions sur la gestion des risques de façon efficace et opportune, comme des décisions sur les autorisations de sécurité permanente. L'automatisation permet d'accroître la fréquence des mises à jour des trousses d'autorisation de sécurité, des inventaires de matériel, de logiciels et de micrologiciels, ainsi que d'autres systèmes d'information. Il est possible d'accroître l'efficacité lorsque les résultats de la surveillance continue sont modifiés de sorte à fournir de l'information précise, mesurable, concrète, pertinente et opportune. Les activités de surveillance continue sont adaptées aux catégories de sécurité des systèmes d'information. Contrôles connexes : CA-2, CA-5, CA-6, CM-3, CM-4, RA-5, SA-11, SA-12, SI-2, SI-4.

Améliorations du contrôle :

(1) SURVEILLANCE CONTINUE | ÉVALUATION INDÉPENDANTE

L'organisation fait appel à des évaluateurs ou à des équipes d'évaluateurs ayant *[Affectation : niveau d'indépendance défini par l'organisation]* pour surveiller continuellement les contrôles de sécurité dans le système d'information.

Conseils supplémentaires sur l'amélioration : Les organisations peuvent optimiser la valeur de leurs évaluations de contrôles de sécurité dans le cadre du processus de surveillance continue en exigeant que des évaluateurs ou des équipes d'évaluateurs détenant un niveau d'indépendance suffisant mènent les évaluations en tenant compte des stratégies de surveillance continue. L'indépendance des évaluateurs offre un degré d'impartialité au processus de surveillance. Pour s'assurer de leur impartialité, les évaluateurs ne doivent pas : (i) avoir un intérêt commun ou concurrentiel avec les organisations pour lesquelles ils mènent des évaluations, (ii) évaluer leur propre travail, (iii) être gestionnaires ou employés des organisations pour lesquelles ils mènent l'évaluation ou (iv) agir à titre de conseillers pour les organisations qui ont recours à leurs services.

(2) SURVEILLANCE CONTINUE | TYPES D'ÉVALUATION

[Annulé : Intégré au contrôle CA-2]

(3) SURVEILLANCE CONTINUE | ANALYSES DES TENDANCES

L'organisation utilise des analyses de tendances pour déterminer s'il faut modifier les mises en œuvre de contrôles de sécurité, la fréquence des activités de surveillance continue ou tout autre type d'activités utilisées dans le cadre du processus de surveillance continue, en se basant sur des données empiriques.

Conseils supplémentaires sur l'amélioration : On compte parmi les analyses de tendances l'examen de l'information récente sur les menaces associées aux types d'événements menaçants qui ont eu lieu au sein de l'organisation ou au gouvernement fédéral, des taux de réussite de certains types de cyberattaques, des vulnérabilités émergentes dans les technologies d'information, des techniques d'ingénierie sociale qui ne cessent d'évoluer, des résultats provenant de différentes évaluations de contrôle de sécurité, de l'efficacité des paramètres de configuration et les constatations de l'inspecteur général ou des vérificateurs.

Référence :

SCT, *Directive sur la gestion de la sécurité ministérielle* [Référence 10].

CA-8 TESTS DE PÉNÉTRATION

Contrôle :

(A) L'organisation effectue des tests de pénétration *[Affectation : fréquence définie par l'organisation]* sur *[Affectation : systèmes d'information ou composants de systèmes d'information définis par l'organisation]*.

Conseils supplémentaires : Les tests de pénétration sont des évaluations spécialisées menées sur des systèmes d'information ou sur des composants de système d'information individuels qui visent à détecter des vulnérabilités que pourraient exploiter des adversaires. Ils permettent de valider les vulnérabilités ou de déterminer le degré de résistance des systèmes d'information des organisations contre les activités des adversaires en tenant compte de certaines contraintes (temps, ressources ou compétences). Les organisations effectuent des tests de pénétration afin de reproduire les opérations des adversaires en se lançant elles-mêmes des cyberattaques hostiles, ce qui leur permet d'analyser de façon approfondie leurs lacunes et leurs faiblesses en matière de sécurité. Les organisations peuvent aussi se servir des résultats des analyses de vulnérabilités pour soutenir les activités liées aux tests de pénétration. Ces tests peuvent être effectués sur des composants matériels, logiciels et micrologiciels d'un système d'information et peuvent exercer des contrôles de sécurité à la fois physiques et techniques. Une méthode utilisée dans le cadre de ces tests consiste (i) à mener une analyse prétest basée sur une connaissance détaillée du système cible, (ii) à effectuer une détection prétest des vulnérabilités potentielles basée sur l'analyse prétest et (iii) à réaliser des tests conçus pour déterminer l'exploitabilité des vulnérabilités détectées. Toutes les parties doivent convenir des règles d'engagement avant le début des scénarios de test de pénétration. Il faut établir une corrélation entre ces règles d'engagement et les outils, les techniques ainsi que les procédures dont on prévoit l'utilisation par les adversaires qui lanceront les attaques. Des évaluations organisationnelles des risques permettent de décider du niveau d'indépendance exigé du personnel chargé des tests de pénétration. Contrôle connexe : SA-12.

Améliorations du contrôle :

(1) TESTS DE PÉNÉTRATION | ÉQUIPE OU AGENT INDÉPENDANT CHARGÉ DES TESTS DE PÉNÉTRATION

L'organisation fait appel à une équipe ou à un agent indépendant pour lancer des tests de pénétration sur le système d'information ou sur les composants de système d'information.

Conseils supplémentaires sur l'amélioration : Les équipes ou les agents indépendants chargés des tests de pénétration sont des personnes ou des groupes qui effectuent des tests de pénétration impartiaux sur les systèmes d'information organisationnels. L'impartialité sous-entend que les équipes ou les agents ne doivent en aucun cas se trouver en un conflit d'intérêts, subjectif ou réel, en ce qui a trait au développement, aux opérations ou à la gestion des systèmes d'information organisationnels qui font l'objet des tests de pénétration. Les conseils supplémentaires du contrôle CA-2 (1) fournissent d'autres renseignements sur les évaluations indépendantes qui peuvent s'appliquer aux tests de pénétration. Contrôle connexe : CA-2.

(2) TESTS DE PÉNÉTRATION | EXERCICES EEFECTUÉS PAR L'ÉQUIPE DE TESTEURS

L'organisation a recours à *[Affectation : exercices effectués par l'équipe de testeurs définis par l'organisation]* pour simuler des tentatives de compromission des systèmes d'information organisationnels lancées par des adversaires conformément à *[Affectation : règles d'engagement définies par l'organisation]*.

Conseils supplémentaires sur l'amélioration : Les exercices effectués par l'équipe de testeurs vont au-delà des objectifs liés aux tests de pénétration en permettant d'examiner la posture de sécurité des organisations et leur capacité à mettre en place des contrôles de cyberdéfense efficaces. Les exercices qu'effectue l'équipe de testeurs sont menés de manière à simuler des tentatives lancées par des adversaires qui cherchent à compromettre des fonctions opérationnelles ou liées à la mission de l'organisation afin d'évaluer de façon exhaustive les capacités en matière de sécurité du système d'information et de l'organisation. On compte parmi ces tentatives les attaques axées sur les technologies (interactions avec des composants matériels, logiciels ou micrologiciels et avec des processus opérationnels ou liés à la mission) de même que les attaques axées sur l'ingénierie sociale (interactions à l'aide de courriels, d'appels téléphoniques, d'espionnage par-dessus l'épaule ou de conversations personnelles). Bien que les tests de pénétration se fassent surtout dans des laboratoires, les organisations se servent des exercices qu'effectue l'équipe de testeurs afin de mener des évaluations exhaustives qui reflètent les conditions réelles. Les exercices de l'équipe de testeurs permettent d'améliorer la sensibilisation et la formation en matière de sécurité de même d'évaluer les niveaux d'efficacité de contrôle de sécurité.

Référence :

Aucune

CA-9 CONNEXIONS DES SYSTÈMES D'INFORMATION INTERNES

Contrôle :

(A) L'organisation autorise les connexions internes de *[Affectation : composants de système d'information ou types de composants définis par l'organisation]* au système d'information.

(B) L'organisation consigne, pour chaque connexion interne, les caractéristiques d'interface, les exigences de sécurité et la nature de l'information communiquée.

Conseils supplémentaires : Ce contrôle s'applique aux connexions entre des systèmes d'information organisationnels et leurs composants (distincts) (c.-à-d. des connexions intrasystèmes), notamment les connexions de systèmes à des dispositifs mobiles, à des ordinateurs de bureau ou à des ordinateurs portatifs, à des imprimantes, à des photocopieurs, à des télécopieurs, à des numériseurs, à des capteurs et à des serveurs. Plutôt que d'autoriser chacune des connexions internes, les organisations peuvent autoriser des connexions internes pour un type de composants qui ont des caractéristiques ou des configurations communes, par exemple, toutes les imprimantes et tous les numériseurs et les photocopieurs numériques ayant une capacité de traitement, de stockage et de transmission précise ou tous les téléphones intelligents ayant une configuration de référence précise. Contrôles connexes : AC-3, AC-4, AC-18, AC-19, AU-2, AU-12, CA-7, CM-2, IA-3, SC-7, SI-4.

Améliorations du contrôle :

(1) CONNEXIONS DES SYSTÈMES D'INFORMATION INTERNES | VÉRIFICATIONS DE CONFORMITÉ À LA SÉCURITÉ

Le système d'information vérifie la conformité de ses composants aux exigences de sécurité avant d'établir une connexion interne.

Conseils supplémentaires sur l'amélioration : Les vérifications de conformité aux exigences de sécurité comprennent la vérification de la configuration de référence pertinente. Contrôle connexe : CM -6.

Référence :

Aucune

3.5 FAMILLE : GESTION DES CONFIGURATIONS

CLASSE : OPÉRATIONNELLE

CM-1 POLITIQUE ET PROCÉDURES DE GESTION DES CONFIGURATIONS

Contrôle :

(A) L'organisation élabore, consigne et diffuse à *[Affectation : liste des employés et des rôles définie par l'organisation]*.

(a) une politique de gestion des configurations qui définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et le respect;

(b) des procédures visant à faciliter la mise en place de la politique de gestion de configuration et les contrôles connexes.

(B) L'organisation examine et met à jour :

(a) la politique de gestion des configurations *[Affectation : fréquence définie par l'organisation]*;

(b) des procédures de gestion des configurations *[Affectation : fréquence définie par l'organisation]*.

Conseils supplémentaires : Ce contrôle permet de mettre en place la politique et les procédures nécessaires à la mise en œuvre efficace de certains contrôles de sécurité et de certaines améliorations dans la famille CM. Les politiques et les procédures de gestion des configurations rendent compte des lois du GC de même que des politiques, des directives et des normes du SCT. Les politiques et les procédures du programme de sécurité de l'organisation peuvent rendre facultatives les politiques et procédures propres au système. La politique peut être intégrée à la politique générale sur la sécurité de l'information de l'organisation ou, inversement, elle peut être représentée par de multiples politiques compte tenu de la nature complexe de certaines organisations. Les procédures peuvent être établies pour le programme de sécurité général (ou le programme TI) et pour des systèmes d'information particuliers, au besoin. La stratégie organisationnelle de gestion des risques est un facteur clé dans l'établissement de la politique et des procédures.

Améliorations du contrôle :

Aucune

Référence :

SCT, *Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information* [Référence 7].

CM-2 CONFIGURATION DE RÉFÉRENCE

Contrôle :

(A) L'organisation élabore, consigne et tient à jour une configuration de référence courante du système d'information dans le cadre du contrôle des configurations.

Conseils supplémentaires : Ce contrôle établit les configurations de référence des systèmes d'information et de leurs composants, y compris les communications et les éléments de connectivité des systèmes. Les configurations de référence sont des spécifications des systèmes d'information et des éléments de configuration connexes documentées dont on a convenu et qui font officiellement l'objet d'examens. Les versions, les publications ou les changements à venir concernant les systèmes d'information reposent sur les configurations de référence. Elles fournissent de l'information sur les composants de système d'information (p. ex. les logiciels standards installées sur les postes de travail, les ordinateurs portatifs, les serveurs, les composants réseau ou les dispositifs mobiles; les numéros de versions courantes et l'information liée aux rustines qui sont apportées aux

applications et aux systèmes d'exploitation; et les paramètres de configuration), la topologie du réseau et l'emplacement logique de ces composants dans l'architecture du système. Sa tenue à jour requiert la création de nouvelles bases de référence à mesure que les systèmes d'information organisationnels évoluent. Les configurations de référence des systèmes d'information sont conformes à l'architecture d'entreprise. Contrôles connexes : CM-3, CM-6, CM-8, CM-9, SA-10.

Améliorations du contrôle :

(1) CONFIGURATION DE RÉFÉRENCE | EXAMENS ET MISES À JOUR

L'organisation examine et met à jour la configuration de référence du système d'information :

(a) *[Affectation : fréquence définie par l'organisation]*;

(b) Au besoin, selon *[Affectation : circonstances définies par l'organisation]*;

(c) lors des installations et des mises à niveau des composants du système d'information.

Conseils supplémentaires sur l'amélioration : Contrôle connexe : CM-5.

(2) CONFIGURATION DE RÉFÉRENCE | AUTOMATISATION DU SOUTIEN AUX FINS D'EXACTITUDE ET D'ACTUALITÉ

L'organisation utilise des mécanismes automatisés pour maintenir la configuration de référence du système d'information à jour, complète, exacte et facilement accessible.

Conseils supplémentaires sur l'amélioration : Les outils d'inventaire de logiciels et de matériel, les outils de gestion de configuration et les outils de gestion de réseau sont des exemples de mécanismes d'automatisation qui permettent aux organisations de maintenir l'uniformité des configurations de référence de leurs systèmes d'information. Ils peuvent être déployés ou utilisés comme des contrôles courants sur le système d'information, le système d'exploitation ou les composants de système (p. ex. les postes de travail, les serveurs, les ordinateurs portatifs, les composants réseau ou les dispositifs mobiles). Ils peuvent par exemple servir à faire le suivi des numéros de version des applications et des types de logiciel installés sur les systèmes d'exploitation de même que des niveaux des rustines actuelles. Les organisations qui choisissent de combiner l'inventaire de composants de système d'information et des activités de configuration de référence peuvent répondre à cette amélioration en mettant en place le contrôle CM-8(2). Contrôles connexes : CM-7, RA-5.

(3) CONFIGURATION DE RÉFÉRENCE | CONSERVATION DES CONFIGURATIONS ANTÉRIEURES

L'organisation conserve *[Affectation : versions de configuration de référence antérieures du système d'information définies par l'organisation]* pour permettre le retour à la version précédente.

Conseils supplémentaires sur l'amélioration : Pour permettre le retour à des versions antérieures, on peut par exemple conserver des versions de configuration de référence précédentes de matériel, de logiciels, de micrologiciels de même que de fichiers et de données de configuration.

(4) CONFIGURATION DE RÉFÉRENCE | LOGICIELS NON AUTORISÉS

[Annulé : Intégré au contrôle CM-7]

(5) CONFIGURATION DE RÉFÉRENCE | LOGICIELS AUTORISÉS

[Annulé : Intégré au contrôle CM-7]

(6) CONFIGURATION DE RÉFÉRENCE | ENVIRONNEMENTS DE TESTS ET DE DÉVELOPPEMENT

L'organisation conserve pour les environnements de développement et de tests des systèmes d'information une configuration de référence gérée séparément de la configuration de référence opérationnelle.

Conseils supplémentaires sur l'amélioration : L'établissement de configurations de référence distinctes pour les environnements opérationnels, de développement et de tests contribue à protéger les systèmes d'information contre les événements imprévus liés aux activités de développement et de tests. Les configurations de référence distinctes permettent aux organisations d'adopter la gestion de configuration qui convient le plus à chaque type de configuration. Par exemple, la gestion des configurations pour les

environnements opérationnels est axée sur le besoin de stabilité, tandis que la gestion des configurations pour les environnements de développement et de tests requiert une flexibilité accrue. Les configurations utilisées dans un environnement de tests et dans un environnement opérationnel doivent se ressembler dans la mesure du possible afin que les résultats des tests soient représentatifs des changements que l'on propose d'apporter aux systèmes d'exploitation. Cette amélioration exige d'utiliser des configurations distinctes, mais pas nécessairement à des environnements physiques séparés. Contrôles connexes : CM-4, SC-3, SC-7.

(7) CONFIGURATION DE RÉFÉRENCE | CONFIGURATION DE SYSTÈMES, DE COMPOSANTS OU DE DISPOSITIFS POUR DES SECTEURS À RISQUES ÉLEVÉS

(a) L'organisation remet *[Affectation : systèmes d'information, composants de système ou dispositifs définis par l'organisation]* dotés de *[Affectation : configurations définies par l'organisation]* aux personnes qui se rendent dans des endroits que l'organisation juge très risqués.

(b) L'organisation applique *[Affectation : mesures de protection de sécurité définies par l'organisation]* aux dispositifs lors du retour de ces personnes.

Conseils supplémentaires sur l'amélioration : Lorsque l'on sait que des systèmes d'information, des composants de systèmes ou des dispositifs (comme des ordinateurs portatifs ou des dispositifs mobiles) se retrouveront dans des secteurs à risque élevé, il est possible de mettre en place des contrôles de sécurité supplémentaires pour contrer la menace accrue associée à ces endroits, où aucun des contrôles de sécurité physique normalement utilisés dans les zones contrôlées par l'organisation n'est en place. Par exemple, les politiques et les procédures organisationnelles sur les ordinateurs portatifs utilisés par des employés qui partent en voyage ou en reviennent comprennent ce qui suit : déterminer les endroits à risque qui seront visités, définir les configurations requises pour les dispositifs, veiller à ce que les dispositifs soient configurés correctement avant le voyage et appliquer des mesures de protection propres aux dispositifs après le retour de voyage. Les ordinateurs portatifs spécialement configurés comprennent les ordinateurs dont le disque dur a été nettoyé, qui sont dotés d'un nombre limité d'applications et qui ont fait l'objet d'un renforcement supplémentaire (p. ex. paramètres de configuration plus stricts). Les mesures de protection particulières qui sont appliquées aux dispositifs à leur retour comprennent un examen aux fins de détection d'indices de trafiquage physique, ainsi que le nettoyage et la recréation d'image du lecteur de disque dur. La protection de l'information contenue dans les dispositifs mobiles est traitée dans la famille des contrôles liés à la protection des supports.

Référence :

Aucune

CM-3 CONTRÔLE DES CHANGEMENTS DE CONFIGURATION

Contrôle :

(A) L'organisation détermine les types de changements au système d'information qui sont contrôlés par la configuration.

(B) L'organisation examine les changements proposés au système d'information qui sont contrôlés par la configuration, puis les approuve ou les refuse en tenant compte explicitement des analyses concernant les répercussions sur la sécurité.

(C) L'organisation consigne les décisions liées aux changements de configuration du système d'information.

(D) L'organisation met en place les changements approuvés au système d'information qui sont contrôlés par la configuration.

(E) L'organisation conserve les dossiers sur les changements contrôlés par la configuration du système d'information pendant *[Affectation : période définie par l'organisation]*.

(F) L'organisation vérifie et examine les activités associées aux changements contrôlés par la configuration du système d'information.

(G) L'organisation coordonne et surveille les activités de contrôle des changements de configuration effectuées *par [Affectation : élément de contrôle des changements de configuration défini par l'organisation (p. ex. comité, conseil)]* qui se réunit *[Sélection : (une ou plusieurs) : [Affectation : fréquence définie par l'organisation]; [Affectation : conditions de changement de configuration définies par l'organisation]]*.

Conseils supplémentaires : Les contrôles des changements de configuration des systèmes d'information organisationnels comprennent la proposition systématique, la justification, la mise en œuvre, les tests, l'examen et l'application de changements aux systèmes, y compris leurs mises à niveau et leurs modifications. Les modifications aux configurations de référence des composants et des éléments de configuration des systèmes d'information, les changements aux paramètres de configuration des produits de technologie de l'information (systèmes d'exploitation, applications, coupe-feux, routeurs et dispositifs mobiles), les changements imprévus ou non autorisés et les changements visant à réduire les vulnérabilités sont des exemples de contrôles des changements de configuration. Les processus usuels concernant la gestion des changements de configuration des systèmes d'information comprennent les conseils de gestion des configurations qui sont chargés d'approuver les changements proposés aux systèmes. Pour ce qui est du développement de nouveaux systèmes d'information ou les systèmes qui font l'objet de mises à niveau importantes, les organisations pensent à intégrer des représentants des organisations de développement aux conseils de gestion des configurations. La vérification des changements comprend les activités qui ont eu lieu avant ou qui auront lieu après que les changements soient apportés aux systèmes d'information organisationnels et que les activités de vérification nécessaires appliquent ces changements. Contrôles connexes : CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI-12.

Améliorations du contrôle :

(1) CONTRÔLE DES CHANGEMENTS DE CONFIGURATION | AUTOMATISATION CONCERNANT LA DOCUMENTATION, LES AVIS ET LES INTERDICTIONS DE CHANGEMENTS

L'organisation emploie des mécanismes automatisés dans les cas suivants :

(a) documenter les changements proposés au système d'information;

(b) aviser *[Affectation : autorités d'approbation définies par l'organisation]* des changements proposés au système d'information et des demandes de changement approuvées;

(c) souligner les changements proposés au système d'information qui n'ont pas été approuvés ou qui ont été jugés défavorables avant *[Affectation : période définie par l'organisation]*;

(d) interdire tout changement au système d'information jusqu'à l'obtention des approbations requises;

(e) documenter tous les changements proposés au système d'information;

(f) aviser *[Affectation : liste des employés définie par l'organisation]* des changements au système d'information approuvés.

(2) CONTRÔLE DES CHANGEMENTS DE CONFIGURATION | TESTS, VALIDATION ET DOCUMENTATION DES CHANGEMENTS

L'organisation teste, valide et documente les changements au système d'information avant de les mettre en œuvre dans le système d'exploitation.

Conseils supplémentaires sur l'amélioration : Les changements aux systèmes d'information englobent les modifications aux composants matériels, logiciels ou micrologiciels ainsi qu'aux paramètres de configuration définis dans le contrôle CM-6. Les organisations veillent à ce que les tests n'interfèrent pas avec les opérations du système d'information. Les personnes ou les groupes chargés des tests comprennent les politiques et les procédures de sécurité de l'organisation, les politiques et les procédures liées au système d'information et les risques propres à la santé, à la sécurité et à l'environnement qui sont associés à certaines installations ou à certains processus. Il peut arriver que l'on doive mettre hors ligne des systèmes d'exploitation, ou les reproduire autant que possible, avant de pouvoir effectuer des tests. Si les systèmes d'information doivent être mis hors ligne, il faut que ce soit durant une période d'interruption prévue, dans la mesure du possible. S'il est impossible de mener des tests sur les systèmes d'exploitation,

les organisations doivent utiliser des contrôles de compensation (p. ex. mener des tests sur des copies des systèmes).

(3) CONTRÔLE DES CHANGEMENTS DE CONFIGURATION | MISE EN ŒUVRE AUTOMATISÉE DES CHANGEMENTS

L'organisation utilise des mécanismes automatisés pour apporter des changements au système d'information de référence et les déploie ensuite dans tous les systèmes installés.

(4) CONTRÔLE DES CHANGEMENTS DE CONFIGURATION | REPRÉSENTANT DE LA SÉCURITÉ

L'organisation exige qu'un représentant de la sécurité de l'information soit membre de *[Affectation : élément de contrôle des changements de configuration (p. ex. comité, conseil) défini par l'organisation]*.

Conseils supplémentaires sur l'amélioration : Les agents supérieurs de sécurité de l'information, les agents de sécurité des systèmes d'information et les gestionnaires de la sécurité des systèmes d'information peuvent représenter des exemples de représentants de la sécurité de l'information. Il est important d'avoir parmi le personnel des représentants qui sont dotés d'une expertise en sécurité de l'information, car les changements aux configurations des systèmes d'information peuvent avoir des répercussions imprévues, dont certaines peuvent avoir trait à la sécurité. La détection rapide de ces changements permet d'éviter des conséquences négatives inattendues qui pourraient avoir des conséquences sur l'état de sécurité des systèmes d'information de l'organisation. L'élément de contrôle des changements de configuration de cette amélioration reflète ceux définis par l'organisation dans le contrôle CM-3.

(5) CONTRÔLE DES CHANGEMENTS DE CONFIGURATION | MESURES DE SÉCURITÉ AUTOMATISÉES

Le système d'information met automatiquement en place *[Affectation : mesures de sécurité définies par l'organisation]* lorsque des configurations de référence sont modifiées sans autorisation.

Conseils supplémentaires sur l'amélioration : Les mesures de sécurité comprennent par exemple l'interruption du traitement du système d'information et de certaines fonctions du système ou la publication d'avis ou d'alertes à l'intention du personnel de l'organisation lorsqu'un élément de configuration est modifié sans autorisation.

(6) CONTRÔLE DES CHANGEMENTS DE CONFIGURATION | GESTION DE LA CRYPTOGRAPHIE

L'organisation veille à ce que les mécanismes cryptographiques utilisés pour fournir *[Affectation : mesures de protection définies par l'organisation]* soient intégrés à la gestion des configurations.

Conseils supplémentaires sur l'amélioration : Peu importe les moyens cryptographiques employés (p. ex. clé publiques, clé privées, secrets partagés), les organisations s'assurent que des processus et des procédures sont en place pour gérer efficacement ces moyens. Par exemple, si des dispositifs utilisent des certificats aux fins d'identification et d'authentification, il faut mettre en place un processus pour prendre des mesures concernant l'expiration de ces certificats. Contrôle connexe : SC-13.

Référence :

Aucune

CM-4 ANALYSE CONCERNANT LES RÉPERCUSSIONS SUR LA SÉCURITÉ

Contrôle :

(A) L'organisation analyse les changements au système d'information pour déterminer les répercussions possibles sur la sécurité avant de les mettre en œuvre.

Conseils supplémentaires sur l'amélioration : Le personnel de l'organisation qui détient des responsabilités liées à la sécurité de l'information (p. ex. les administrateurs de systèmes d'information, les agents de sécurité des systèmes d'information, les gestionnaires de sécurité des systèmes d'information et les techniciens en sécurité des systèmes d'information) mènent des analyses concernant les répercussions sur la sécurité. Ces employés

possèdent les compétences et l'expertise technique nécessaires pour analyser les changements aux systèmes d'information et leurs ramifications au plan de la sécurité. Les analyses concernant les répercussions sur la sécurité comptent par exemple l'examen des plans de sécurité afin de comprendre les exigences en matière de contrôle de sécurité et l'examen de la documentation sur la conception du système afin de comprendre l'application du contrôle et la manière dont certains changements peuvent influencer les contrôles. Elles peuvent également comprendre les évaluations des risques visant à bien saisir l'incidence des changements et à déterminer si des contrôles de sécurité supplémentaires sont requis. Les analyses concernant les répercussions sur la sécurité sont adaptées aux catégories de sécurité des systèmes d'information. Contrôles connexes : CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, SA-10, SI-2.

Améliorations du contrôle :

(1) ANALYSE DES RÉPERCUSSIONS SUR LA SÉCURITÉ | ENVIRONNEMENTS DE TESTS DISTINCTS

L'organisation analyse les changements au système d'information dans un environnement de tests distinct avant de les appliquer à un environnement opérationnel dans le but de déceler toute lacune, faiblesse, incompatibilité ou intention malveillante susceptible d'influer sur la sécurité.

Conseils supplémentaires sur l'amélioration : Dans ce contexte, on entend par *environnement de tests distinct* un environnement qui est physiquement ou logiquement isolé et distinct de l'environnement opérationnel. La séparation suffit à faire en sorte que les activités menées dans l'environnement de tests n'influent aucunement sur les activités effectuées dans l'environnement opérationnel, et l'information se trouvant dans l'environnement opérationnel n'est pas transmise à l'environnement de tests par inadvertance. Il est possible de distinguer les environnements de façon physique ou logique. Lorsque les environnements de tests séparés physiquement ne sont pas utilisés, les organisations déterminent la force du mécanisme qui est requise lorsqu'elles appliquent la séparation de façon logique (p. ex. lorsque la séparation se fait par machines virtuelles). Contrôles connexes : SA-11, SC-3, SC-7.

(2) ANALYSE DES RÉPERCUSSIONS SUR LA SÉCURITÉ | VÉRIFICATION DES FONCTIONS DE SÉCURITÉ

L'organisation, après que les changements ont été apportés au système d'information, vérifie les fonctions de sécurité pour s'assurer qu'elles ont été mises en œuvre correctement, qu'elles fonctionnent comme il se doit et qu'elles produisent les résultats souhaités, conformément aux exigences en matière de contrôles de sécurité du système.

Conseils supplémentaires sur l'amélioration : Dans ce contexte, on entend par *mise en œuvre* l'installation du code modifié dans le système d'information opérationnel. Contrôle connexe : SA-11.

Référence :

Aucune

CM-5 RESTRICTIONS D'ACCÈS CONCERNANT LES CHANGEMENTS

Contrôle :

(A) L'organisation définit, documente, approuve et applique les restrictions d'accès logique et physique concernant les changements au système d'information.

Conseils supplémentaires : Les changements aux composants matériels, logiciels ou micrologiciels des systèmes d'information peuvent avoir des effets importants sur la sécurité globale des systèmes. Les organisations permettent donc uniquement aux personnes qualifiées et autorisées d'accéder aux systèmes d'information pour y effectuer des changements, y compris des mises à niveau et des modifications. Les organisations tiennent un registre des accès pour s'assurer que le contrôle des changements de configuration est en place et pour appuyer les interventions après coup dans l'éventualité où les organisations détecteraient un changement non autorisé au système d'information. Les restrictions d'accès concernant les changements comprennent également les bibliothèques de logiciels. Les contrôles d'accès physique et logique (voir les contrôles AC-3 et PE-3), l'automatisation des flux de travail, les bibliothèques de supports, les couches abstraites

(p. ex. les changements apportés aux interfaces de tierces parties plutôt que directement aux systèmes d'information) et les créneaux de changement (p. ex. les changements autorisés seulement à des moments précis, ce qui permet de repérer facilement les changements non autorisés) sont des exemples de restrictions d'accès. Contrôles connexes : AC-3, AC-6, PE-3.

Améliorations du contrôle :

(1) RESTRICTIONS D'ACCÈS ASSOCIÉES AUX CHANGEMENTS | VÉRIFICATION ET APPLICATION DES RESTRICTIONS D'ACCÈS AUTOMATISÉES

Le système d'information applique les restrictions d'accès et facilite la vérification des mesures d'application.

Conseils supplémentaires sur l'amélioration : Contrôles connexes : AU-2, AU-12, AU-6, CM-3 et CM-6.

(2) RESTRICTIONS D'ACCÈS ASSOCIÉES AUX CHANGEMENTS | EXAMEN DES CHANGEMENTS APPORTÉS AU SYSTÈME

L'organisation passe en revue les changements apportés au système d'information *[Affectation : fréquence définie par l'organisation]* et *[Affectation : circonstances définies par l'organisation]* pour déterminer si des changements non autorisés ont été apportés.

Conseils supplémentaires sur l'amélioration : Des indications qui justifient l'examen des changements au système d'information et les circonstances précises qui justifient ce besoin peuvent découler d'activités menées par des organisations durant le processus de changement de configuration. **Contrôles connexes :** AU-6, AU-7, CM-3, CM-5, PE-6, PE-8.

(3) RESTRICTIONS D'ACCÈS ASSOCIÉES AUX CHANGEMENTS | COMPOSANTS SIGNÉS

Le système d'information empêche l'installation de *[Affectation : composants logiciels ou micrologiciels définis par l'organisation]* jusqu'à ce que l'organisation vérifie que le composant a été signé numériquement à l'aide d'un certificat que reconnaît et approuve l'organisation.

Conseils supplémentaires sur l'amélioration : Les mises à niveau des versions de logiciels et de micrologiciels, les rustines, les ensembles de modifications provisoires, les pilotes de périphérique et les mises à niveau de systèmes d'entrée-sortie de base sont des exemples de composants logiciels et micrologiciels impossibles à installer s'ils n'ont pas été signés numériquement à l'aide de certificats reconnus et approuvés. Les organisations peuvent classer les composants logiciels et micrologiciels applicables par type ou élément particulier ou encore selon une combinaison des deux. Les signatures numériques et la vérification de ces signatures par l'organisation est une méthode d'authentification. Contrôles connexes : CM-7, SC-13, SI-7.

(4) RESTRICTIONS D'ACCÈS ASSOCIÉES AUX CHANGEMENTS | DOUBLE AUTORISATION

L'organisation applique le principe d'autorisation double avant d'apporter des changements à *[Affectation : information système et composants du système d'information définis par l'organisation]*.

Conseils supplémentaires sur l'amélioration : Les organisations ont recours au principe d'autorisation double pour veiller à ce qu'aucun changement ne soit apporté à certains composants de système d'information et aux données système à moins que deux personnes qualifiées mettre en œuvre les changements voulus. Ces deux personnes doivent posséder assez de compétences et d'expertise pour déterminer si les changements proposés représentent des applications adéquates des changements approuvés. La double autorisation est également appelée le contrôle par deux personnes. Contrôles connexes : AC-5 et CM-3.

(5) RESTRICTIONS D'ACCÈS ASSOCIÉES AUX CHANGEMENTS | PRIVILÈGES DE PRODUCTION ET D'OPÉRATION LIMITÉS

(a) L'organisation limite les privilèges concernant les changements aux composants de système d'information et aux données système dans un environnement de production et d'opération.

(b) L'organisation examine et réévalue les privilèges *[Affectation : fréquence définie par l'organisation]*.

Conseils supplémentaires sur l'amélioration : Dans bon nombre d'organisations, les systèmes d'information appuient plusieurs fonctions essentielles liées à la mission et aux activités de l'organisation. Il

faut limiter les privilèges liés aux changements à apporter aux composants de système d'information des systèmes d'exploitation, car le fait d'apporter des changements à un composant de système d'information particulier peut avoir de graves conséquences sur les processus liés à la mission et aux activités de l'organisation que prend en charge le système dans lequel se trouvent les composants. Parfois, les développeurs ne connaissent pas les liens complexes de plusieurs à plusieurs qui existent entre les systèmes et les processus liés à la mission et aux activités de l'organisation. Contrôle connexe : AC-2.

(6) RESTRICTIONS D'ACCÈS ASSOCIÉES AUX CHANGEMENTS | PRIVILÈGES DE BIBLIOTHÈQUE LIMITÉS

L'organisation restreint les privilèges de changement concernant les logiciels résidents des bibliothèques de logiciels.

Conseils supplémentaires : Les bibliothèques de logiciels comportent des programmes privilégiés. Contrôle connexe : AC-2.

(7) RESTRICTIONS D'ACCÈS ASSOCIÉES AUX CHANGEMENTS | AUTOMATISATION DE LA MISE EN ŒUVRE DE MESURES DE PROTECTION DE SÉCURITÉ

[Annulé : Intégré au contrôle SI-7]

Référence :

Aucune

CM-6 PARAMÈTRES DE CONFIGURATION

Contrôle :

(A) L'organisation établit et documente les paramètres de configuration pour les produits de technologie de l'information intégrés au système d'information en utilisant *[Affectation : listes de vérification concernant la configuration de sécurité définies par l'organisation]* qui cadrent avec le mode le plus rigoureux sur le plan des exigences opérationnelles.

(B) L'organisation met en œuvre les paramètres de configuration.

(C) L'organisation détermine, documente et approuve tout écart en ce qui a trait aux paramètres de configuration établis pour *[Affectation : composants de système d'information définis par l'organisation]* en tenant compte de *[Affectation : exigences opérationnelles définies par l'organisation]*.

(D) L'organisation surveille et contrôle les changements apportés aux paramètres de configuration conformément à ses politiques et à ses procédures.

Conseils supplémentaires : Les paramètres de configuration représentent l'ensemble des paramètres que l'on peut modifier dans le matériel, les logiciels ou les micrologiciels du système d'information et qui ont une incidence sur la posture de sécurité ou les fonctions du système. Les produits de technologie de l'information pour lesquels il est possible de définir les paramètres de configuration de sécurité comptent les ordinateurs centraux, les serveurs (p. ex. les bases de données, le courrier électronique, l'authentification, le Web, les serveurs mandataires, les dossiers, les noms de domaine), les postes de travail, les périphériques d'entrée et de sortie (comme les numériseurs, les photocopieurs et les imprimantes), les composants réseau (comme les coupe-feux, les routeurs, les passerelles, les commutateurs vocaux et de données, les points d'accès sans fil, les appareils réseau, les capteurs), les systèmes d'exploitation, les intergiciels et les applications. Les paramètres de sécurité ont une incidence sur l'état de sécurité des systèmes d'information, ce qui comprend les paramètres qui visent à satisfaire aux autres exigences liées au contrôle de sécurité. Les paramètres de sécurité comprennent ce qui suit : (1) les paramètres de registre, (ii) les paramètres d'accès aux comptes, aux dossiers et aux répertoires, et (iii) les paramètres liés aux fonctions, aux ports, aux protocoles, aux services et aux connexions à distance. Les organisations établissent les paramètres de configuration à l'échelle de l'organisation puis les paramètres propres aux systèmes d'information. Les paramètres deviennent une partie intégrante de la configuration de référence des systèmes.

Les configurations sécurisées communes (que l'on appelle aussi les listes de vérification concernant la configuration de sécurité, les guides de verrouillage et de renforcement, les guides de sécurité, les guides techniques de mise en œuvre de la sécurité [STIG pour *Security Technical Implementation Guide*]) sont des points de repère reconnus, normalisés et établis qui indiquent les paramètres de configuration sécurisée propres à chaque plateforme ou produit de technologie de l'information et les instructions liées à la configuration de ces composants de système d'information afin de répondre aux exigences opérationnelles. Diverses organisations peuvent développer des configurations sécurisées communes, dont des développeurs de produits de technologie de l'information, des fabricants, des fournisseurs, des consortiums, des universités, des industries, des organismes du gouvernement fédéral et d'autres groupes des secteurs public et privé. Le protocole SCAP (pour *Security Content Automation Protocol*) et les normes qu'il définit (p. ex. la norme CCE [pour *Common Configuration Enumeration*]) offrent une méthode efficace et unique d'identification, de suivi et de contrôle des paramètres de configuration. Contrôles connexes : AC-19, CM-2, CM-3, CM-7, SI-4.

Améliorations du contrôle :

(1) PARAMÈTRES DE CONFIGURATION | GESTION CENTRALISÉE, APPLICATION ET VÉRIFICATION AUTOMATISÉES

L'organisation a recours à des mécanismes d'automatisation pour gérer, appliquer et vérifier les paramètres de configuration de *[Affectation : composants de système d'information définis par l'organisation]*.

Conseils supplémentaires sur l'amélioration : Contrôles connexes : CA-7, CM-4.

(2) PARAMÈTRES DE CONFIGURATION | INTERVENTIONS DANS LES CAS DE CHANGEMENTS NON AUTORISÉS

L'organisation a recours à *[Affectation : mesures de protection de sécurité définies par l'organisation]* pour intervenir lorsque des changements non autorisés sont apportés aux *[Affectation : paramètres de configuration définis par l'organisation]*.

Conseils supplémentaires sur l'amélioration : Les interventions en cas de changement non autorisé des paramètres de configuration comprennent le signalement au personnel désigné par l'organisation, la restauration des paramètres de configuration établis ou, dans des cas extrêmes, l'interruption du traitement du système d'information en cause. Contrôles connexes : IR-4, SI-7.

(3) PARAMÈTRES DE CONFIGURATION | DÉTECTION DE CHANGEMENT NON AUTORISÉ

[Annulé : Intégré au contrôle SI-7]

(4) PARAMÈTRES DE CONFIGURATION | DÉMONSTRATION DE CONFORMITÉ

[Annulé : Intégré au contrôle CM-4]

Références :

CST, ITSG-20, *Sécurité de base recommandée pour Windows Serveur 2003* [Référence 40].
CST, ITSG-23, *Isolement d'un serveur d'entreprise Blackberry dans un environnement Microsoft Exchange* [Référence 42].

CM-7 FONCTIONNALITÉ MINIMALE

Contrôle :

(A) L'organisation configure le système d'information pour qu'il ne fournisse que les capacités essentielles.

(B) L'organisation interdit ou restreint l'utilisation des fonctions, des ports, des protocoles ou des services suivants : *[Affectation : fonctions, ports, protocoles ou services définis par l'organisation]*.

Conseils supplémentaires : Les systèmes d'information peuvent offrir une grande variété de fonctions et de services. Il peut arriver que des fonctions et des services fournis par défaut ne soient pas nécessaires au soutien des activités essentielles (p. ex. missions et fonctions clés) de l'organisation. Il est en outre parfois utile d'offrir

plusieurs services à partir de composants uniques du système d'information. Or, cette façon de faire représente un risque accru comparativement au fait de limiter les services fournis par un seul composant. Dans la mesure du possible, les organisations limitent la fonctionnalité d'un composant de système d'information à une seul fonction par dispositif (p. ex. serveurs de courrier ou serveurs Web, mais non les deux). Les organisations examinent les fonctions et les services que fournissent leurs systèmes d'information ou les composants individuels de ces systèmes pour déterminer ceux qu'elles peuvent éliminer (p. ex. VoIP, messagerie instantanée, auto-exécution, partage de fichiers). Les organisations doivent penser à désactiver les ports physiques et logiques et les protocoles inutilisés ou non requis (p. ex. USB, FTP, protocole Internet, version 6 (IPv6 pour *Internet Protocol Version 6)*, protocole de transfert hypertexte (HTTP pour *Hypertext Transfer Protocol*) des composants des systèmes d'information pour éviter les connexions de dispositifs, les transferts d'information ou la tunnellisation non autorisés. Elles peuvent recourir à des outils d'analyse de réseau, à des systèmes de détection et de prévention d'intrusions et à des mécanismes de protection de point terminal (coupe-feux, systèmes de détection d'intrusions intégré, etc.) pour identifier les fonctions, les ports, les protocoles et les services interdits et en empêcher l'utilisation. Contrôles connexes : AC-6, CM-2, RA-5, SA-5, SC-7.

Améliorations du contrôle :

(1) FONCTIONNALITÉ MINIMALE | EXAMEN PÉRIODIQUE

L'organisation examine le système d'information *[Affectation : fréquence définie par l'organisation]* pour déterminer et supprimer les fonctions, ports, protocoles ou services inutiles ou non sécurisés.

L'organisation désactive *[Affectation : fonctions, ports, protocoles ou services du système d'information jugés inutiles ou non sécurisés définis par l'organisation].*

Conseils supplémentaires sur l'amélioration : L'organisation peut déterminer la sécurité relative de la fonction, du port, du protocole ou du service ou baser sa décision en matière de sécurité sur l'évaluation d'autres entités. Les services Bluetooth, FTP et pair à pair sont des exemples de protocoles dont le degré de sûreté est moindre. Contrôles connexes : AC-18, CM-7, IA-2.

(2) FONCTIONNALITÉ MINIMALE | PRÉVENTION DE L'EXÉCUTION DES PROGRAMMES

Le système d'information empêche l'exécution des programmes conformément à *[Sélection (un choix ou plus) : [Affectation : politiques sur l'utilisation de programmes logiciels et restrictions connexes définies par l'organisation]; règles d'autorisation des modalités d'utilisation d'un programme]*.

Conseils supplémentaires sur l'amélioration : Contrôle connexe : CM-8.

(3) FONCTIONNALITÉ MINIMALE | CONFORMITÉ AUX EXIGENCES D'ENREGISTREMENT

L'organisation assure la conformité à *[Affectation : exigences d'enregistrement définies par l'organisation des fonctions, des ports, des protocoles et des services].*

Conseils supplémentaires sur l'amélioration : Les organisations utilisent le processus d'enregistrement pour gérer, faire le suivi et surveiller les systèmes d'information et les fonctions, les ports, les protocoles et les services mis en œuvre.

(4) FONCTIONNALITÉ MINIMALE | LOGICIELS NON AUTORISÉS ET LISTE NOIRE

(a) L'organisation détermine *[Affectation : programmes logiciels qui ne peuvent pas être exécutés sur le système d'information]*.

(b) L'organisation a recours à une politique tout permettre, interdire par exception pour empêcher l'exécution des programmes logiciels non autorisés sur le système d'information.

(c) L'organisation examine et met à jour la liste des programmes logiciels non autorisés *[Affectation : fréquence définie par l'organisation]*.

Conseils supplémentaires sur l'amélioration : La mise en place d'une liste noire est le processus utilisé pour déterminer les programmes logiciels qui ne peuvent pas être exécutés sur les systèmes d'information de l'organisation. Les organisations peuvent appliquer le contrôle CM-7 (5) à la place de cette amélioration si la création d'une liste blanche (la plus forte des deux politiques) est privilégiée pour empêcher l'exécution de programmes logiciels. Contrôles connexes : CM-6, CM-8.

(5) FONCTIONNALITÉ MINIMALE | LOGICIELS AUTORISÉS ET LISTE BLANCHE

(a) L'organisation détermine *[Affectation : programmes logiciels qui peuvent être exécutés sur le système d'information]*.

(b) L'organisation a recours à une politique tout interdire, permettre par exception pour autoriser l'exécution des programmes logiciels autorisés sur le système d'information.

(c) L'organisation examine et met à jour la liste des programmes logiciels autorisés *[Affectation : fréquence définie par l'organisation]*.

Conseils supplémentaires sur l'amélioration : La mise en place d'une liste blanche est le processus utilisé pour déterminer les programmes logiciels qui peuvent être exécutés sur les systèmes d'information de l'organisation. En plus des listes blanches, les organisations tiennent compte de la vérification de l'intégrité des programmes logiciels qui font partie des listes blanches en utilisant par exemple des totaux de contrôle cryptographiques, des signatures numériques ou des fonctions de hachage. La vérification des logiciels qui font partie de listes blanches peut s'effectuer avant l'exécution du système ou au démarrage du système. Contrôles connexes : CM-2, CM-6, CM-8, SA-10, SC-34, SI-7

Référence :

Aucune

CM-8 INVENTAIRE DES COMPOSANTS DE SYSTÈME D'INFORMATION

Contrôle :

(A) L'organisation élabore et tient un inventaire des composants de système d'information qui illustre exactement le système d'information actuel.

(B) L'organisation élabore et tient un inventaire des composants de système d'information qui contient tous les composants se trouvant à l'intérieure de la limite d'autorisation du système d'information.

(C) L'organisation élabore et tient un inventaire des composants de système d'information qui est au niveau de granularité jugé nécessaire aux fins de suivi et de production de rapports.

(D) L'organisation élabore et tient un inventaire des composants de système d'information qui comprend [*Affectation : information définie par l'organisation et jugée nécessaire à la comptabilisation efficace des composants de système d'information*].

(E) L'organisation examine et met à jour l'inventaire des composants de système d'information *[Affectation : fréquence définie par l'organisation]*.

Conseils supplémentaires : Les organisations peuvent choisir de mettre en place des inventaires de composants de système d'information centralisés qui contiennent les composants de tous les systèmes d'information organisationnels. Le cas échéant, les organisations s'assurent que ces inventaires comportent l'information propre au système qui est nécessaire à la comptabilisation des composants (p. ex. les associations du système d'information, le propriétaire du système d'information). L'information jugée nécessaire à la comptabilisation efficace des composants de système d'information comprend les spécifications de l'inventaire du matériel, l'information sur la licence d'utilisation d'un logiciel, les numéros de versions des logiciels, les propriétaires de composants et, dans le cas des dispositifs ou des composants réseau, les noms des machines et les adresses réseau. Le fabricant, le type de dispositif, le modèle, le numéro de série et l'emplacement physique sont des exemples de spécifications de l'inventaire. Contrôles connexes : CM-2, CM-6.

Améliorations du contrôle :

(1) INVENTAIRE DES COMPOSANTS DE SYSTÈME D'INFORMATION | MISES À JOUR DURANT LES INSTALLATIONS ET LES RETRAITS

L'organisation met à jour l'inventaire des composants de système d'information lorsqu'elle installe ou retire des composants et met à jour le système d'information.

(2) INVENTAIRE DES COMPOSANTS DE SYSTÈME D'INFORMATION | AUTOMATISATION DE LA MAINTENANCE

L'organisation utilise des mécanismes automatisés pour faciliter la tenue d'un inventaire des composants du système d'information qui soit à jour, complet, exact et facilement accessible.

Conseils supplémentaires sur l'amélioration : Dans la mesure du possible, les organisations tiennent à jour les inventaires des systèmes d'information. Il peut par exemple être difficile de surveiller les machines virtuelles, car elles sont invisibles dans le réseau lorsqu'elles ne sont pas utilisées. Dans ces situations, les organisations tiennent le plus possible l'inventaire raisonnablement à jour, complet et exact. Il est possible de satisfaire à cette amélioration en mettant en œuvre le contrôle CM-2 (2) pour les organisations qui choisissent de combiner l'inventaire des composants de système d'information et les activités de configuration de référence. Contrôle connexe : SI-7.

(3) INVENTAIRE DES COMPOSANTS DE SYSTÈME D'INFORMATION | DÉTECTION AUTOMATISÉE DE COMPOSANTS NON AUTORISÉS

(a) L'organisation utilise des mécanismes *automatisés [Affectation : fréquence définie par l'organisation]* pour détecter la présence de composants matériels, logiciels et micrologiciels non autorisés dans le système d'information.

(b) L'organisation prend les mesures suivantes lorsqu'elle détecte des composants non autorisés : *[Sélection (un choix ou plus) : désactiver l'accès réseau de ces composants; isoler les composants; aviser [Affectation : liste des employés ou des rôles définie par l'organisation]].*

Conseils supplémentaires sur l'amélioration : On applique cette amélioration en plus de surveiller les connexions à distance et les dispositifs mobiles non autorisés. La surveillance des composants système non autorisés peut être effectuée de façon continue ou lors d'analyses périodiques des systèmes menées à cette fin. Des mécanismes automatisés peuvent être mis en place dans les systèmes d'information ou dans d'autres dispositifs distincts. On peut isoler les composants de système d'information non autorisés en les plaçant dans des domaines ou des sous-réseaux séparés ou en les mettant en quarantaine. On appelle souvent ce type d'isolation le principe du bac à sable. Contrôles connexes : AC-17, AC-18, AC-19, CA-7, SI-3, SI-4, SI-7, RA-5.

(4) INVENTAIRE DES COMPOSANTS DE SYSTÈME D'INFORMATION | INFORMATION SUR LA COMPTABILISATION

L'organisation inclut dans l'information liée à l'inventaire de composants de système d'information une façon d'identifier par *[Sélection (un choix ou plus) : nom; poste; rôle]* les personnes responsables de l'administration de ces composants.

Conseils supplémentaires sur l'amélioration : L'identification des personnes responsables de l'administration des composants de système d'information permet de faire en sorte que les composants concernés sont bien administrés et que les organisations peuvent communiquer avec les personnes désignées si des mesures doivent être prises (p. ex. si l'on détermine qu'un composant de système d'information est source de manquement ou de compromission, ce composant doit être rappelé ou remplacé, ou encore relocalisé).

(5) INVENTAIRE DES COMPOSANTS DE SYSTÈME D'INFORMATION | AUCUNE COMPTABILISATION EN DOUBLE DES COMPOSANTS

L'organisation s'assure que tous les composants respectant la limite d'autorisation du système d'information ne sont pas reproduits dans d'autres inventaires de composants de système d'information.

Conseils supplémentaires sur l'amélioration : Cette amélioration vise à régler le problème potentiel de la double comptabilisation des composants de système d'information dans des systèmes interconnectés importants ou complexes.

(6) INVENTAIRE DES COMPOSANTS DE SYSTÈME D'INFORMATION | CONFIGURATIONS ÉVALUÉES ET ÉCARTS APPROUVÉS

L'organisation inclut dans l'inventaire des composants du système d'information les configurations de composants évaluées et les écarts approuvés en ce qui a trait aux configurations déjà déployées.

Conseils supplémentaires sur l'amélioration : Cette amélioration est axée sur les paramètres de configuration qu'ont établis les organisations concernant les composants de système d'information, sur les composants précis qui ont été évalués afin de vérifier leur conformité aux paramètres de configuration requis et sur tous les écarts approuvés des paramètres de configuration établis. Contrôles connexes : CM-2, CM-6.

(7) INVENTAIRE DES COMPOSANTS DE SYSTÈME D'INFORMATION | DÉPÔT CENTRALISÉ

L'organisation fournit un dépôt centralisé contenant l'inventaire des composants de système d'information.

Conseils supplémentaires sur l'amélioration : Les organisations peuvent choisir de mettre en place des inventaires de composants de système d'information centralisés qui comportent les composants de tous les systèmes d'information organisationnels. Les dépôts centralisés des inventaires de composants de système d'information permettent d'améliorer l'efficience de la comptabilisation des biens matériels, logiciels et micrologiciels. Grâce à ces dépôts, les organisations peuvent rapidement trouver l'emplacement des composants de système ayant fait l'objet d'une compromission ou d'une intrusion ou pour lesquels il faut prendre des mesures d'atténuation, de même que déterminer les personnes qui sont responsables de ces composants. Les organisations s'assurent que ces inventaires centralisés comportent l'information propre au système qui est nécessaire à la comptabilisation des composants (p. ex. les associations du système d'information, le propriétaire du système d'information).

(8) INVENTAIRE DES COMPOSANTS DE SYSTÈME D'INFORMATION | LOCALISATION AUTOMATISÉE

L'organisation utilise des mécanismes automatisés pour géolocaliser les composants de système d'information.

Conseils supplémentaires sur l'amélioration : L'utilisation de mécanismes automatisés pour géolocaliser les composants de système d'information permet d'améliorer la précision des inventaires de composants. Grâce à cette capacité, les organisations peuvent rapidement trouver l'emplacement des composants de système ayant fait l'objet d'une compromission ou d'une intrusion ou pour lesquels il faut prendre des mesures d'atténuation, de même que déterminer les personnes qui sont responsables de ces composants.

(9) INVENTAIRE DES COMPOSANTS DE SYSTÈME D'INFORMATION | ATTRIBUTION DE COMPOSANTS À DES SYSTÈMES

(a) L'organisation attribue *[Affectation : composants de système d'information définis par l'organisation]* à un système d'information.

(b) L'organisation reçoit un avis concernant cette attribution de la part du propriétaire du système d'information.

Conseils supplémentaires sur l'amélioration : Les organisations déterminent les critères concernant les composants ou les types de composants de système d'information (p. ex. les microprocesseurs, les cartes mères, les logiciels, les contrôleurs programmables et les dispositifs réseau) qui sont concernés par cette amélioration. Contrôle connexe : SA-4.

Référence :

Aucune

CM-9 PLAN DE GESTION DES CONFIGURATIONS

Contrôle :

(A) L'organisation élabore, documente et met en œuvre pour le système d'information un plan de gestion des configurations qui traite des rôles et des responsabilités de même que des processus et des procédures liés à la gestion des configurations.

(B) L'organisation élabore, documente et met en œuvre pour le système d'information un plan de gestion des configurations qui établit un processus visant à définir les éléments de configuration durant le cycle de vie du développement du système ainsi qu'à gérer leur configuration.

(C) L'organisation élabore, documente et met en œuvre pour le système d'information un plan de gestion des configurations qui définit les éléments de configuration et les intègre à la gestion des configurations.

(D) L'organisation élabore, documente et met en œuvre un plan de gestion des configurations pour le système d'information aux fins de protection contre toute divulgation et modification non autorisée.

Conseils supplémentaires : Les plans de gestion des configurations répondent aux exigences des politiques de gestion des configurations tout en étant adaptés aux systèmes d'information individuels. Ils définissent en détail les processus et les procédures d'utilisation de la gestion des configurations qui servent à appuyer les activités du cycle de vie du développement du système au niveau du système d'information même. Les plans de gestion des configurations sont habituellement élaborés durant la phase de développement ou d'acquisition du cycle de vie de développement du système. Les plans décrivent comment apporter un changement à l'aide des processus de gestion des changements, comment mettre à jour les paramètres de configuration et les configurations de référence, comment tenir des inventaires des composants de système d'information, comment contrôler les environnements de développement, de tests et d'opérations et, enfin, comment élaborer, diffuser et mettre à jour les documents clés. Les organisations peuvent utiliser des modèles pour veiller à l'élaboration et à la mise en œuvre uniformes et rapides des plans de gestion des configurations. Ces modèles peuvent être un plan de gestion des configurations général pour l'ensemble de l'organisation; les sous-ensembles du plan peuvent être appliqués à un système, en fonction du système visé. Les processus d'approbation de la gestion des configurations comprennent la nomination d'intervenants de gestion clés chargés d'examiner et d'approuver les changements proposés aux systèmes d'information et du personnel chargé d'analyser les incidences sur la sécurité avant d'apporter les changements aux systèmes. Les éléments de configuration sont des éléments du système d'information (matériel, logiciels, micrologiciels et documentation) dont la configuration doit être gérée. Durant les cycles de vie de développement des systèmes d'information, de nouveaux éléments de configuration peuvent être signalés et certains éléments de configuration peuvent ne plus être nécessaires dans le cadre du contrôle des configurations. Contrôles connexes : CM-2, CM-3, CM-4, CM-5, CM-8, SA-10.

Améliorations du contrôle :

(1) PLAN DE GESTION DES CONFIGURATIONS | ATTRIBUTION DES RESPONSABILITÉS

L'organisation confie la responsabilité de développer le processus de gestion des configurations à des employés de l'organisation qui ne participent pas directement au développement du système d'information.

Conseils supplémentaires sur l'amélioration : En l'absence d'équipe de gestion des configurations spécialisée au sein des organisations, les développeurs de systèmes peuvent se voir assigner l'élaboration des processus de gestion de la configuration et devoir faire appel à des employés qui ne participent pas directement au développement ou à l'intégration du système. Cette séparation des tâches permet de veiller à ce que les organisations établissent et maintiennent un degré suffisant d'indépendance entre les processus de développement et d'intégration du système d'information et les processus de gestion des configurations afin de faciliter le contrôle de la qualité et d'améliorer l'efficacité de la surveillance.

Référence :

Aucune

CM-10 RESTRICTIONS RELATIVES À L'UTILISATION DES LOGICIELS

Contrôle :

(A) L'organisation utilise des logiciels et la documentation connexe conformément aux ententes contractuelles et aux lois sur le droit d'auteur.

(B) L'organisation fait le suivi de l'utilisation des logiciels et de la documentation connexe qui sont protégés par des licences limitant la copie et la diffusion du produit.

(C) L'organisation contrôle et documente l'utilisation de la technologie de partage de fichiers pair à pair pour s'assurer qu'elle n'est pas utilisée à des fins non autorisées de distribution, d'affichage, d'exécution ou de reproduction d'œuvres protégées par le droit d'auteur.

Conseils supplémentaires : Le suivi des licences d'utilisation de logiciel peut s'effectuer de façon manuelle (p. ex. à l'aide de simples tableaux) ou automatique (p. ex. à l'aide d'applications de suivi spécialisées), selon les besoin de l'organisation. Contrôles connexes : AC-17, CM-8, SC-7.

Améliorations du contrôle :

(1) RESTRICTIONS RELATIVES À L'UTILISATION DES LOGICIELS | LOGICIELS DE SOURCE OUVERTE

L'organisation applique les restrictions suivantes concernant l'utilisation de logiciels de source ouverte : *[Affectation : restrictions définies par l'organisation].*

Conseils supplémentaires sur l'amélioration : On entend par *logiciels de source ouverte* les logiciels offerts sous forme de code source. Certains droits d'utilisation de logiciels normalement réservés aux détenteurs de droits d'auteur sont habituellement accordés conformément à des contrats de licence et autorisent des personnes à étudier, modifier ou améliorer le logiciel. Au chapitre de la sécurité, l'avantage principal des logiciels de source ouverte est le fait qu'ils offrent aux organisations la possibilité d'étudier le code source. Il existe toutefois divers enjeux liés aux licences de logiciels de source ouverte, comme les contraintes associées à l'utilisation dérivée de ces logiciels.

Référence :

CST, ITSB-95, *Utilisation d'une liste blanche des applications - Conseils à l'intention du gouvernement du Canada.* [Référence 65].
CST, ITSB-89 Version 3, *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information du gouvernement du Canada* [Référence 66].

CM-11 LOGICIELS INSTALLÉS PAR L'UTILISATEUR

Contrôle :

(A) L'organisation établit *[Affectation : politiques définies par l'organisation]* qui régissent l'installation de logiciels par des utilisateurs.

(B) L'organisation applique des politiques d'installation de logiciels au moyen de *[Affectation : politiques définies par l'organisation]*.

(C) L'organisation s'assure du respect des politiques *[Affectation : fréquence définie par l'organisation].*

Conseils supplémentaires : Si on leur accorde les privilèges nécessaires, les utilisateurs peuvent installer des logiciels sur les systèmes d'information de l'organisation. Pour garder le contrôle sur les types de logiciels installés, les organisations déterminent des actions autorisées et interdites en ce qui a trait à l'installation de logiciels. Les mises à jour et les rustines de sécurité aux logiciels installés et aux applications téléchargés se trouvant dans les boutiques d'applications approuvées par les organisations sont des exemples d'installations autorisées. Les installations non autorisés comprennent les logiciels dont la provenance est inconnue ou suspecte, ou les logiciels qui sont potentiellement malveillantes d'après les organisations. Les politiques que choisissent les organisations pour régir les logiciels installés par des utilisateurs peuvent être élaborés par les organisations ou fournis par des entités externes. Les méthodes procédurales (p. ex. examens périodiques des comptes utilisateur), les méthodes automatisées (p. ex. les paramètres de configuration mis en œuvre sur les systèmes d'information de l'organisation) ou les deux types de méthodes sont des exemples de méthodes d'application des politiques. Contrôles connexes : AC-3, CM-2, CM-3, CM-5, CM-6, CM-7, PL-4.

Améliorations du contrôle :

(1) LOGICIELS INSTALLÉS PAR L'UTILISATEUR | AVERTISSEMENTS EN CAS D'INSTALLATIONS NON AUTORISÉES

Le système d'information avertit *[Affectation : liste des employés et des rôles définie par l'organisation]* lorsqu'il détecte des installations de logiciels non autorisées.

Conseils supplémentaires sur l'amélioration : Contrôles connexes : CA-7, SI-4.

(2) LOGICIELS INSTALLÉS PAR L'UTILISATEUR | INSTALLATION INTERDITE SANS STATUT PRIVILÉGIÉ

Le système d'information interdit toute installation de logiciel par des utilisateurs qui n'ont pas de statut privilégié explicite.

Conseils supplémentaires sur l'amélioration : Il est possible d'obtenir un statut privilégié en assumant par exemple des fonctions d'administrateur système. Contrôle connexe : AC-6.

Référence :

Aucune

3.6 FAMILLE : PLANIFICATION D'URGENCE (PLANIFICATION DE LA CONTINUITÉ)

CLASSE : OPÉRATIONNELLE

CP-1 POLITIQUE ET PROCÉDURES DE PLANIFICATION D'URGENCE

Contrôle :

(A) L'organisation élabore et consigne, ainsi que diffuse aux [*Affectation : personnel ou rôles définis par l'organisation*] :

(a) une politique planification d'urgence qui définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et le respect;

(b) des procédures pour faciliter la mise en œuvre de la politique de planification d'urgence et des contrôles de planification d'urgence connexes.

(B) L'organisation examine et met à jour :

(a) la politique de planification d'urgence actuelle tous les [*Affectation : fréquence définie par l'organisation*];

(b) les procédures de planification d'urgence actuelles tous les [*Affectation : fréquence définie par l'organisation*].

(AA) L'organisation développe un cycle de vérification du programme de planification d'urgence à titre de base des rapports réguliers au SCT.

Conseils supplémentaires : Ce contrôle permet de créer la politique et les procédures nécessaires à la mise en œuvre efficace de divers contrôles de sécurité et de diverses améliorations des contrôles pour la famille de planification d'urgence. La politique et les procédures de planification d'urgence sont conformes aux lois du GC et aux politiques, directives et normes du SCT. Les politiques et procédures organisationnelles existantes peuvent rendre inutiles les politiques et procédures supplémentaires. La politique de planification d'urgence peut être intégrée à la politique générale de sécurité de l'information de l'organisation. Les procédures de planification d'urgence peuvent être développées pour le programme de sécurité général et pour un système d'information particulier, le cas échéant. La stratégie organisationnelle de gestion du risque est un élément clé du développement de la politique de planification d'urgence.

Améliorations du contrôle :

Aucune

Références :

SCT, Norme opérationnelle de sécurité - Programme de planification de la continuité des activités (PCA) [Référence 11].
SCT, Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information [Référence 7].
CST, ITSD-03A, Directive sur le contrôle du matériel COMSEC au sein du gouvernement du Canada [Référence 36].

CP-2 PLAN D'URGENCE

Contrôle :

(A) L'organisme élabore, pour le système d'information, un plan d'urgence qui :

(a) identifie les fonctions opérationnelles et de mission essentielles et les exigences connexes en matière d'urgence;

(b) définit les objectifs de reprise, les priorités de restauration et les paramètres;

(c) établit les rôles et responsabilités liés aux urgences ainsi que les personnes assignées à ces fonctions, y compris leurs coordonnées;

(d) traite du besoin de maintenir les fonctions opérationnelles et de mission essentielles en dépit de toute perturbation, compromission ou défaillance du système d'information;

(e) traite de la restauration complète du système d'information sans détérioration des mesures de protection de la sécurité initialement prévues et mises en œuvre;

(f) est examiné et approuvé par [*Affectation : employés ou rôles définis par l'organisation*].

(B) L'organisation distribue des exemplaires du plan d'urgence à [*Affectation : liste (par nom ou rôle) définie par l'organisation des principaux responsables des mesures d'urgence et des éléments organisationnels*].

(C) L'organisation coordonne les activités de planification d'urgence avec les activités de traitement des incidents.

(D) L'organisation examine le plan d'urgence pour le système d'information [*Affectation : fréquence définie par l'organisation*].

(E) L'organisation met à jour le plan d'urgence pour tenir compte des changements apportés à l'organisation, au système d'information ou à l'environnement d'exploitation et des problèmes survenus lors de la mise en œuvre, de l'exécution ou des tests du plan.

(F) L'organisation communique les changements apportés au plan d'urgence à [*Affectation : liste (par nom ou rôle) définie par l'organisation des principaux responsables des mesures d'urgence et des éléments organisationnels*].

(G) L'organisation protège le plan d'urgence contre toute divulgation ou modification non autorisée.

Conseils supplémentaires : La planification d'urgence pour les systèmes d'information fait partie du programme global de l'organisation sur la continuité des activités liées à la mission ou aux fonctions opérationnelles. En cas de compromission des systèmes, la planification d'urgence tient compte de la restauration des systèmes d'information et de la mise en œuvre de processus de secours liés à la mission et aux opérations. L'efficacité de la planification d'urgence est optimisée lorsqu'elle est tenue en compte au cours de toutes les étapes du cycle de vie de développement des systèmes. Afin d'atteindre efficacement l'objectif de résilience des systèmes informatiques, il faut exécuter la planification d'urgence pour le développement de matériel, de logiciels et de micrologiciels. Les plans d'urgence correspondent à l'effort requis pour la restauration des systèmes d'information organisationnels puisque ceux-ci ne doivent pas tous être nécessairement complètement restaurés pour pouvoir assurer le niveau de continuité des opérations requis. Les objectifs de récupération des systèmes d'information tiennent compte des lois applicables du GC ainsi que des politiques, des directives et des normes du SCT. En plus des événements qui menacent la disponibilité des systèmes d'information, le plan d'urgence aborde également les autres événements de sécurité susceptibles de réduire l'efficacité de la mission ou des opérations dont notamment les attaques malveillantes qui compromettent la confidentialité ou l'intégrité des systèmes d'information. Les actions prévues dans les plans d'urgence incluent la dégradation progressive et ordonnée, la mise hors tension des systèmes d'information, le passage en mode manuel, l'utilisation de flux

d'information de secours et le fonctionnement en modes réservés aux situations d'attaque contre les systèmes. En coordonnant étroitement la planification d'urgence et les activités de traitement des incidents, les organisations peuvent veiller à ce que les activités nécessaires de planification d'urgence soient en place et mises en œuvre en cas d'incident de sécurité. Contrôles connexes : AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5.

Améliorations du contrôle :

(1) PLAN D'URGENCE | COORDINATION AVEC LES PLANS CONNEXES

L'organisation coordonne le développement du plan d'urgence avec les éléments organisationnels responsables des plans connexes.

Conseils supplémentaires sur l'amélioration : Les plans connexes aux plans d'urgence pour les systèmes d'information organisationnels comprennent les suivants : plans de continuité des activités, plans de reprise après sinistre, plans de continuité des opérations, plans des communications en temps de crise, plans de l'infrastructure essentielle, plans d'intervention en cas de cyberincident, plans de mise en œuvre en cas de menace interne et plans de mesures d'urgence pour les occupants.

(2) PLAN D'URGENCE | PLANIFICATION DE LA CAPACITÉ

L'organisation planifie la capacité de manière à disposer des ressources nécessaires pour traiter l'information, utiliser les télécommunications et prendre en charge l'environnement durant les opérations d'urgence.

Conseils supplémentaires sur l'amélioration : Une planification de la capacité est requise puisque différents types de menaces (p. ex. désastres naturels, cyberattaques ciblées, etc.) peuvent nuire à la capacité de traitement, à l'utilisation des télécommunications et aux services de soutien prévus à l'appui des fonctions opérationnelles et de la mission de l'organisation. Les organisations doivent prévoir une dégradation des opérations durant la mise en œuvre d'opérations d'urgence et doivent tenir compte de cette dégradation lors de la planification de la capacité.

(3) PLAN D'URGENCE | REPRISE DES FONCTIONS OPÉRATIONNELLES ET DE MISSION ESSENTIELLES

L'organisation planifie la reprise des fonctions opérationnelles et de mission essentielles dans un délai de [*Affectation : durée définie par l'organisation*] suivant l'activation du plan d'urgence.

Conseils supplémentaires sur l'amélioration : Les organisations peuvent choisir de mettre en œuvre les activités de planification d'urgence suggérées dans la présente amélioration du contrôle dans le cadre de la planification de la continuité des activités organisationnelles, dont entre autres dans le cadre des analyses de l'incidence sur les activités. Le délai de reprise des fonctions opérationnelles et de mission essentielles dépend de la gravité et de la portée des perturbations aux systèmes d'information et à l'infrastructure d'appui. Contrôle connexe : PE-12.

(4) PLAN D'URGENCE | REPRISE DE TOUTES LES FONCTIONS OPÉRATIONNELLES ET DE MISSION

L'organisation planifie la reprise de toutes les fonctions opérationnelles et de mission dans un délai de [*Affectation : durée définie par l'organisation*] suivant l'activation du plan d'urgence.

Conseils supplémentaires sur l'amélioration : Les organisations peuvent choisir de mettre en œuvre les activités de planification d'urgence suggérées dans la présente amélioration des contrôles dans le cadre de la planification de la continuité des activités organisationnelles, dont entre autres dans le cadre des analyses de l'incidence sur les activités. Le délai de reprise de toutes les fonctions opérationnelles et de mission dépend de la gravité et de la portée des perturbations aux systèmes d'information et à l'infrastructure d'appui. Contrôle connexe : PE-12.

(5) PLAN D'URGENCE | MAINTIEN DES FONCTIONS OPÉRATIONNELLES ET DE MISSION ESSENTIELLES

L'organisation planifie le maintien des fonctions opérationnelles et de mission essentielles avec peu ou pas de perte sur le plan de la continuité des activités et elle maintient cet état jusqu'à la restauration complète des systèmes d'information dans les sites principaux de traitement ou de stockage.

Conseils supplémentaires sur l'amélioration : Les organisations peuvent choisir de mettre en œuvre les activités de planification d'urgence suggérées dans la présente amélioration du contrôle dans le cadre de la planification de la continuité des activités organisationnelles, dont entre autres dans le cadre des analyses de l'incidence sur les activités. Les sites de traitement et de stockage définis par l'organisation dans le cadre de la planification d'urgence peuvent changer en fonction des circonstances liées à l'urgence (p. ex. les sites de secours peuvent devenir les sites primaires). Contrôle connexe : PE-12.

(6) PLAN D'URGENCE | SITE DE TRAITEMENT ET STOCKAGE DE SECOURS

L'organisation prévoit le transfert des fonctions opérationnelles et de mission essentielles vers des sites de traitement ou de stockage de secours avec peu ou pas de perte sur le plan de la continuité des activités et maintient cet état pendant la restauration complète vers les sites principaux de traitement ou de stockage des systèmes d'information.

Conseils supplémentaires sur l'amélioration : Les organisations peuvent choisir de mettre en œuvre les activités de planification d'urgence suggérées dans la présente amélioration du contrôle dans le cadre de la planification de la continuité des activités organisationnelles, dont entre autres dans le cadre des analyses de l'incidence sur les activités. Les sites de traitement et de stockage définis par l'organisation dans le cadre de la planification d'urgence peuvent changer en fonction des circonstances liées à l'urgence (p. ex. les sites de secours peuvent devenir les sites primaires). Contrôle connexe : PE-12.

(7) PLAN D'URGENCE | COORDINATION AVEC LES FOURNISSEURS DE SERVICES EXTERNES

L'organisation coordonne son plan d'urgence avec ceux des fournisseurs de services externes pour veiller à répondre aux exigences des plans d'urgence.

Conseils supplémentaires sur l'amélioration : Il peut être difficile pour une organisation d'élaborer un plan d'urgence complet et opportun si sa capacité d'exécuter avec succès ses fonctions opérationnelles et de mission principales dépend de ses fournisseurs de services externes. Dans ce cas, il vaut mieux pour les organisations de coordonner leurs activités de planification d'urgence avec les entités externes pour veiller à ce que le plan de chaque organisation et de chaque entité réponde à ses besoins globaux en cas d'urgence. Contrôle connexe : SA-9.

(8) PLAN D'URGENCE | DÉSIGNATION DES BIENS ESSENTIELS

L'organisation désigne ses biens essentiels en matière de systèmes d'information à l'appui des fonctions opérationnelles et de mission essentielles.

Conseils supplémentaires sur l'amélioration : Les organisations peuvent choisir de mettre en œuvre les activités de planification d'urgence suggérées dans la présente amélioration du contrôle dans le cadre de la planification de la continuité des activités organisationnelles, dont entre autres dans le cadre des analyses de l'incidence sur les activités. Les organisations désignent les biens essentiels en matière de systèmes d'information afin qu'il soit possible d'utiliser des mesures de protection et des contremesures additionnelles (bien au-delà des mesures de protection et des contremesures régulièrement mises en œuvre) pour veiller à la continuité des fonctions opérationnelles et de mission de l'organisation lors des opérations d'urgence. De plus, la désignation des biens essentiels en matière d'information facilite la priorisation des ressources organisationnelles. Les biens essentiels en matière de systèmes d'information comprennent des éléments techniques et opérationnels. Les éléments techniques comprennent, entre autres, les services des technologies de l'information, les composants des systèmes d'information et les produits et mécanismes des technologies de l'information. Les éléments opérationnels comprennent, entre autres, les procédures (opérations exécutées manuellement) et le personnel (des personnes opérant des mécanismes de protection techniques ou exécutant des procédures manuelles). Les plans de protection des programmes organisationnels peuvent faciliter la désignation des biens essentiels. Contrôles connexes : SA-14, SA-15.

Références :

SCT, Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information [Référence 7].
SCT, Norme opérationnelle de sécurité - Programme de planification de la continuité des activités (PCA) [Référence 11].

SCT, Norme opérationnelle de sécurité - Niveaux de préparation des installations du gouvernement fédéral [Référence 12].
CST, ITSD-03A, Directive sur le contrôle du matériel COMSEC au sein du gouvernement du Canada [Référence 36].

CP-3 FORMATION EN MESURES D'URGENCE

Contrôle :

(A) L'organisation offre une formation en mesures d'urgence aux utilisateurs des systèmes d'information. La formation est adaptée en fonction des rôles et des responsabilités assignés aux utilisateurs lors d'une situation d'urgence et ce, dans un délai de [*Affectation : délai défini par l'organisation*] après leur affectation.

(B) L'organisation offre une formation en mesures d'urgence aux utilisateurs des systèmes d'information adaptée à leurs rôles et responsabilités lorsque des changements aux systèmes d'information le justifient.

(C) L'organisation offre une formation en mesures d'urgence aux utilisateurs des systèmes d'information adaptée à leurs rôles et responsabilités tous les [*Affectation : fréquence définie par l'organisation*] par la suite.

Conseils supplémentaires : La formation en mesures de sécurité offerte par l'organisation correspond aux responsabilités et aux rôles assignés à son personnel de sorte à assurer un contenu et un niveau de détails appropriés. Les utilisateurs ordinaires ont peut-être seulement besoin de savoir quand et où ils doivent se présenter pour le travail lors d'opérations d'urgence et si ces mesures auront une incidence sur l'exécution de leurs fonctions normales; les administrateurs de systèmes pourraient avoir besoin d'une formation additionnelle sur l'installation et le paramétrage de systèmes d'information aux sites de traitement et de stockage de secours; les gestionnaires et les cadres pourraient requérir plus de formation précise sur l'exécution de fonctions essentielles à la mission depuis des emplacements hors site et sur l'établissement de modes de communication avec d'autres entités gouvernementales aux fins de coordination des activités connexes au plan d'urgence. La formation sur les mesures d'urgence adaptée aux rôles et aux responsabilités répond à des besoins précis de continuité relevés dans le plan d'urgence. Contrôles connexes : AT-2, AT-3, CP-2, IR-2.

Améliorations du contrôle :

(1) FORMATION EN MESURES D'URGENCE | SIMULATION D'ÉVÉNEMENTS

L'organisation intègre des événements simulés à la formation en mesures d'urgence pour faciliter l'intervention efficace du personnel en situation de crise.

(2) FORMATION EN MESURES D'URGENCE | ENVIRONNEMENT DE FORMATION AUTOMATISÉ

L'organisation utilise des mécanismes automatisés pour créer un environnement de formation en mesures d'urgence complet et plus réaliste.

Références :

Aucune

CP-4 TESTS ET EXERCICES RELATIFS AU PLAN D'URGENCE

Contrôle :

(A) L'organisation teste le plan d'urgence pour les systèmes d'information [*Affectation : fréquence définie par l'organisation*] en utilisant [*Affectation : tests ou exercices définis par l'organisation*] pour en déterminer l'efficacité et établir la mesure dans laquelle l'organisation est prête à l'exécuter.

(B) L'organisation étudie les résultats des tests du plan d'urgence.

(C) Au besoin, l'organisation prend les mesures correctives nécessaires.

Conseils supplémentaires : Il existe plusieurs méthodes pour tester les plans d'urgence en vue de déterminer leur efficacité et de relever des faiblesses possibles, dont notamment les exercices de révision structurée et d'analyse des documents, les listes de vérification, les simulations en parallèle et en état d'arrêt complet et les exercices détaillés. Les tests effectués par les organisations visent à vérifier les exigences en matière de continuité établies dans les plans d'urgence et à déterminer les répercussions sur les opérations organisationnelles, les biens et les personnes découlant des opérations d'urgence. Les organisations disposent d'une certaine souplesse et discrétion quant à la portée, l'étendue et le calendrier des mesures correctives. Contrôles connexes : CP-2, CP-3, IR-3.

Améliorations du contrôle :

(1) TESTS RELATIFS AU PLAN D'URGENCE | COORDINATION AVEC LES PLANS CONNEXES

L'organisation coordonne le test du plan d'urgence avec les éléments organisationnels responsables des plans connexes.

Conseils supplémentaires sur l'amélioration : Les plans connexes aux plans d'urgence pour les systèmes d'information organisationnels comprennent les suivants : plans de continuité des activités, plans de reprise après sinistre, plans de continuité des opérations, plans de reprise des activités, plans d'intervention en cas d'incident et plans d'action d'urgence. Cette amélioration du contrôle n'exige pas des organisations qu'elles créent des éléments organisationnels pour traiter des plans connexes ni qu'elles ne lient ces éléments avec les plans particuliers. Toutefois, si de tels éléments organisationnels existent et qu'ils sont responsables des plans connexes, l'amélioration du contrôle exige une coordination entre ces éléments et l'organisation. Contrôle connexe : IR-8.

(2) TESTS RELATIFS AU PLAN D'URGENCE | SITE DE TRAITEMENT DE SECOURS

(a) L'organisation teste le plan d'urgence au site de traitement de secours afin que le personnel participant au plan d'urgence connaisse mieux l'installation et les ressources qui y sont accessibles.

(b) L'organisation teste le plan d'urgence au site de traitement de secours afin d'évaluer si celui-ci peut prendre en charge les opérations d'urgence.

Conseils supplémentaires sur l'amélioration : Contrôle connexe : CP-7.

(3) TESTS RELATIFS AU PLAN D'URGENCE | TESTS AUTOMATISÉS

L'organisation utilise des mécanismes automatisés pour tester ou vérifier le plan d'urgence de manière plus détaillée et efficace.

Conseils supplémentaires sur l'amélioration : L'organisation utilise des mécanismes automatisés pour tester ou vérifier le plan d'urgence de manière plus détaillée et efficace : i) en assurant une couverture plus complète des situations d'urgence; ii) en sélectionnant des scénarios et des environnements de test plus réalistes; iii) en soumettant les systèmes d'information et les missions concernées à un volume de demandes élevé.

(4) TESTS RELATIFS AU PLAN D'URGENCE | REPRISE / RECONSTITUTION COMPLÈTE

L'organisation inclut dans les tests du plan d'urgence une reprise et une reconstitution complètes du système d'information à un état connu.

Conseils supplémentaires sur l'amélioration : Contrôles connexes : CP-10, SC-24.

Références :

Aucune

CP-5 MISE À JOUR DU PLAN D'URGENCE

[Annulé : Intégré au contrôle CP-2]

CP-6 SITE DE STOCKAGE DE SECOURS

Contrôle :

(A) L'organisation établit un site de stockage de secours, y compris les ententes nécessaires pour permettre le stockage et la récupération de l'information de sauvegarde des systèmes.

(B) L'organisation s'assure que le site de stockage de secours offre des mesures de protection de la sécurité de l'information équivalentes à celles du site principal.

Conseils supplémentaires : Les sites de stockage de secours sont des sites séparés par la géographie des sites de stockage principaux. Les sites de stockage de secours gardent des copies de l'information et des données au cas où le site de stockage principal n'est pas accessible. Les conventions d'utilisation des sites de stockage de secours comprennent des dispositions traitant des conditions environnementales du site de secours, des règles d'accès, des exigences de protection environnementale et physique et de la coordination de la livraison et de la récupération des supports de sauvegarde. Les sites de stockage de secours répondent à l'exigence, inscrite dans les plans d'urgence, selon laquelle les organisations doivent maintenir la capacité d'exécuter les fonctions opérationnelles et de mission essentielles en dépit de toute perturbation, compromission ou défaillance des systèmes d'information organisationnels. Contrôles connexes : CP-2, CP-7, CP-9, CP-10, MP-4.

Améliorations du contrôle :

(1) SITE DE STOCKAGE DE SECOURS | SÉPARATION DU SITE PRINCIPAL

L'organisation identifie un site de stockage de secours distinct du site principal en vue de réduire sa susceptibilité aux mêmes risques.

Conseils supplémentaires sur l'amélioration : Les menaces auxquelles sont susceptibles les sites de stockage de secours sont généralement définies dans les évaluations des risques de l'organisation et comprennent les suivantes : les désastres naturels, les défaillances structurales, les cyberattaques hostiles et les erreurs par omission et par action. Les organisations déterminent la distance géographique suffisante entre les sites de stockage principaux et de secours en fonction des types de menaces auxquelles elles font face. Dans le cas de cyberattaques hostiles, la séparation entre les sites est moins pertinente. Contrôle connexe : RA-3.

(2) SITE DE STOCKAGE DE SECOURS | OBJECTIFS DE DÉLAI ET DE POINT DE REPRISE

L'organisation configure le site de secours de manière à faciliter les opérations de reprise conformément aux objectifs de délai et de point de reprise.

(3) SITE DE STOCKAGE DE SECOURS | ACCESSIBILITÉ

L'organisation identifie les problèmes d'accessibilité potentiels du site stockage de secours dans l'éventualité d'une perturbation ou d'un désastre touchant à toute la région et énonce des mesures d'atténuation explicites.

Conseils supplémentaires sur l'amélioration : Les perturbations touchant à toute la région sont des perturbations dont l'étendue géographique est vaste (p. ex. un ouragan, une panne d'électricité régionale). Une organisation doit identifier elle-même les problèmes d'accessibilité en fonction de son évaluation des risques. Les mesures d'atténuation des risques explicites comprennent les suivantes : (i) copier l'information de sauvegarde à d'autres sites de stockage de secours si un problème d'accessibilité survient aux sites de secours originaux et (ii) planifier l'accès physique en prévision d'une récupération de l'information de sauvegarde au cas où l'accessibilité électronique au site de secours est perturbée. Contrôle connexe : RA-3.

Références :

Aucune

CP-7 SITE DE TRAITEMENT DE SECOURS

Contrôle :

(A) L'organisation établit un site de traitement de secours, y compris les ententes nécessaires pour permettre le transfert et la reprise [*Affectation : opérations des systèmes d'information définies par l'organisation*] pour les fonctions opérationnelles et de mission essentielles dans un délai de [*Affectation : durée conforme aux objectifs de délai et de point de reprise définis par l'organisation*], lorsque les capacités de traitement principales ne sont pas accessibles.

(B) L'organisation s'assure que l'équipement et les fournitures nécessaires au transfert et à la reprise des opérations sont accessibles au site de traitement secours, ou qu'il existe des contrats pour assurer leur livraison au site, et ce, dans les délais définis par l'organisation pour le transfert ou la reprise des activités.

(C) L'organisation s'assure que le site de traitement de secours offre des mesures de protection de la sécurité de l'information équivalentes à celles du site principal.

Conseils supplémentaires : Les sites de traitement de secours sont des sites géographiquement séparés des sites de traitement principaux. Un site de traitement de secours offre une capacité de traitement au cas où le site de traitement principal n'est pas accessible. Les conventions d'utilisation des sites de traitement de secours comprennent des dispositions traitant des conditions environnementales du site de secours, des règles d'accès, des exigences de protection environnementale et physique et de la coordination du transfert ou de l'affectation du personnel. Les plans d'urgence font état d'exigences particulières attribuées à des sites de traitement de secours précis afin que les organisations maintiennent la capacité d'exécuter les fonctions opérationnelles et de mission essentielles en dépit de toute perturbation, compromission ou défaillance des systèmes d'information organisationnels. Contrôles connexes : CP-2, CP-6, CP-8, CP-9, CP-10, MA-6.

Améliorations du contrôle :

(1) SITE DE TRAITEMENT DE SECOURS | SÉPARATION DU SITE PRINCIPAL

L'organisation désigne un site de traitement de secours distinct du site principal en vue de réduire sa susceptibilité aux mêmes risques.

Conseils supplémentaires sur l'amélioration : Les menaces auxquelles sont susceptibles les sites de traitement de secours sont généralement définies dans les évaluations des risques de l'organisation et comprennent les suivantes : les désastres naturels, les défaillances structurales, les cyberattaques hostiles et les erreurs par omission et par action. Les organisations déterminent la distance géographique suffisante entre les sites de traitement principaux et de secours en fonction des types de menaces auxquelles elles font face. Dans le cas de cyberattaques hostiles, la séparation entre les sites est moins pertinente. Contrôle connexe : RA-3.

(2) SITE DE TRAITEMENT DE SECOURS | ACCESSIBILITÉ

L'organisation relève les problèmes d'accessibilité potentiels du site traitement de secours dans l'éventualité d'une perturbation ou d'un désastre touchant à toute la région et énonce des mesures d'atténuation explicites.

Conseils supplémentaires sur l'amélioration : Les perturbations touchant à toute la région sont des perturbations dont l'étendue géographique est vaste (p. ex. un ouragan, une panne d'électricité régionale). Une organisation doit relever elle-même les problèmes d'accessibilité en fonction de son évaluation des risques. Contrôle connexe : RA-3

(3) SITE DE TRAITEMENT DE SECOURS | PRIORITÉ DE SERVICE

L'organisation élabore, pour le site de traitement de secours, des conventions qui prévoient des dispositions de priorité de service conformément aux exigences d'accessibilité de l'organisation (y compris les objectifs de délai de récupération).

Conseils supplémentaires sur l'amélioration : Les conventions de priorité de services sont des ententes négociées avec des fournisseurs de service pour veiller à ce que l'organisation reçoive une priorité de service qui reflète ses exigences d'accessibilité et la disponibilité des ressources d'information au site de traitement de secours.

(4) SITE DE TRAITEMENT DE SECOURS | PRÉPARATION EN VUE DE L'UTILISATION

L'organisation prépare le site de traitement de secours de manière qu'il soit prêt à être utilisé comme site opérationnel pouvant prendre en charge les fonctions opérationnelles et de mission essentielles.

Conseils supplémentaires sur l'amélioration : La préparation du site de secours comprend : déterminer les paramètres de configuration des composants des systèmes d'information de sorte qu'ils correspondent aux exigences établies au site principal; approvisionner le site des fournitures essentiels; veiller à mettre en place tous les éléments de logistique. Contrôles connexes : CM-2, CM-6.

(5) SITE DE TRAITEMENT DE SECOURS | MESURES DE PROTECTION DE LA SÉCURITÉ DE L'INFORMATION ÉQUIVALENTES

[Annulé : Intégré au contrôle CP-7]

(6) SITE DE TRAITEMENT DE SECOURS | IMPOSSIBILITÉ DE REVENIR AU SITE PRINCIPAL

L'organisation planifie et se prépare à composer avec des circonstances qui empêchent le retour au site de traitement principal.

Références :

Aucune

CP-8 SERVICES DE TÉLÉCOMMUNICATIONS

Contrôle :

(A) L'organisation établit des services de télécommunications de secours, y compris les conventions nécessaires pour permettre la reprise de [*Affectation : opérations des systèmes d'information définies par l'organisation*] pour les fonctions opérationnelles et de mission essentielles dans un délai de [*Affectation : durée définie par l'organisation*] lorsque les capacités de télécommunications principales ne sont pas accessibles aux sites de stockage ou de traitement principaux ou de secours.

Conseils supplémentaires : Ce contrôle s'applique aux services de télécommunications (données et voix) aux sites principaux et de secours de traitement et de stockage. Les services de télécommunications de secours répondent aux exigences de continuité des activités établies dans les plans de secours et permettent le maintien des fonctions opérationnelles et de mission essentielles en dépit de la perte des services de télécommunications principaux. Les organisations peuvent préciser des délais différents pour les sites principaux et de secours. Les services de télécommunications de secours comprennent, entre autres, les lignes ou circuits terrestres

commerciaux ou organisationnels ou les satellites au lieu des communications terrestres. Les organisations tiennent compte de facteurs comme la disponibilité, la qualité de service et l'accès lorsqu'elles signent des conventions de télécommunications de secours. Contrôles connexes : CP-2, CP-6, CP-7.

Améliorations du contrôle :

(1) SERVICES DE TÉLÉCOMMUNICATIONS | DISPOSITIONS DE PRIORITÉ DE SERVICE

(a) L'organisation élabore des conventions de services de télécommunications principaux et de secours qui prévoient des dispositions de priorité de service conformes aux exigences d'accessibilité de l'organisation (y compris les objectifs de délai de récupération);

(b) L'organisation demande une priorité de services de télécommunications pour tous les services de télécommunications utilisés dans le cadre de préparatifs d'urgence en cas d'événement portant atteinte à la sécurité nationale dans l'éventualité où les services de télécommunications principaux ou de secours sont assurés par une entreprise de télécommunications.

Conseils supplémentaires sur l'amélioration : Les organisations doivent évaluer l'incidence possible sur les opérations et la mission si les fournisseurs de services de télécommunications offrent des services à d'autres organisations ayant des dispositions de priorité de service semblables.

(2) SERVICES DE TÉLÉCOMMUNICATIONS | POINTS DE DÉFAILLANCE UNIQUES

L'organisation obtient les services de télécommunications de secours pour réduire la probabilité de partage d'un point de défaillance unique avec les services de télécommunications principaux.

(3) SERVICES DE TÉLÉCOMMUNICATIONS | SÉPARATION DES FOURNISSEURS PRINCIPAUX ET DE SECOURS

L'organisation obtient des services de télécommunications de secours auprès de fournisseurs distincts des fournisseurs principaux afin de réduire la vulnérabilité aux mêmes menaces.

Conseils supplémentaires sur l'amélioration : Les menaces auxquelles sont vulnérables les services de télécommunications sont généralement définies dans les évaluations des risques de l'organisation et comprennent les suivantes : les désastres naturels, les défaillances structurales, les cyberattaques hostiles, les attaques physiques hostiles et les erreurs par omission et par action. Les organisations visent à réduire les vulnérabilités communes en minimisant l'utilisation, par les fournisseurs de services de télécommunications, d'une infrastructure partagée et en sélectionnant des services ayant une séparation géographique adéquate. Les organisations peuvent considérer l'utilisation d'un seul fournisseur de services lorsque celui-ci peut fournir des services de télécommunications de secours qui répondent aux exigences de séparation établies dans l'évaluation des risques.

(4) SERVICES DE TÉLÉCOMMUNICATIONS | PLAN D'URGENCE DU FOURNISSEUR

(a) L'organisation exige des fournisseurs de services de télécommunications principaux et de secours qu'ils possèdent des plans d'urgence.

(b) L'organisation examine les plans d'urgence des fournisseurs afin de s'assurer qu'ils répondent aux exigences organisationnelles en matière d'urgence.

(c) L'organisation obtient la preuve de mises à l'essai et de formation en mesures d'urgence tous les [*Affectation : fréquence définie par l'organisation*] auprès des fournisseurs.

Conseils supplémentaires sur l'amélioration : L'examen des plans d'urgence des fournisseurs tient compte du caractère exclusif de ces plans. Un résumé des plans d'urgence des fournisseurs peut parfois constituer une preuve suffisante des plans d'urgence et satisfaire à l'exigence d'examen. Les fournisseurs de services de télécommunications peuvent participer aux exercices permanents de reprise après sinistre en collaboration avec Sécurité publique Canada et les administrations municipales et provinciales. Les organisations peuvent utiliser ce type d'activités à titre de preuve satisfaisant aux exigences de formation liée aux plans d'urgence et d'examen et de mise à l'essai de ceux-ci.

(5) SERVICES DE TÉLÉCOMMUNICATIONS | TEST DES SERVICES DE TÉLÉCOMMUNICATIONS DE SECOURS

L'organisation teste les services de télécommunications de secours [*Affectation : fréquence définie par l'organisation*].

Références :

Aucune

CP-9 SAUVEGARDE DU SYSTÈME D'INFORMATION

Contrôle :

(A) L'organisation effectue des sauvegardes des données utilisateur contenues dans le système d'information [*Affectation : fréquence définie par l'organisation et conforme aux objectifs de délai et de point de reprise*].

(B) L'organisation effectue des sauvegardes des données système contenues dans le système d'information [*Affectation : fréquence définie par l'organisation et conforme aux objectifs de temps et de point de reprise*].

(C) L'organisation effectue des sauvegardes de la documentation liée au système d'information, y compris la documentation sur la sécurité [*Affectation : fréquence définie par l'organisation et conforme aux objectifs de temps et de point de reprise*].

(D) L'organisation protège la confidentialité, l'intégrité et l'accessibilité de l'information de sauvegarde aux sites de stockage.

(AA) L'organisation détermine les périodes de conservation de l'information opérationnelle essentielle et des sauvegardes archivées.

Conseils supplémentaires : L'information système comprend, par exemple, l'information d'état, les logiciels du système d'exploitation et d'application, de même que les licences. L'information utilisateur comprend toute information qui n'est pas de l'information système. Les organisations utilisent des mécanismes de protection de l'intégrité des sauvegardes des systèmes d'information qui comprennent les signatures numériques et le hachage cryptographique. La protection de l'information sur les sauvegardes système en transit est hors de la portée de ce contrôle. Les sauvegardes de systèmes d'information répondent aux exigences établies dans les plans d'urgence ainsi qu'aux exigences organisationnelles concernant la sauvegarde d'information. Contrôles connexes : CP-2, CP-6, MP-4, MP-5, SC-13.

Améliorations du contrôle :

(1) SAUVEGARDE DU SYSTÈME D'INFORMATION | TESTS DE FIABILITÉ ET D'INTÉGRITÉ

L'organisation effectue des tests de l'information de sauvegarde [*Affectation : fréquence définie par l'organisation*] pour vérifier la fiabilité des supports et l'intégrité de l'information.

Conseils supplémentaires sur l'amélioration : Contrôle connexe : CP-4.

(2) SAUVEGARDE DU SYSTÈME D'INFORMATION | ESSAI DE RESTAURATION AU MOYEN DE L'ÉCHANTILLONNAGE

L'organisation utilise un échantillon de l'information de sauvegarde pour restaurer certaines fonctions du système d'information dans le cadre des tests du plan d'urgence.

Conseils supplémentaires sur l'amélioration : Contrôle connexe : CP-4.

(3) SAUVEGARDE DU SYSTÈME D'INFORMATION | STOCKAGE DISTINCT POUR L'INFORMATION ESSENTIELLE

L'organisation conserve des copies de sauvegarde [*Affectation : information liée à la sécurité et logiciels des systèmes d'information essentiels définis par l'organisation*], dans une installation distincte ou un conteneur résistant au feu situé hors de l'emplacement du système opérationnel.

Conseils supplémentaires sur l'amélioration : Les logiciels des systèmes d'information essentiels comprennent les systèmes d'exploitation, les systèmes de gestion de clés cryptographiques et les systèmes de détection et de prévention d'intrusions. L'information liée à la sécurité comprend les inventaires organisationnels de composants matériels, logiciels et micrologiciels. Les sites de stockage de secours servent généralement aussi à titre d'installation de stockage distincte pour les organisations. Contrôles connexes : CM-2, CM-8.

(4) SAUVEGARDE DU SYSTÈME D'INFORMATION | PROTECTION CONTRE LES MODIFICATIONS NON AUTORISÉES

[Annulé : Intégré au contrôle CP-9]

(5) SAUVEGARDE DU SYSTÈME D'INFORMATION | TRANSFERT AU SITE DE STOCKAGE DE SECOURS

L'organisation transfère l'information de sauvegarde du système d'information à un site de stockage de secours [*Affectation : durée et débit de transfert définis par l'organisation et conformes aux objectifs de délai et de point de reprise*].

Conseils supplémentaires sur l'amélioration : L'information de sauvegarde des systèmes d'information peut être transférée à des sites de stockage de secours par voie électronique ou par l'envoi physique de dispositifs de stockage.

(6) SAUVEGARDE DU SYSTÈME D'INFORMATION | SYSTÈME SECONDAIRE REDONDANT

L'organisation effectue la sauvegarde du système d'information au moyen d'un système secondaire redondant n'étant pas situé au même endroit que le système principal et pouvant être activé sans perte d'information ou perturbation des opérations.

Conseils supplémentaires sur l'amélioration : Contrôles connexes : CP-7, CP-10.

(7) SAUVEGARDE DU SYSTÈME D'INFORMATION | DOUBLE AUTORISATION

L'organisation applique l'exigence de double autorisation pour la suppression ou la destruction [*Affectation : information de sauvegarde définie par l'organisation*].

Conseils supplémentaires sur l'amélioration : La double autorisation fait en sorte qu'il est impossible de supprimer ou de détruire l'information de sauvegarde à moins que deux personnes qualifiées le fassent. Les personnes responsables de la suppression et de la destruction de l'information de sauvegarde détiennent les compétences nécessaires pour déterminer si la suppression/destruction de l'information de sauvegarde respecte les politiques et les procédures organisationnelles. La double autorisation est également appelée le contrôle par deux personnes. Contrôles connexes : AC-3, MP-2.

Références :

SCT, Norme opérationnelle sur la sécurité matérielle [Référence 6].
SCT, Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information [Référence 7].

CP-10 REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION

Contrôle :

(A) L'organisation permet la reprise et la reconstitution du système d'information à un état connu après une interruption, une compromission ou une défaillance.

Conseils supplémentaires : La reprise consiste à exécuter les activités du plan d'urgence du système d'information pour restaurer les fonctions opérationnelles et de mission de l'organisation. La reconstitution suit la reprise et englobe les activités de restauration des systèmes d'information organisationnels à un état opérationnel complet. Les opérations de reprise et de reconstitution correspondent aux priorités opérationnelles et de la mission, aux objectifs de délai ou de point de reprise et de reconstitution, ainsi qu'aux paramètres organisationnels lesquels sont conformes aux exigences du plan d'urgence. La reconstitution inclut la

désactivation de toute capacité intérimaire du système d'information qui aurait pu servir durant les opérations de reprise. Elle comprend également des évaluations des capacités des systèmes d'information restaurés, du rétablissement des activités de surveillance continue, des réautorisations possibles des systèmes d'information et des activités visant à préparer les systèmes en cas de perturbation, de compromission ou de défaillance future. Les capacités de reprise et de reconstitution utilisées par les organisations peuvent comprendre des mécanismes automatisés et des procédures manuelles. Contrôles connexes : CA-2, CA-6, CA-7, CP-2, CP-4, CP-6, CP-7, CP-9, SC-24.

Améliorations du contrôle :

(1) REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION | TESTS RELATIFS AU PLAN D'URGENCE

[Annulé : Intégré au contrôle CP-4]

(2) REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION | REPRISE DES TRANSACTIONS

Les systèmes d'information appliquent un processus de reprise des transactions pour les systèmes de traitement transactionnel.

Conseils supplémentaires sur l'amélioration : Les systèmes d'information transactionnels comprennent, entre autres, les systèmes de gestion des bases de données et les systèmes de traitement des transactions. Les mécanismes d'annulation et de journalisation de transactions sont des exemples de mécanismes à l'appui de la reprise de transactions.

(3) REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION | CONTRÔLES DE SÉCURITÉ COMPENSATOIRES

[Annulé : Intégré aux procédures d'adaptation.]

(4) REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION | RESTAURATION DANS LES DÉLAIS PRÉCISÉS

L'organisation a la capacité de restaurer les composants des systèmes d'information [*Affectation : durées de restauration définies par l'organisation*] en utilisant de l'information dont la configuration est contrôlée et l'intégrité est protégée et représentant les composants dans un état connu et opérationnel.

Conseils supplémentaires sur l'amélioration : La restauration des composants des systèmes d'information comprend le reformatage, lequel restaure les composants à un état opérationnel connu. Contrôle connexe : CM -2.

(5) REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION | CAPACITÉ DE BASCULEMENT

[Annulé : Intégré au contrôle SI-13.]

(6) REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION | PROTECTION DES COMPOSANTS

L'organisation protège le matériel, les micrologiciels et les logiciels de sauvegarde et de restauration.

Conseils supplémentaires sur l'amélioration : La protection des composants du matériel, des micrologiciels et des logiciels de sauvegarde et de restauration comprend des mesures de protection à la fois physiques et techniques. Les logiciels de sauvegarde et de restauration comprennent, entre autres, les routeurs, les compilateurs et d'autres systèmes logiciels liés à la sécurité. Contrôles connexes : AC-3, AC-6, PE-3.

Références :

SCT, Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information [Référence 7].

CP-11 PROTOCOLES DES COMMUNICATIONS DE SECOURS

Contrôle :

(A) Le système d'information permet l'utilisation [*Affectation : protocoles de communications de secours définis par l'organisation*] afin de maintenir la continuité des opérations.

Conseils supplémentaires : Les plans de secours, ainsi que la formation et les tests liés aux plans, intègrent la capacité de protocoles de communications de secours dans le cadre du renforcement de la résilience des systèmes d'information organisationnels. Les protocoles de communications de secours comprennent, entre autres, le remplacement du protocole TCP/IP version 4 par le protocole TCP/IP version 6. L'utilisation d'un différent protocole de communications peut perturber les applications logicielles; les effets secondaires de l'introduction de protocoles de communications de secours sont donc analysés avant la mise en œuvre de cette mesure.

Améliorations du contrôle :

Aucune

Références :

Aucune

CP-12 MODE SANS ÉCHEC

Contrôle :

(A) Le système d'information passe au mode sans échec [*Affectation : contraintes du mode d'opération sans échec définies par l'organisation*] lorsqu'il détecte [*Affectation : conditions définies par l'organisation*].

Conseils supplémentaires : Lorsque les systèmes d'information sont utilisés pour exécuter certaines fonctions opérationnelles et de mission critiques (p. ex. les systèmes d'armes et les opérations militaires, les activités spatiales civiles, l'exploitation de centrales nucléaires et les activités de contrôle de la circulation aérienne), surtout lorsqu'il s'agit d'environnements opérationnels en temps réel, les organisations peuvent choisir de déterminer quelles conditions entraîneront un passage au mode d'opération sans échec prédéfini. Le mode d'opération sans échec, lequel peut être déclenché manuellement ou automatiquement, limite le type d'activités ou d'opérations qu'un système d'information peut exécuter si certaines conditions sont présentes. Le système pourrait notamment forcer une réduction de l'alimentation ou de la bande passante avant de permettre l'exécution de certaines fonctions.

Améliorations du contrôle :

Aucune

Références :

Aucune

CP-13 MÉCANISMES DE SÉCURITÉ DE SECOURS

Contrôle :

(A) L'organisation utilise [*Affectation : mécanismes de sécurité de secours ou additionnels définis par l'organisation*] en vue d'exécuter [*Affectation : fonctions de sécurité définies par l'organisation*] lorsque le mode principal d'exécution de la fonction de sécurité est compromis ou n'est pas disponible.

Conseils supplémentaires : Ce contrôle appuie les exigences en matière de résilience du système d'information, de planification d'urgence et de continuité des opérations. Afin de veiller à la continuité des opérations et de la mission, les organisations peuvent mettre en œuvre des mécanismes de sécurité de secours ou additionnels. Les mécanismes pourraient être moins efficaces que les mécanismes primaires (p. ex. moins conviviaux ou moins sûrs). Toutefois, la facilité d'accès à ces mécanismes additionnels ou de secours rehausse la capacité générale d'une organisation d'assurer la continuité de la mission et des opérations qui pourraient être touchées si l'organisation devait suspendre ses opérations organisationnelles jusqu'à la reprise du mode d'exécution primaire des fonctions. Étant donné le coût et l'effort global requis pour assurer de telles capacités de secours, le présent contrôle ne s'applique généralement qu'aux fonctions de sécurités critiques assurées par les systèmes d'information, les composants systèmes ou les services de systèmes d'information. Une organisation pourrait, par exemple, donner un carnet de clés à usage unique aux cadres supérieurs et aux administrateurs de systèmes leur permettant d'être authentifiés de manière sûre à distance au cas où il y avait une compromission du mode d'authentification habituel de l'organisation. Contrôle connexe : CP-2.

Améliorations du contrôle :

Aucune

Références :

Aucune

3.7 FAMILLE : IDENTIFICATION ET AUTHENTIFICATION

CLASSE : TECHNIQUE

IA-1 POLITIQUE ET PROCÉDURES D'IDENTIFICATION ET D'AUTHENTIFICATION

Contrôle :

(A) L'organisation élabore et consigne, ainsi que diffuse [*Affectation : personnel ou rôles définis par l'organisation*] :

(a) une politique d'identification et d'authentification qui définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité;

(b) des procédures pour faciliter la mise en œuvre de la politique d'identification et d'authentification et des contrôles d'identification et d'authentification connexes.

(B) L'organisation examine et met à jour :

(a) la politique d'identification et d'authentification tous les [*Affectation : fréquence définie par l'organisation*];

(b) les procédures d'identification et d'authentification tous les [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : Ce contrôle traite de la mise en place d'une politique et de procédures nécessaires à la mise en œuvre efficace de contrôles de sécurité particuliers et d'améliorations précises des contrôles pour la famille d'identification et d'authentification. La politique et les procédures tiennent compte des lois applicables du GC ainsi que des politiques, des directives et des normes du SCT. Les politiques et les procédures du programme de sécurité organisationnel peuvent rendre facultatives les politiques et procédures propres au système. La politique peut être intégrée à la politique générale sur la sécurité de l'information des organisations ou, inversement, elle peut être représentée par de multiples politiques compte tenu de la nature complexe de certaines organisations. Les procédures peuvent être déterminées pour le programme de sécurité général et pour des systèmes d'information particuliers, au besoin. La stratégie organisationnelle de gestion des risques est un facteur clé dans l'établissement de la politique et des procédures.

Améliorations du contrôle :

Aucune

Références :

SCT, *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* [Référence 7].

IA-2 IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS ORGANISATIONNELS)

Contrôle :

(A) Le système d'information identifie et authentifie les utilisateurs organisationnels (ou les processus exécutés en leur nom) de façon unique.

Conseils supplémentaires : Les utilisateurs organisationnels incluent les employés ou les personnes dont l'organisation juge le statut équivalent à celui d'un employé (p. ex. entrepreneurs et chercheurs invités). Ce

contrôle s'applique à tous les accès autres que (i) les accès identifiés explicitement et consignés dans le contrôle AC -14 et (ii) les accès accordés sans authentification individuelle grâce à l'utilisation autorisée d'authentifiants de groupe. Les organisations pourraient exiger l'identification individuelle de chacune des personnes comprises dans un compte de groupe (p. ex. les comptes à privilèges partagés) aux fins de comptabilisation détaillée des activités de chaque personne. Les organisations utilisent des mots de passe, des jetons ou la biométrie pour authentifier les identités d'utilisateurs, ou encore une combinaison de ces trois méthodes pour l'authentification multifactorielle. L'accès aux systèmes d'information organisationnels est soit local, soit réseau. Un accès local est tout accès à des systèmes d'information de l'organisation, par un utilisateur ou par un processus exécuté au nom d'un utilisateur, effectué par une connexion directe, sans recours à un réseau. L'accès réseau est tout accès aux systèmes d'information organisationnels, par un utilisateur ou un processus exécuté au nom d'un utilisateur, effectué au moyen de connexions réseau (c.-à-d. des accès non locaux). L'accès à distance est un type d'accès réseau qui requiert la communication au moyen de réseaux externes (p. ex. Internet). Les réseaux internes incluent les réseaux locaux et les réseaux élargis. De plus, les RPV chiffrés servant aux connexions réseau entre des points terminaux contrôlés par l'organisation et des points terminaux contrôlés par une autre entité peuvent être traités comme des réseaux internes du point de vue de protection de la confidentialité et de l'intégrité de l'information transmise sur ces réseaux.

L'authentification multifactorielle exige l'utilisation de deux facteurs différents ou plus aux fins d'authentification. Les facteurs sont définis comme suit : (i) une information connue (p. ex. un mot de passe ou un numéro d'identification personnel [NIP]); (ii) une possession (p. ex. un dispositif d'identification cryptographique ou un jeton); (iii) un attribut personnel (p. ex. la biométrie). Les solutions multifactorielles exigeant des dispositifs distincts des systèmes d'information obtenant l'accès comprennent, entre autres, les jetons matériels offrant des authentifiants temporels et de simulation-réponse ainsi que les cartes à puce d'identité. En plus de permettre l'identification et l'authentification des utilisateurs au niveau du système d'information (c.-à-d., au moment de l'ouverture de session), les organisations utilisent aussi des mécanismes d'identification et d'authentification au niveau de l'application, selon le besoin, pour accroître la sécurité de l'information. Les exigences d'identification et d'authentification pour des personnes autres que les utilisateurs organisationnels sont décrites dans le contrôle IA-8. Contrôles connexes : AC-2, AC-3, AC -14, AC -17, AC -18, IA-4, IA-5, IA-8.

Améliorations du contrôle :

(1) IDENTIFICATION ET AUTHENTIFICATION | ACCÈS RÉSEAU AUX COMPTES PRIVILÉGIÉS

Le système d'information applique l'authentification multifactorielle pour l'accès réseau aux comptes privilégiés.

Conseils supplémentaires sur l'amélioration : Contrôle connexe : AC -6.

(2) IDENTIFICATION ET AUTHENTIFICATION | ACCÈS RÉSEAU AUX COMPTES NON PRIVILÉGIÉS

Le système d'information applique l'authentification multifactorielle pour l'accès réseau aux comptes non privilégiés.

(3) IDENTIFICATION ET AUTHENTIFICATION | ACCÈS LOCAL AUX COMPTES PRIVILÉGIÉS

Le système d'information applique l'authentification multifactorielle pour l'accès local aux comptes privilégiés.

Conseils supplémentaires sur l'amélioration : Contrôle connexe : AC -6.

(4) IDENTIFICATION ET AUTHENTIFICATION | ACCÈS LOCAL AUX COMPTES NON PRIVILÉGIÉS

Le système d'information applique l'authentification multifactorielle pour l'accès local aux comptes non privilégiés.

(5) IDENTIFICATION ET AUTHENTIFICATION | AUTHENTIFICATION DE GROUPE

L'organisation exige des utilisateurs qu'ils soient authentifiés par un authentifiant individuel lorsqu'un authentifiant de groupe est utilisé.

Conseils supplémentaires sur l'amélioration : Les organisations exigeant l'utilisation d'authentifiants individuels à titre de deuxième niveau d'authentification leur permet de réduire les risques associés à l'utilisation d'authentifiants de groupe.

(6) IDENTIFICATION ET AUTHENTIFICATION | ACCÈS RÉSEAU AUX COMPTES PRIVILÉGIÉS - DISPOSITIF DISTINCT

Le système d'information utilise l'authentification multifactorielle pour l'accès réseau aux comptes privilégiés de la manière suivante : un des facteurs est fourni par un dispositif distinct du système demandant l'accès et le dispositif satisfait [*Affectation : exigences de la force du mécanisme définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Contrôle connexe : AC -6.

(7) IDENTIFICATION ET AUTHENTICATION | ACCÈS RÉSEAU AUX COMPTES NON PRIVILÉGIÉS - DISPOSITIF DISTINCT

Le système d'information utilise l'authentification multifactorielle pour l'accès réseau aux comptes non privilégiés de la manière suivante : un des facteurs est fourni par un dispositif distinct du système demandant l'accès et le dispositif satisfait [*Affectation : exigences de la force du mécanisme définies par l'organisation*].

(8) IDENTIFICATION ET AUTHENTICATION | ACCÈS RÉSEAU AUX COMPTES PRIVILÉGIÉS - RÉSISTANCE À LA RÉINSERTION

Le système d'information met en œuvre des mécanismes d'authentification résistants à la réinsertion pour l'accès réseau aux comptes privilégiés.

Conseils supplémentaires sur l'amélioration : Les processus d'authentification résistent aux attaques par réinsertion lorsqu'il n'est pas pratique de réaliser une authentification réussie en réinsérant un message d'authentification antérieur. Les techniques de résistance à la réinsertion incluent, entre autres, les protocoles qui font appel aux nonces ou aux défis (p. ex. le protocole TLS) et à des authentifiants à usage unique synchrones ou simulation-réponse.

(9) IDENTIFICATION ET AUTHENTICATION | ACCÈS RÉSEAU AUX COMPTES NON PRIVILÉGIÉS - RÉSISTANCE À LA RÉINSERTION

Le système d'information applique des mécanismes d'authentification résistants à la réinsertion pour l'accès réseau aux comptes non privilégiés.

Conseils supplémentaires sur l'amélioration : Les processus d'authentification résistent aux attaques par réinsertion lorsqu'il n'est pas pratique de réussir une authentification réussie en enregistrant ou réinsérant un message d'authentification antérieur. Les techniques de résistance à la réinsertion incluent, entre autres, les protocoles qui font appel aux nonces ou aux défis (p. ex. le protocole TLS) et à des authentifiants à usage unique synchrones ou simulation-réponse.

(10) IDENTIFICATION ET AUTHENTIFICATION | AUTHENTIFICATION UNIQUE (SSO)

Le système d'information offre une fonctionnalité d'authentification unique (SSO) pour [*Affectation : liste définie par l'organisation des services et des comptes du système d'information*].

Conseils supplémentaires sur l'amélioration : L'authentification unique permet aux utilisateurs d'ouvrir une session une seule fois et d'accéder à multiples ressources du système d'information. Les organisations doivent évaluer l'efficacité opérationnelle offerte par la fonctionnalité d'authentification unique ainsi que l'augmentation du risque que celle-ci comporte relativement à la divulgation et à l'accès accordé par celle-ci à de nombreuses ressources du système.

(11) IDENTIFICATION ET AUTHENTIFICATION | ACCÈS À DISTANCE - DISPOSITIF DISTINCT

Le système d'information utilise l'authentification multifactorielle pour l'accès à distance aux comptes privilégiés et non privilégiés de la manière suivante : un des facteurs est fourni par un dispositif distinct du

système auquel on accède et le dispositif satisfait [*Affectation : exigences de la force du mécanisme définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Pour ce qui est de l'accès à distance aux comptes privilégiés et non privilégiés, il est possible de réduire la probabilité de compromission des justificatifs d'authentification stockés sur le système d'information auquel on accède en exigeant l'utilisation, pour un des facteurs lors d'une authentification multifactorielle, d'un dispositif distinct du système. Par exemple, des adversaires pourraient déployer un programme malveillant sur des systèmes d'information organisationnels et possiblement compromettre les justificatifs stockés sur le système de manière à usurper l'identité des utilisateurs autorisés. Contrôle connexe : AC-6.

(12) IDENTIFICATION ET AUTHENTIFICATION | ACCEPTATION DES JUSTIFICATIFS DE VÉRIFICATION DE L'IDENTITÉ PERSONNELLE (PIV)

Le système d'information accepte et vérifie électroniquement les justificatifs de vérification de l'identité personnelle (PIV pour *Personal Identity Verification*).

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle s'applique aux organisations qui mettent en œuvre des systèmes de contrôle d'accès logique et physique. Les justificatifs PIV sont attribués par les organismes fédéraux conformes à la publication 201 des Federal Information Processing Standards (*FIPS Publication 201*) et aux documents d'orientation connexes. Le SCT n'exige pas l'utilisation des cartes PIV, mais le CST recommande leur utilisation à titre de justificatif d'identité. Contrôles connexes : AU-2, PE-3, SA-4.

(13) IDENTIFICATION ET AUTHENTIFICATION | AUTHENTIFICATION HORS BANDE

Le système d'information applique [*Affectation : authentification hors bande définie par l'organisation*] si les circonstances suivantes sont présentes : [*Affectation : conditions définies par l'organisation*].

Conseils supplémentaires pour l'amélioration : Par authentification hors bande, on entend l'utilisation de deux chemins de communication distincts pour identifier et authentifier les utilisateurs ou les dispositifs auprès d'un système d'information. Le premier chemin (c.-à-d. le chemin en bande) sert à identifier et authentifier les utilisateurs ou les dispositifs, et est généralement le chemin par lequel est transmise l'information. Le deuxième chemin (c.-à-d. le chemin hors bande) sert à vérifier l'authentification de manière indépendante et à demander une action. Par exemple, un utilisateur est authentifié au moyen d'un ordinateur portatif auprès d'un serveur à distance auquel l'utilisateur veut accéder et auquel il transmet une demande d'action en employant le même chemin de communication. Le serveur communique ensuite avec l'utilisateur au moyen de son téléphone cellulaire afin de confirmer que l'action demandée provenait de l'utilisateur. L'utilisateur peut soit confirmer l'action demandée directement à la personne l'ayant appelé, ou il peut fournir un code d'authentification au téléphone. Ce type d'authentification peut être utilisé par les organisations souhaitant atténuer les attaques par interception réelles ou soupçonnées. Les conditions d'activation peuvent inclure, entre autres, des activités suspectes, de nouveaux indicateurs de menace, des niveaux de menace élevés, l'incidence d'une divulgation ou le niveau de classification de l'information transmise par les transactions. Contrôles connexes : IA-10, IA-11, SC-37.

(100) LE SYSTÈME D'INFORMATION UTILISE L'AUTHENTIFICATION MULTIFACTORIELLE POUR L'ACCÈS À DISTANCE AUX COMPTES PRIVILÉGIÉS.

[Annulé : Intégré aux contrôles IA-2 Amélioration du contrôle 11]

Références :

CST, *ITSG-31, Guide sur l'authentification des utilisateurs pour les systèmes TI* [Référence 18].
CST, *ITSB-60, Conseils sur l'utilisation du protocole TLS (Transport Layer Security) au sein du gouvernement du Canada* [Référence 34].

IA-3 IDENTIFICATION ET AUTHENTIFICATION DES DISPOSITIFS

Contrôle :

(A) Le système d'information identifie et authentifie, de manière unique [*Affectation : dispositifs particuliers ou types de dispositifs définis par l'organisation*] avant d'établir une connexion [*Sélection (une ou plusieurs) : locale, à distance, réseau*].

Conseils supplémentaires : Les dispositifs organisationnels devant être identifiés et authentifiés de façon unique de dispositif à dispositif peuvent être définis par type, par dispositif, ou par une combinaison des deux. Les systèmes d'information utilisent normalement soit de l'information partagée connue (p. ex. adresses de contrôle d'accès au support [MAC pour *Media Access Control*] ou TCP/IP [*Transmission Control Protocol/Internet Protocol*]) aux fins d'identification de dispositif, soit des solutions d'authentification organisationnelles (p. ex. Institute of Electrical and Electronics Engineers [IEEE] 802.1x et EAP, serveur Radius avec authentification EAP-TLS, Kerberos) pour identifier et authentifier les dispositifs sur les réseaux locaux ou étendus. Les organisations déterminent la robustesse requise des mécanismes d'authentification en fonction des catégories de sécurité des systèmes d'information. Étant donné la difficulté de mettre en place un tel contrôle à grande échelle, on encourage les organisations à n'appliquer le contrôle qu'aux quelques dispositifs (et aux types de dispositifs) qui doivent réellement prendre cette fonctionnalité en charge. Contrôles connexes : AC -17, AC -18, AC -19, CA-3, IA-4, IA-5.

Améliorations du contrôle :

(1) IDENTIFICATION ET AUTHENTIFICATION DES DISPOSITIFS | AUTHENTIFICATION BIDIRECTIONNELLE CRYPTOGRAPHIQUE

Le système d'information identifie et authentifie [*Affectation : dispositifs particuliers ou types de dispositifs définis par l'organisation*] avant d'établir une connexion [*Sélection (une ou plusieurs) : locale, à distance, réseau*] utilisant l'authentification bidirectionnelle reposant sur la cryptographie.

Conseils supplémentaires sur l'amélioration : Une connexion locale est toute connexion à un dispositif communiquant sans utiliser de réseau. Une connexion réseau est toute connexion à un dispositif qui communique au moyen d'un réseau (p. ex. un réseau local ou étendu et Internet). Une connexion à distance est toute connexion à un dispositif qui communique par un réseau externe (p. ex. Internet). L'authentification bidirectionnelle offre des mesures de protection plus robustes afin de valider l'identité d'autres dispositifs pour les connexions comportant un risque plus élevé (p. ex. les connexions à distance). Contrôles connexes : SC-8, SC-12, SC-13.

(2) IDENTIFICATION ET AUTHENTIFICATION DES DISPOSITIFS | AUTHENTIFICATION BIDIRECTIONNELLE CRYPTOGRAPHIQUE DU RÉSEAU

[Annulé : Intégré au contrôle IA-3 (1)]

(3) IDENTIFICATION ET AUTHENTIFICATION DES DISPOSITIFS | ATTRIBUTION DYNAMIQUE DES ADRESSES

(a) L'organisation normalise l'information de location de l'attribution dynamique d'adresses ainsi que la durée de la location attribuée aux dispositifs conformément à [*Affectation : information sur la location et durée de la location définies par l'organisation*];

(b) L'organisation vérifie l'information de location lorsqu'elle est attribuée à un dispositif.

Conseils supplémentaires sur l'amélioration : Un exemple typique d'attribution d'adresse dynamique pour les dispositifs est un client DHCP qui obtient une location d'adresse IP auprès d'un serveur DHCP. Contrôles connexes : AU-2, AU-3, AU-6, AU-12.

(4) IDENTIFICATION ET AUTHENTIFICATION DES DISPOSITIFS | ATTESTATION DES DISPOSITIFS

L'organisation doit veiller à ce que l'identification et à l'authentification des dispositifs appuyée sur l'attestation soit traité au moyen [*Affectation : processus de gestion des configurations défini par l'organisation*].

Conseils supplémentaires sur l'amélioration : L'attestation des dispositifs signifie l'identification et l'authentification d'un dispositif en fonction de sa configuration et de son état d'exploitation connu, lesquels peuvent être déterminés au moyen d'un hachage cryptographique du dispositif. Si l'attestation d'un dispositif est le mode d'identification et d'authentification, il est important d'appliquer les correctifs et d'effectuer les mises à niveaux du dispositif au moyen d'un processus de gestion des configurations pour assurer que l'application de correctifs et les mises à niveaux soient effectuées de manière sûre et sans perturber l'identification et l'authentification des autres dispositifs.

Références :

Aucune

IA-4 GESTION DES IDENTIFICATEURS

Contrôle :

(A) L'organisation gère les identificateurs des systèmes d'information en obtenant l'autorisation d'attribuer un identificateur à une personne, un groupe, un rôle ou un dispositif auprès [*Affectation : employés ou rôles définis par l'organisation*].

(B) L'organisation gère les identificateurs du système d'information en sélectionnant un identificateur qui identifie l'utilisateur, le groupe, le rôle ou le dispositif.

(C) L'organisation gère les identificateurs du système d'information en attribuant un identificateur à la personne, au groupe, au rôle ou au dispositif.

(D) L'organisation gère les identificateurs du système d'information en prévenant la réutilisation d'identificateurs pendant [*Affectation : durée définie par l'organisation*].

(E) L'organisation gère les identificateurs du système d'identification en désactivant les identificateurs après [*Affectation : période d'inactivité définie par l'organisation*].

Conseils supplémentaires : Les identificateurs de dispositif courants comprennent, entre autres, les adresses MAC ou IP, ou les identificateurs à jeton particuliers à un dispositif. La gestion des identificateurs de personnes ne s'applique pas aux comptes partagés du système d'information (p. ex. comptes d'invité et anonymes). En général, les identificateurs de personnes sont les noms d'utilisateurs des comptes du système d'information qu'on leur a attribués. Dans cette situation, les activités de gestion de compte d'AC -2 utilisent les noms de comptes fournis par IA-4. Ce contrôle traite également des identificateurs de personnes non nécessairement associés à des comptes du système d'information (p. ex. les identificateurs utilisés dans des bases de données de contrôle de la sécurité physique consultées par des systèmes de lecture de cartes aux fins d'accès aux systèmes d'information). La prévention de la réutilisation d'identificateurs suppose la prévention de l'attribution d'identificateurs de personnes, de groupes, de rôles ou de dispositifs déjà utilisés à d'autres personnes, groupes, rôles ou dispositifs. Contrôles connexes : AC-2, IA-2, IA-3, IA-5, IA-8, SC-37.

Améliorations du contrôle :

(1) GESTION DES IDENTIFICATEURS | INTERDICTION DE L'UTILISATION D'IDENTIFICATEURS DE COMPTE COMME IDENTIFICATEURS PUBLICS

L'organisation interdit l'utilisation d'identificateurs de compte du système d'information pareils aux identificateurs publics pour les comptes de courrier électronique personnels.

Conseils supplémentaires pour l'amélioration : Il est plus difficile pour les adversaires de deviner les identificateurs des utilisateurs utilisés pour les systèmes d'information organisationnels lorsqu'une

organisation interdit l'utilisation d'identificateurs de compte pour les systèmes d'information pareils à certains identificateurs publics tels que les sections d'identificateurs personnels des adresses de courriel. Contrôle connexe : AT-2.

(2) GESTION DES IDENTIFICATEURS | AUTORISATION DU SUPERVISEUR

L'organisation exige que le processus d'inscription requis pour l'obtention d'un identificateur personnel comprenne l'autorisation d'un superviseur.

(3) GESTION DES IDENTIFICATEURS | DIVERSES FORMES DE CERTIFICATION

L'organisation exige plusieurs formes de certification d'identification individuelle, dont notamment la présentation à l'autorité d'enregistrement d'un document probant ou d'une combinaison de documents et de données biométriques.

Conseils supplémentaires sur l'amélioration : L'obligation d'utiliser plus d'une forme d'identification réduit le risque qu'une personne souhaitant établir une identité utilise une forme d'identification frauduleuse, ou du moins, elle complexifie la tâche des adversaires potentiels.

(4) GESTION DES IDENTIFICATEURS | DÉTERMINATION DE L'ÉTAT D'UN UTILISATEUR

L'organisation gère les identificateurs personnels en identifiant de façon unique chaque personne comme [*Affectation : caractéristique définie par l'organisation déterminant le statut de la personne*].

Conseils supplémentaires sur l'amélioration : Les caractéristiques permettant de déterminer le statut de personnes comprennent notamment le statut d'entrepreneur ou de ressortissant étranger. Il est possible, en déterminant le statut de personnes au moyen de caractéristiques précises, d'obtenir plus d'information au sujet des personnes avec qui les employés d'une organisation communiquent. Il pourrait, par exemple, être utile pour un fonctionnaire de savoir qu'un des destinataires d'un courriel est un entrepreneur. Contrôle connexe : AT-2.

(5) GESTION DES IDENTIFICATEURS | GESTION DYNAMIQUE

Le système d'information gère de manière dynamique les identificateurs.

Conseils supplémentaires sur l'amélioration : Contrairement aux approches conventionnelles d'identification qui supposent des comptes statiques pour les utilisateurs préenregistrés, plusieurs systèmes d'information distribués, y compris les architectures orientées services, dépendent de l'identification en temps réel des entités inconnues. Dans ces cas, les organisations prévoient l'établissement dynamique d'identificateurs. Il est essentiel de pouvoir compter sur des relations de confiance préétablies et des mécanismes dotés de pouvoirs appropriés pour valider les identités et justificatifs connexes. Contrôle connexe : AC-16.

(6) GESTION DES IDENTIFICATEURS | GESTION INTERORGANISATIONNELLE

L'organisation collabore avec [*Affectation : organisations externes définies par l'organisme*] aux fins de gestion interorganisationnelle des identificateurs.

Conseils supplémentaires sur l'amélioration : La gestion interorganisationnelle d'identificateurs permet aux organisations d'identifier adéquatement des personnes, des groupes, des rôles ou des dispositifs lorsqu'elles mènent des activités interorganisationnelles concernant le traitement, le stockage ou la transmission d'information.

(7) GESTION DES IDENTIFICATEURS | INSCRIPTION EN PERSONNE

L'organisation exige que la demande d'attribution d'un identificateur personnel soit présentée en personne devant une autorité d'enregistrement désignée.

Conseils supplémentaires sur l'amélioration : L'inscription en personne réduit la possibilité d'émission d'identificateurs frauduleux puisqu'elle exige la présence physique de personnes et une interaction en personne avec les autorités d'enregistrement désignées.

Références :

Aucune

IA-5 GESTION DES AUTHENTIFIANTS

Contrôle :

(A) L'organisation gère les authentifiants du système d'information en vérifiant, au moment de la distribution initiale d'un authentifiant, l'identité de la personne, du groupe, du rôle ou du dispositif recevant l'authentifiant.

(B) L'organisation gère les authentifiants du système d'information en établissant le contenu initial des authentifiants définis par l'organisation.

(C) L'organisation gère les authentifiants du système d'information en s'assurant que le mécanisme d'authentification est suffisamment robuste pour l'utilisation prévue.

(D) L'organisation gère les authentifiants du système d'information en établissant et mettant en œuvre les procédures administratives nécessaires à la distribution initiale des authentifiants, aux authentifiants perdus, compromis ou endommagés et à la révocation des authentifiants.

(E) L'organisation gère les authentifiants du système d'information en modifiant le contenu par défaut des authentifiants avant l'installation des systèmes d'information.

(F) L'organisation gère les authentifiants du système d'information en établissant les restrictions minimales et maximales de durée et les conditions de réutilisation des authentifiants.

(G) L'organisation gère les authentifiants du système d'information en modifiant ou actualisant les authentifiants [*Affectation : durée définie par l'organisation selon le type d'authentifiant*].

(H) L'organisation gère les authentifiants du système d'information en protégeant le contenu de l'authentifiant contre toute divulgation et modification non autorisées.

(I) L'organisation gère les authentifiants du système d'information en exigeant des personnes et des dispositifs qu'ils appliquent des mesures spécifiques de protection de la sécurité de sorte à protéger les authentifiants.

(J) L'organisation gère les authentifiants du système d'information en modifiant les authentifiants pour les comptes de groupes ou de rôles lorsque les membres de ceux-ci changent.

Conseils supplémentaires : Les authentifiants de personnes comprennent notamment les mots de passe, les jetons, les données biométriques, les certificats d'infrastructure à clé publique (ICP) et les cartes d'accès. Le contenu initial de l'authentifiant est le contenu réel (p. ex. le mot de passe initial) et non les exigences relatives au contenu (p. ex. la longueur minimale du mot de passe). Les développeurs envoient fréquemment les composants du système d'information avec les justificatifs d'authentification par défaut du fabricant pour permettre l'installation et la configuration initiale du composant. Ces justificatifs sont souvent bien connus et peuvent être facilement découverts, ce qui pose un risque important à la sécurité. Les exigences de protection des authentifiants de personnes peuvent être appliquées par les contrôles PL-4 ou PS-6 pour les authentifiants qui se trouvent dans la possession de personnes et par les contrôles AC-3, AC-6 et SC-28 pour ceux qui sont stockés dans les systèmes d'information organisationnels (p. ex. mots de passe stockés sous forme hachée ou chiffrée, fichiers contenant des mots de passe hachés ou chiffrés accessibles à l'aide de privilèges d'administrateurs). Les systèmes d'information prennent en charge la gestion des authentifiants de personnes en fonction des paramètres et des restrictions définis par l'organisation pour différentes caractéristiques d'authentifiants, dont entre autres : la longueur minimale et la composition des mots de passe, la fenêtre de validation des jetons à utilisation unique et le nombre de rejets permis durant le stade de vérification d'une authentification biométrique. Il est possible de mettre en œuvre des mesures de protection des authentifiants précises, dont notamment le maintien de la

possession des authentifiants personnels, l'interdiction de prêter ou de partager les authentifiants avec d'autres personnes et le signalement immédiat des authentifiants perdus, volés ou compromis. La gestion des authentifiants comprend l'émission puis la révocation, lorsque ceux-ci ne sont plus requis, des authentifiants utilisés pour un accès temporaire (p. ex. pour la maintenance à distance). Les authentifiants de dispositif comprennent notamment les certificats et les mots de passe. Contrôles connexes : AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS-5, PS-6, SC-12, SC-13, SC-17, SC-28.

Améliorations du contrôle :

(1) GESTION DES AUTHENTIFIANTS | AUTHENTIFCATION FONDÉE SUR UN MOT DE PASSE

(a) Pour l'authentification fondée sur le mot de passe, le système d'information applique un mot de passe dont la complexité minimale est la suivante [*Affectation : exigences définies par l'organisation concernant la sensibilité à la casse, le nombre de caractères, la combinaison minuscules-majuscules, les lettres minuscules, les chiffres et les caractères spéciaux, y compris les exigences minimales pour chaque type*].

(b) Pour l'authentification fondée sur le mot de passe, le système d'information exige la modification d'au moins [*Affectation : nombre défini par l'organisation*] caractères lors de la création de nouveaux mots de passe.

(c) Pour l'authentification fondée sur le mot de passe, le système d'information ne stocke et ne transmet que les mots de passe protégés par la cryptographie.

(d) Pour l'authentification fondée sur le mot de passe, le système d'information applique les restrictions minimales et maximales de durée des mots de passe, soit [*Affectation : nombre défini par l'organisation pour la durée minimale ou maximale*].

(e) Pour l'authentification fondée sur le mot de passe, le système d'information interdit la réutilisation des mots de passe pendant [*Affectation : nombre défini par l'organisation*] générations.

(f) Pour l'authentification fondée sur le mot de passe, le système d'information permet l'utilisation d'un mot de passe temporaire servant à l'ouverture d'une session pourvu que celui-ci soit changé immédiatement à un mot de passe permanent après l'ouverture de session au moyen du mot de passe temporaire.

Conseils supplémentaires sur l'amélioration : Ce contrôle s'applique aux authentifications à facteur unique de personnes utilisant un mot de passe à titre d'authentifiant personnel ou de groupe. De plus, il s'applique lorsque le mot de passe est utilisé dans le cadre d'un authentifiant multifactoriel. Cette amélioration du contrôle ne s'applique pas lorsque les mots de passe servent à déverrouiller les authentifiants matériels (p. ex. les cartes de vérification de l'identité d'une personne). L'application de ces mécanismes de mot de passe pourrait ne pas satisfaire à toutes les exigences de l'amélioration. Les mots de passe protégés par la cryptographie comprennent notamment les versions chiffrées de mots de passe et le hachage cryptographique en sens unique de mots de passe. Le nombre de caractères modifiés signifie le nombre de modifications requises du nombre total de places dans le mot de passe actuel. Les restrictions de durée de vie des mots de passe ne s'appliquent pas aux mots de passe temporaires. Pour atténuer les attaques exhaustives contre les mots de passe, les organisations peuvent considérer le salage des mots de passe. Contrôle connexe : IA-6.

(2) GESTION DES AUTHENTIFIANTS | AUTHENTIFICATION FONDÉE SUR L'ICP

(a) Pour l'authentification fondée sur l'ICP, le système d'information valide les certifications en créant un chemin de certification avec l'information d'état vers un point d'ancrage de confiance autorisé. Il vérifie aussi l'information d'état des certificats.

(b) Pour l'authentification fondée sur l'ICP, le système d'information applique une politique d'accès autorisé à la clé privée correspondante.

(c) Pour l'authentification fondée sur l'ICP, le système d'information associe l'identité authentifiée au compte d'une personne ou d'un groupe.

(d) Pour l'authentification fondée sur l'ICP, le système d'information utilise une mémoire cache locale de données de révocation afin de prendre en charge la découverte et la validation de chemins au cas où il devenait impossible d'accéder à l'information de révocation au moyen du réseau.

Conseils supplémentaires sur l'amélioration : L'information d'état pour les chemins de certification comprend, par exemple, les listes de certificats révoqués ou les réponses du protocole OCSP *(Online Certificate Status Protocol*). La validation des certificats pour les cartes PIV comprend la création et la vérification d'un chemin de certification vers le point d'ancrage Common Policy Root, y compris le traitement des politiques de certification. Contrôle connexe : IA-6.

(3) GESTION DES AUTHENTIFIANTS | ENREGISTREMENT EN PERSONNE OU PAR L'INTERMÉDIAIRE D'UN TIERS DE CONFIANCE

L'organisation exige que le processus de demande de [*Affectation : types d'authentifiant ou authentifiants spécifiques définis par l'organisation*] soit effectué [*Affectation : en personne; par une tierce partie de confiance*] auprès [*Affectation : autorité d'enregistrement définie par l'organisation*] avec l'autorisation [*Affectation : employé ou rôle défini par l'organisation*].

(4) GESTION DES AUTHENTIFIANTS | SOUTIEN AUTOMATISÉ AUX FINS DE DÉTERMINATION DE LA ROBUSTESSE DU MOT DE PASSE

L'organisation utilise des outils automatisés pour déterminer si les authentifiants sont suffisamment robustes pour satisfaire [*Affectation : exigences définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle concerne principalement la création de mots de passe robustes et les caractéristiques de tels mots de passe (p. ex. la complexité) avant leur utilisation. L'application de cette mesure d'amélioration est effectuée par les systèmes d'information organisationnels dans IA-5 (1). Contrôles connexes : CA-2, CA-7, RA-5.

(5) GESTION DES AUTHENTIFIANTS | CHANGEMENT DES AUTHENTIFIANTS PAR DÉFAUT AVANT LA LIVRAISON

L'organisation exige des développeurs et des installateurs de composants de systèmes d'information qu'ils fournissent des authentifiants uniques ou qu'ils changent les authentifiants par défaut avant la livraison/l'installation.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle élargit l'exigence selon laquelle les organisations doivent modifier les authentifiants par défaut au moment de l'installation du système d'information en exigeant des développeurs et des installateurs qu'ils fournissent des authentifiants uniques ou qu'ils modifient les authentifiants par défaut des composants du système avant leur livraison et installation. Toutefois, cette amélioration de contrôle ne s'applique généralement pas aux développeurs de produits de technologie de l'information commerciaux. L'exigence concernant les authentifiants uniques peut être ajoutée aux documents d'acquisition préparés par les organisations au moment de l'acquisition de systèmes d'information ou de composants de ceux-ci.

(6) GESTION DES AUTHENTIFIANTS | PROTECTION DES AUTHENTIFIANTS

L'organisation protège les authentifiants au niveau de sécurité qui correspond à la catégorie de sécurité de l'information à laquelle l'authentifiant permet l'accès.

Conseils supplémentaires sur l'amélioration : Les authentifiants permettant l'accès aux systèmes sont protégés au niveau de sécurité de la catégorie de classification de sécurité de l'information la plus élevée dans les systèmes d'information contenant plusieurs catégories de sécurité de l'information sans séparation fiable physique ou logique entre celles-ci.

(7) GESTION DES AUTHENTIFIANTS | AUCUN AUTHENTIFIANT STATIQUE INTÉGRÉ NON CHIFFRÉ

L'organisation s'assure que des authentifiants statiques non chiffrés ne sont pas intégrés à des applications ou à des scripts d'accès, ni activés par des touches de fonction.

Conseils supplémentaires sur l'amélioration : Les organisations doivent prendre soin de déterminer si les authentifiants intégrés ou stockés sont chiffrés ou non. Si les authentifiants sont utilisés de la manière

qu'ils sont stockés, l'on considère que les représentations sont des authentifiants non chiffrés, peu importe si les représentations sont des versions chiffrées d'autre chose (p. ex. un mot de passe).

(8) GESTION DES AUTHENTIFIANTS | COMPTES MULTIPLES DES SYSTÈMES D'INFORMATION

L'organisation met en œuvre [*Affectation : mesures de protection de la sécurité définies par l'organisation*] pour gérer le risque de compromission que posent les utilisateurs qui possèdent des comptes dans plusieurs systèmes d'information.

Conseils supplémentaires sur l'amélioration : Si les utilisateurs ont des comptes dans plusieurs systèmes d'information et utilisent les mêmes authentifiants, la compromission d'un compte pourrait mener à la compromission des autres comptes. Les solutions de rechange possibles comprennent notamment les suivantes : (1) l'utilisation de différents authentifiants sur chaque système; (2) l'utilisation d'un mécanisme quelconque d'ouverture de session unique; (3) l'utilisation de mots de passe à usage unique sur tous les systèmes.

(9) GESTION DES AUTHENTIFIANTS | GESTION INTERORGANISATIONNELLE DES JUSTIFICATIFS

L'organisation collabore avec [*Affectation : organisations externes définies par l'organisme*] aux fins de gestion interorganisationnelle des justificatifs.

Conseils supplémentaires sur l'amélioration : La gestion de justificatifs interorganisationnelle permet aux organisations d'authentifier adéquatement des personnes, des groupes, des rôles ou des dispositifs lorsqu'elles mènent des activités interorganisationnelles concernant le traitement, le stockage ou la transmission d'information.

(10) GESTION DES AUTHENTIFIANTS | ASSOCIATION DYNAMIQUE DE JUSTIFICATIFS

Le système d'information fournit des identités de manière dynamique.

Conseils supplémentaires sur l'amélioration : L'authentification exige une liaison quelconque entre une identité et l'authentifiant utilisé pour confirmer l'identité. Dans les approches classiques, la liaison est établie en fournissant au préalable l'identité et l'authentifiant au système d'information. La liaison entre un nom d'utilisateur (c.-à-d. l'identité) et un mot de passe (c.-à-d. l'authentifiant), par exemple, est réalisée en fournissant l'identité et l'authentifiant au système d'information comme une paire. Les nouvelles techniques d'authentification permettent d'établir la liaison entre l'identité et l'authentifiant à l'extérieur du système d'information. Par exemple, l'identité et l'authentifiant des justificatifs de cartes à puce sont liés sur la carte. Les systèmes d'information peuvent se servir de ces justificatifs pour authentifier les identités qui n'ont pas été fournies au préalable, et fournir l'identité de manière dynamique après l'authentification. Dans ces situations, les organisations peuvent anticiper la fourniture dynamique d'identités. Il est essentiel de pouvoir compter sur des relations de confiance préétablies et des mécanismes dotés de pouvoirs appropriés pour valider les identités et justificatifs connexes.

(11) GESTION DES AUTHENTIFIANTS | AUTHENTIFICATION PAR JETON MATÉRIEL

Pour l'authentification par jeton matériel, le système d'information utilise des mécanismes qui répondent [*Affectation : exigences en matière de qualité des jetons définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : L'authentification par jeton matériel signifie habituellement l'utilisation de jetons d'ICP tels que la carte PIV (*Personal Identity Verification*) du gouvernement américain. Les organisations définissent certaines exigences précises pour les jetons, dont notamment la compatibilité à une ICP en particulier.

(12) GESTION DES AUTHENTIFIANTS | AUTHENTIFICATION BIOMÉTRIQUE

Pour l'authentification fondée sur la biométrie, le système d'information utilise des mécanismes qui répondent [*Affectation : exigences en matière de qualité de la biométrie définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Contrairement à l'authentification fondée sur les mots de passe, laquelle repose sur la correspondance exacte entre les mots de passe entrés par les utilisateurs et les mots de passe stockés, la correspondance exacte ne figure pas dans l'authentification par biométrie. Dépendant du type de biométrie et du mécanisme de collecte, il peut y avoir certaines différences entre les données biométriques présentées et les données biométriques stockées aux fins de comparaison. Il est

probable que la comparaison de ces données donne lieu à de faux positifs et de faux négatifs. Lorsque les taux de fausses acceptations et de faux refus sont égaux, il s'agit du taux critique. Les exigences de qualité en matière de biométrie comprennent notamment les taux critiques acceptables puisque ceux-ci reflètent l'exactitude de la biométrie.

(13) GESTION DES AUTHENTIFIANTS | ÉCHÉANCE DES AUTHENTIFIANTS EN MÉMOIRE CACHE

Le système d'information interdit l'utilisation d'authentifiants en mémoire cache après [*Affectation : délai défini par l'organisation*].

(14) GESTION DES AUTHENTIFIANTS | GESTION DU CONTENU DES MAGASINS DE CONFIANCE D'ICP

Pour l'authentification fondée sur l'ICP, l'organisation entière utilise une méthodologie de gestion du contenu des magasins de confiance d'ICP installés sur toutes les plateformes, y compris les réseaux, les systèmes d'exploitation, les navigateurs et les applications.

(15) GESTION DES AUTHENTIFIANTS | PRODUITS ET SERVICES APPROUVÉS PAR FICAM

Sans objet pour le GC.

Références :

CST, *ITSG-31, Guide sur l'authentification des utilisateurs pour les systèmes TI* [Référence 18].

IA-6 RÉINJECTION D'AUTHENTIFICATION

Contrôle :

(A) Le système d'information obscure les réinjections d'information durant le processus d'authentification afin de protéger l'information contre de possibles exploitations ou utilisations par des personnes non autorisées.

Conseils supplémentaires : Les réinjections des systèmes d'information ne fournissent aucune donnée qui permettrait à des personnes non autorisées de compromettre les mécanismes d'authentification. La menace (souvent nommée l'espionnage par-dessus l'épaule) peut être non négligeable pour certains types de systèmes d'information ou certains composants de systèmes d'information (p. ex. les ordinateurs de bureau et portatifs avec de gros moniteurs). Pour d'autres types de systèmes ou de composants, dont les dispositifs mobiles ayant des écrans de deux à quatre pouces, la menace est beaucoup moins importante. La réduction de la menace doit toutefois faire contrepoids à la susceptibilité aux erreurs de frappe étant donné la petite taille des claviers. Il est donc nécessaire de choisir un moyen d'obscurcir la réinjection d'authentification de manière appropriée. L'obscurcissement de la réinjection de l'information d'authentification comprend, entre autres, l'affichage d'astérisques lorsqu'un utilisateur entre son mot de passe dans un dispositif et l'affichage de l'information d'authentification pendant une très courte durée avant de l'obscurcir. Contrôle connexe : PE-18.

Améliorations du contrôle :

Aucune

Références :

Aucune

IA-7 AUTHENTIFICATION DES MODULES CRYPTOGRAPHIQUES

Contrôle :

(A) Le système d'information met en œuvre des mécanismes d'authentification auprès d'un module cryptographique qui satisfont aux lois du GC ainsi qu'aux politiques, aux directives et aux normes du SCT en matière d'authentification.

Conseils supplémentaires : Il pourrait être nécessaire d'intégrer des mécanismes d'authentification à un module cryptographique afin d'authentifier l'opérateur accédant au module ainsi que de vérifier si l'opérateur a le droit d'assumer le rôle demandé et d'effectuer des fonctions dans ce rôle. Contrôles connexes : SC-12 et SC-13.

Améliorations du contrôle :

Aucune

Références :

CST, *ITSA-11, Algorithmes cryptographiques approuvés par le CST pour la protection des renseignements protégés* [Référence 8].
CST, *ITSG-31, Guide sur l'authentification des utilisateurs pour les systèmes TI* [Référence 18].
CST, *ITSB-40A, Politique du gouvernement du Canada pour la protection de l'information classifiée à l'aide d'algorithmes Suite B* [Référence 28].
NIST, *FIPS 140-2, Security Requirements for Cryptographic Modules* [Référence 4].

IA-8 IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS NON ORGANISATIONNELS)

Contrôle :

(A) Le système d'information identifie de façon unique et authentifie les utilisateurs non organisationnels (ou les processus exécutés en leur nom).

Conseils supplémentaires : Les utilisateurs non organisationnels incluent les utilisateurs du système d'information autres que les utilisateurs organisationnels explicitement mentionnés dans le contrôle IA-2. Ces utilisateurs sont identifiés de façon unique et authentifiés pour tous les accès autres que ceux explicitement identifiés et documentés dans le contrôle AC-14. On peut exiger l'authentification des utilisateurs non organisationnels qui accèdent aux systèmes d'information du GC afin de protéger les renseignements fédéraux, exclusifs ou assujettis aux lois sur la protection des renseignements personnels (sauf les exceptions prévues pour les systèmes liés à la sécurité nationale). Les organisations se servent de l'évaluation des risques pour déterminer leurs besoins en authentification. Elles doivent considérer l'extensibilité, l'aspect pratique et la sécurité pour assurer un juste équilibre entre le besoin d'accéder facilement à l'information et aux systèmes d'information du GC et le besoin de se protéger et d'atténuer le risque adéquatement. L'IA-2 traite des exigences d'identification et d'authentification pour l'accès aux systèmes d'information par les utilisateurs organisationnels. Contrôles connexes : AC-2, AC -14, AC -17, AC -18, IA-2, IA-4, IA-5, MA-4, RA-3, SA-12, SC-8.

Améliorations du contrôle :

(1) IDENTIFICATION ET AUTHENTIFICATION | ACCEPTATION DES JUSTIFICATIFS DE VÉRIFICATION D'IDENTITÉ PERSONNELLE D'AUTRES ORGANISMES

Sans objet pour le GC.

(2) IDENTIFICATION ET AUTHENTIFICATION | ACCEPTATION DES JUSTIFICATIFS DE TIERCES PARTIES

Sans objet pour le GC.

(3) IDENTIFICATION ET AUTHENTIFICATION | UTILISATION DES PRODUITS HOMOLOGUÉS FICAM

Sans objet pour le GC.

(4) IDENTIFICATION ET AUTHENTIFICATION | UTILISATION DES PROFILS ÉMIS PAR FICAM

Sans objet pour le GC.

(5) IDENTIFICATION ET AUTHENTIFICATION | ACCEPTATION DES JUSTIFICATIFS PIV-I

Sans objet pour le GC.

(100) Conformément à la *Norme sur l'assurance de l'identité et des justificatifs* du SCT (y compris les annexes B et C) [Référence 60], l'organisation détermine les niveaux d'assurance de l'identité et des justificatifs requis, puis sélectionne les contrôles appropriés au moyen des niveaux d'assurance normalisés précisés dans l'Annexe B. Elle met ensuite en œuvre les exigences minimales pour établir un niveau d'assurance de l'identité précisée dans l'Annexe C.

Conseils supplémentaires sur l'amélioration : La *Norme sur l'assurance de l'identité et des justificatifs* du SCT [Référence 60] précise les exigences à respecter pour l'adoption, par une organisation, d'une méthodologie commune d'évaluation de leurs risques relativement à l'identité et aux justificatifs et pour la sélection de contrôles appropriés ou de dispositions visant à atténuer ces risques à l'aide d'un cadre des niveaux d'assurance normalisés. La norme est appuyée par la *Ligne directrice sur la définition des exigences en matière d'authentification* du SCT [Référence 61], et par la *Ligne directrice sur l'assurance de l'identité* du SCT [Référence 62]. Ces lignes directrices doivent être utilisées avec l'*ITSG-31, Guide sur l'authentification des utilisateurs pour les systèmes TI* [Référence 18] du CST.

Références :

CST, *ITSG-31, Guide sur l'authentification des utilisateurs pour les systèmes TI* [Référence 18].
SCT, *Norme sur l'assurance de l'identité et des justificatifs* [Référence 60].
SCT, *Ligne directrice sur la définition des exigences en matière d'authentification* [Référence 61].
SCT, *Ligne directrice sur l'assurance de l'identité* [Référence 62].

IA-9 IDENTIFICATION ET AUTHENTIFICATION DES SERVICES

Contrôle :

(A) L'organisation identifie et authentifie [*Affectation : services du système d'information définis par l'organisation*] au moyen [*Affectation : mesures de protection de sécurité définies par l'organisation*].

Conseils supplémentaires : Ce contrôle appuie les architectures orientées services et les autres approches d'architecture répartie exigeant l'identification et l'authentification des services de systèmes d'information. Les services externes sont souvent générés de manière dynamique pour de telles architectures. Les systèmes d'information doivent donc être en mesure de déterminer, de manière dynamique, si des fournisseurs externes et les services connexes sont authentiques. Les mesures de protection mises en œuvre par les systèmes d'information organisationnels visant à valider l'authenticité des fournisseurs et des services comprennent notamment la signature de code et d'information, les graphiques de provenance et les signatures électroniques indiquant ou incluant les sources des services.

Améliorations du contrôle :

(1) IDENTIFICATION ET AUTHENTIFICATION DES SERVICES | ÉCHANGE D'INFORMATION

L'organisation veille à ce que les fournisseurs de services reçoivent, valident et transmettent de l'information d'identification et d'authentification.

(2) IDENTIFICATION ET AUTHENTIFICATION DES SERVICES | TRANSMISSION DES DÉCISIONS

L'organisation veille à ce que les décisions concernant l'identification et l'authentification soient transmises entre [*Affectation : services définis par l'organisation*] et qu'elles soient conformes aux politiques organisationnelles.

Conseils supplémentaires sur l'amélioration : Il est possible, pour les architectures réparties (p. ex. les architectures orientées services), que les décisions concernant la validation des déclarations d'identification et d'authentification soient prises par des services distincts des services devant mettre en œuvre ces décisions. Dans de tels cas, il est nécessaire de fournir les décisions concernant l'identification et l'authentification (par opposition aux identifiants et au authentifiants comme tel) aux services devant mettre ces décisions en œuvre. Contrôle connexe : SC-8.

Références :

Aucune

IA-10 IDENTIFICATION ET AUTHENTIFICATION ADAPTIVES

Contrôle :

(A) L'organisation exige que les personnes accédant au système d'information utilisent [*Affectation : techniques ou mécanismes d'authentification supplémentaires définis par l'organisation*] pour certaines situations particulières, dont notamment [*Affectation : circonstances ou situations définies par l'organisation*].

Conseils supplémentaires : Les adversaires peuvent compromettre les mécanismes d'authentification de personnes pour ensuite tenter d'usurper l'identité d'utilisateurs légitimes. Cette situation pourrait se produire, peu importe les mécanismes d'authentification utilisés par les organisations. Pour résister à cette menace, les organisations peuvent utiliser des techniques et des mécanismes précis ou établir des protocoles visant à évaluer les comportements suspects (p. ex. les personnes accédant à de l'information à laquelle ils n'accèdent généralement pas dans le cadre de leurs fonctions, rôles ou responsabilités, les personnes accédant à un plus gros volume d'information que celui auquel elles accèdent habituellement et les personnes tentant d'accéder à de l'information en utilisant des adresses réseau suspectes). Lorsqu'une telle situation survient, c'est-à-dire lorsque des conditions établies au préalable sont présentes ou qu'un élément déclencheur est présent, les organisations peuvent exiger que certaines personnes fournissent de l'information d'authentification supplémentaire. Une autre application potentielle de l'identification et de l'authentification adaptatives est le renforcement des mécanismes selon le nombre et le type de dossiers faisant l'objet de la demande d'accès. Contrôles connexes : AU-6, SI-4.

Améliorations du contrôle :

Aucune

Références :

Aucune

IA-11 RÉAUTHENTIFICATION

Contrôle :

(A) L'organisation exige que les utilisateurs et les dispositifs effectuent une réauthentification dans les cas suivants : [*Affectation : circonstances ou situations exigeant une réauthentification définies par l'organisation*].

Conseils supplémentaires : En plus des exigences de réauthentification liées aux verrouillages de session, les organisations peuvent exiger la réauthentification de personnes ou de dispositifs dans d'autres situations, dont les

suivantes : (i) les changements d'authentfiants; (ii) les changements de rôles; (iii) les changements aux catégories de sécurité des systèmes d'information; (iv) au moment de l'exécution de fonctions privilégiées; (v) après un délai précisé; (vi) périodiquement. Contrôle connexe : AC-11.

Améliorations du contrôle :

Aucune

Références :

Aucune

3.8 FAMILLE : INTERVENTION EN CAS D'INCIDENT

CLASSE : OPÉRATIONNELLE

IR-1 POLITIQUE ET PROCÉDURES D'INTERVENTION EN CAS D'INCIDENT

Contrôle :

(A) L'organisation élabore et consigne, ainsi que diffuse [*Affectation : personnel ou rôles définis par l'organisation*] :

(a) une politique d'intervention en cas d'incident qui définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité;

(b) des procédures pour faciliter la mise en œuvre de la politique d'intervention en cas d'incident et des contrôles d'intervention en cas d'incidents connexes.

(B) L'organisation examine et met à jour :

(a) la politique d'intervention en cas d'incident tous les [*Affectation : fréquence définie par l'organisation*];

(b) les procédures d'intervention en cas d'incident tous les [*Affectation : fréquence définie par l'organisation*].

(AA) La politique et les procédures d'intervention en cas d'incident de l'organisation facilitent l'intégration de niveaux relevés de préparation durant les urgences et les situations de menace des TI élevées, conformément à la *Norme opérationnelle de sécurité - Niveaux de préparation des installations du gouvernement fédéral* [Référence 12] et à la *Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT* [Référence 7].

Conseils supplémentaires : Ce contrôle traite de la mise en place d'une politique et de procédures nécessaires à la mise en œuvre efficace de contrôles de sécurité particuliers et d'améliorations précises des contrôles pour la famille d'intervention en cas d'incident. La politique et les procédures tiennent compte des lois applicables du GC ainsi que des politiques, des directives et des normes du SCT. Les politiques et les procédures du programme de sécurité organisationnel peuvent rendre facultatives les politiques et procédures propres au système. La politique peut être intégrée à la politique générale sur la sécurité de l'information des organisations ou, inversement, elle peut être représentée par de multiples politiques compte tenu de la nature complexe de certaines organisations. Les procédures peuvent être déterminées pour le programme de sécurité général et pour des systèmes d'information particuliers, au besoin. La stratégie organisationnelle de gestion des risques est un facteur clé dans l'établissement de la politique et des procédures.

Améliorations du contrôle :

Aucune

Références :

SCT, *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* [Référence 7].
SCT, *Norme opérationnelle de sécurité – Niveaux de préparation des installations du gouvernement fédéral* [Référence 12].
SCT, *Norme de sécurité relative à l'organisation et l'administration* [Référence 13].

CST, ITSD-03A, Directive sur le contrôle du matériel COMSEC au sein du gouvernement du Canada [Référence 36].
SCT, Plan de gestion des incidents des technologies de l'information du gouvernement du Canada [Référence 67].

IR-2 FORMATION SUR LES INTERVENTIONS EN CAS D'INCIDENT

Contrôle :

(A) L'organisation offre une formation sur les interventions en cas d'incident aux utilisateurs des systèmes d'information. La formation est adaptée en fonction des rôles et des responsabilités assignés aux utilisateurs lors d'une intervention en cas d'incident, et ce dans un délai de [*Affectation : délai défini par l'organisation*] après leur affectation à ceux-ci.

(B) L'organisation offre une formation sur les interventions en cas d'incident aux utilisateurs des systèmes d'information adaptée à leurs rôles et responsabilités lorsque des changements aux systèmes d'information le justifient.

(C) L'organisation offre une formation sur les interventions en cas d'incident aux utilisateurs des systèmes d'information adaptée à leurs rôles et responsabilités tous les [*Affectation : fréquence définie par l'organisation*] par la suite.

Conseils supplémentaires : La formation sur les interventions en cas d'incident offerte par l'organisation correspond aux responsabilités et aux rôles assignés à son personnel de sorte à assurer un contenu et un niveau de détails appropriés. Par exemple, les utilisateurs ordinaires ont peut-être seulement besoin de savoir qui appeler ou comment reconnaître un incident sur le système d'information; les administrateurs du système pourraient avoir besoin d'une formation plus poussée sur le traitement de ces incidents ou sur la manière de remédier à ceux-ci; les intervenants en cas d'incident pourraient avoir besoin d'une formation plus précise sur l'informatique judiciaire, la production de rapports, la reprise du système et la restauration. La formation sur les interventions en cas d'incident comprend la formation des utilisateurs sur l'identification et le signalement des activités suspectes, à la fois de sources externes et internes. Contrôles connexes : AT-3, CP-3, IR-8.

Améliorations du contrôle :

(1) FORMATION SUR LES INTERVENTIONS EN CAS D'INCIDENT | SIMULATION D'ÉVÉNEMENTS

L'organisation intègre des événements simulés à la formation sur les interventions en cas d'incident pour permettre une intervention efficace du personnel en situation de crise.

(2) FORMATION SUR LES INTERVENTIONS EN CAS D'INCIDENT | ENVIRONNEMENTS DE FORMATION AUTOMATISÉS

L'organisation utilise des mécanismes automatisés pour créer un environnement de formation complète et plus réaliste.

Références :

Aucune

IR-3 TESTS ET EXERCICES RELATIFS AUX INTERVENTIONS EN CAS D'INCIDENT

Contrôle :

(A) L'organisation teste la capacité d'intervention en cas d'incident pour le système d'information [*Affectation : fréquence définie par l'organisation*] en utilisant [*Affectation : tests ou exercices définis par l'organisation*] pour déterminer l'efficacité des interventions en cas d'incident et documenter les résultats.

Conseils supplémentaires : Les organisations testent les capacités d'intervention en cas d'incident pour déterminer l'efficacité générale des capacités et pour déceler les faiblesses ou lacunes potentielles. Les tests d'intervention en cas d'incident comprennent, entre autres, l'utilisation de listes de contrôle, les exercices sur table, les simulations (en parallèle et en état d'arrêt complet) et les exercices exhaustifs. Les tests d'intervention en cas d'incident peuvent aussi inclure la détermination de l'incidence des interventions en cas d'incident sur les opérations organisationnelles (p. ex. une réduction de la capacité de la mission), les biens organisationnels et les personnes. Contrôles connexes : CP-4, IR-8.

Améliorations du contrôle :

(1) TESTS RELATIFS AUX INTERVENTIONS EN CAS D'INCIDENT | TESTS AUTOMATISÉS

L'organisation utilise des mécanismes automatisés pour tester ou vérifier plus en détail et plus efficacement la capacité d'intervention en cas d'incident.

Conseils supplémentaires sur l'amélioration : L'organisation utilise des mécanismes automatisés pour tester ou vérifier le plan d'urgence de manière plus détaillée et efficace : i) en assurant une couverture plus complète des situations d'urgence; ii) en sélectionnant des scénarios et des environnements de test plus réalistes; iii) en soumettant les systèmes d'information et les missions concernées à un volume de demandes élevé. Contrôle connexe : AT-2

(2) TESTS RELATIFS AUX INTERVENTIONS EN CAS D'INCIDENT | COORDINATION AVEC LES PLANS CONNEXES

L'organisation coordonne les tests d'intervention en cas d'incident avec les éléments organisationnels responsables des plans connexes.

Conseils supplémentaires sur l'amélioration : Les plans organisationnels connexes aux tests des interventions en cas d'incident comprennent les suivants : plans de continuité des activités, plans d'urgence, plans de reprise après sinistre, plans de continuité des opérations, plans des communications en temps de crise, plans de l'infrastructure essentielle et plans de mesures d'urgence pour les occupants.

Références :

Aucune

IR-4 TRAITEMENT DES INCIDENTS

Contrôle :

(A) L'organisation met de l'avant une capacité de traitement des incidents de sécurité qui inclut des activités de préparation, de détection et d'analyse, de confinement, d'éradication et de reprise.

(B) L'organisation coordonne les activités de traitement des incidents avec les activités de planification d'urgence.

(C) L'organisation intègre les leçons apprises découlant des activités de traitement aux procédures d'intervention en cas d'incident, à la formation et aux tests et exercices, et met en œuvre les changements qui en résultent comme il se doit.

Conseils supplémentaires : Les organisations reconnaissent que la capacité d'intervention en cas d'incident dépend des capacités des systèmes d'information organisationnels et des processus opérationnels et de mission pris en charge par ces systèmes. Ainsi, les organisations doivent tenir compte de l'intervention en cas d'incident lors de la définition, de la conception et du développement de processus opérationnels et de mission et des systèmes d'information. L'information liée aux incidents peut provenir d'une variété de sources qui comprennent, sans s'y limiter, la surveillance des vérifications, des réseaux et de l'accès physique, les rapports d'utilisateurs ou d'administrateurs et les incidents d'approvisionnement signalés. La capacité de gestion efficace des incidents comprend la coordination entre les nombreuses entités organisationnelles, dont notamment les

responsables des opérations et de la mission, les responsables des systèmes d'information, les responsables des autorisations, les ressources humaines, la sécurité physique et du personnel, les services juridiques, le personnel opérationnel, les bureaux d'acquisition et les responsables des risques. Contrôles connexes : AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

Améliorations du contrôle :

(1) TRAITEMENT DES INCIDENTS | PROCESSUS AUTOMATISÉS DE TRAITEMENT DES INCIDENTS

L'organisation utilise des mécanismes automatisés pour appuyer le processus de traitement des incidents.

Conseils supplémentaires sur l'amélioration : Les mécanismes automatisés appuyant les processus de traitement des incidents comprennent notamment les systèmes de gestion des incidents en ligne.

(2) TRAITEMENT DES INCIDENTS | RECONFIGURATION DYNAMIQUE

L'organisation intègre la reconfiguration dynamique [*Affectation : composants du système d'information définis par l'organisation*] à sa capacité d'intervention en cas d'incident.

Conseils supplémentaires sur l'amélioration : La reconfiguration dynamique comprend, par exemple, les modifications apportées à ce qui suit : règles du routeur, listes de contrôle d'accès, paramètres de système de détection ou de prévention d'intrusions, règles de filtrage pour les coupe-feux et les passerelles. Les organisations exécutent une reconfiguration dynamique de leurs systèmes d'information pour, entre autres, arrêter les attaques, rediriger les attaquants et isoler les composants de systèmes de sorte à limiter les dommages créés par les atteintes à la sécurité et par les compromissions. Les organisations incluent, dans la définition des capacités de reconfiguration, des délais pour la réalisation de la configuration des systèmes d'information qui tiennent compte du besoin possible d'une intervention rapide en vue de traiter efficacement des cybermenaces sophistiquées. Contrôles connexes : AC-24 AC-4, AC-16, CM-2, CM-3, CM-4.

(3) TRAITEMENT DES INCIDENTS | CONTINUITÉ DES OPÉRATIONS

L'organisation identifie [*Affectation : classes d'incident définies par l'organisation*] et [*Affectation : mesures d'intervention appropriées aux classes d'incident définies par l'organisation*] pour veiller à la continuité de ses missions et fonctions opérationnelles.

Conseils supplémentaires sur l'amélioration : Les classes d'incident comprennent, par exemple, les défectuosités dues aux erreurs ou aux omissions liées à la conception ou à la mise en œuvre, de même que les attaques malveillantes ciblées et non ciblées. Les mesures appropriées d'intervention en cas d'incident comprennent, par exemple, la dégradation progressive, l'arrêt du système d'information, le passage au mode manuel ou le recours à une technologie de secours qui permet de faire fonctionner le système différemment, l'emploi de mesures de déception, l'utilisation de flux d'information différents, ou l'exploitation du système dans un mode réservé aux situations d'attaque.

(4) TRAITEMENT DES INCIDENTS | CORRÉLATION DE L'INFORMATION

L'organisation établit une corrélation entre l'information sur les incidents et les interventions individuelles pour obtenir une perspective organisationnelle de la sensibilisation et des interventions en matière d'incident.

Conseils supplémentaires sur l'amélioration : Il est possible que la nature d'un événement de menace (p. ex. une cyberattaque hostile) fasse en sorte qu'il ne soit possible de le déceler qu'en rassemblant de l'information provenant de différentes sources, y compris divers rapports et procédures de production de rapports déterminés par les organisations.

(5) TRAITEMENT DES INCIDENTS | DÉSACTIVATION AUTOMATIQUE DES SYSTÈMES D'INFORMATION

L'organisation met en œuvre une capacité configurable pour désactiver automatiquement le système d'information dans l'éventualité où l'organisation détectait [*Affectation : atteintes à la sécurité définies par l'organisation*].

(6) TRAITEMENT DES INCIDENTS | MENACES INTERNES - CAPACITÉS PARTICULIÈRES

L'organisation met en œuvre une capacité de traitement des incidents pour les menaces internes.

Conseils supplémentaires sur l'amélioration : Même si plusieurs organisations traitent des incidents de menace interne dans le cadre de leur capacité organisationnelle d'intervention en cas d'incident, cette amélioration du contrôle met l'accent sur ce type particulier de menace et souligne le besoin de mettre en place des capacités précises de traitement des incidents (définies par les organisations) qui leur permettront d'intervenir de manière appropriée et opportune.

(7) TRAITEMENT DES INCIDENTS | MENACES INTERNES - COORDINATION AU SEIN DE L'ORGANISATION

L'organisation coordonne sa capacité de traitement d'incidents liés à la menace interne à l'échelle [*Affectation : composants ou éléments de l'organisation définis par l'organisation*].

Conseils supplémentaires sur l'amélioration : L'efficacité du traitement d'incidents liés aux cybermenaces (y compris la préparation, la détection et l'analyse, le confinement, l'éradication et la reprise) exige une étroite coordination entre divers composants ou éléments de l'organisation afin d'être efficace. Ces composants ou éléments comprennent, entre autres, les responsables organisationnels et de la mission, les responsables des systèmes d'information, les ressources humaines, les responsables de l'acquisition, les responsables de la sécurité physique et du personnel, le personnel des opérations et le responsable de la gestion des risques. De plus, les organisations pourraient faire appel aux organismes fédéraux, provinciaux et municipaux responsables de l'application de la loi afin d'obtenir du soutien.

(8) TRAITEMENT DES INCIDENTS | CORRÉLATION AVEC LES ORGANISATIONS EXTERNES

L'organisation assure une coordination avec [*Affectation : organisations externes définies par l'organisation*] en vue d'échanger [*Affectation : information liée à un incident définie par l'organisation*] de sorte à obtenir une représentation interorganisationnelle de la sensibilisation à l'incident et d'intervenir plus efficacement après celui-ci.

Conseils supplémentaires sur l'amélioration : D'importants avantages peuvent découler de l'échange d'information liée à un incident avec des organisations externes, dont entre autres les partenaires opérationnels et de la mission, les partenaires de la coalition et militaires, les clients et les développeurs à plusieurs niveaux. La coordination interorganisationnelle à l'égard du traitement des incidents peut constituer une capacité de gestion du risque très importante. Cette capacité permet aux organisations de tirer profit d'informations essentielles provenant de diverses sources de manière à intervenir efficacement en cas d'incident lié à la sécurité de l'information et pouvant avoir une incidence sur les opérations, les biens et les employés de ces organisations.

(9) TRAITEMENT DES INCIDENTS | CAPACITÉ D'INTERVENTION DYNAMIQUE

L'organisation utilise [*Affectation : capacités d'intervention dynamique définies par l'organisation*] de sorte à intervenir en cas d'incident de sécurité.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle traite du déploiement, en temps opportun, de nouvelles capacités ou de capacités de rechange afin d'intervenir en cas d'incident de sécurité (p. ex. les actions d'adversaires durant une cyberattaque hostile). Ces capacités comprennent celles qui sont mises en œuvre au niveau des processus opérationnels et de la mission (p. ex. déclencher les processus opérationnels et de mission de remplacement) et au niveau des systèmes d'information. Contrôle connexe : CP-10.

(10) TRAITEMENT DES INCIDENTS | COORDINATION RELATIVE À LA CHAÎNE D'APPROVISIONNEMENT

L'organisation coordonne les activités d'intervention en cas d'incident touchant aux événements d'approvisionnement avec d'autres organisations dans la chaîne d'approvisionnement.

Conseils supplémentaires sur l'amélioration : Les organisations qui participent aux activités d'approvisionnement comprennent notamment les développeurs de produits et de systèmes, les intégrateurs, les fabricants, les emballeurs, les assembleurs, les distributeurs, les fournisseurs et les revendeurs. Les incidents d'approvisionnement incluent entre autres les compromissions et les atteintes liées aux composants des systèmes d'information, des produits de technologie de l'information, des processus de développement, du personnel de développement, des processus de distribution et des installations d'entreposage.

Références :

CST, *ITSD-03A, Directive en matière de sécurité des TI sur le contrôle du matériel COMSEC au sein du gouvernement du Canada* [Référence 36].
SCT, *Plan de gestion des incidents des technologies de l'information du gouvernement du Canada* [Référence 67].

IR-5 SURVEILLANCE DES INCIDENTS

Contrôle :

(A) L'organisation suit et documente les incidents de sécurité liés au système d'information.

Conseils supplémentaires : La consignation des incidents de sécurité du système d'information comprend, entre autres, la tenue de dossiers au sujet de chaque incident, de l'état des incidents et d'autres informations pertinentes à l'informatique judiciaire, ainsi que l'évaluation des détails, des tendances et du traitement de l'incident. L'information relative à un incident est accessible auprès de diverses sources dont notamment les rapports d'incidents, les équipes d'intervention en cas d'incident, la surveillance des vérifications, la surveillance des réseaux, la surveillance des accès physiques et les rapports d'utilisateurs et d'administrateurs. Contrôles connexes : AU-6, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

Améliorations du contrôle :

(1) SURVEILLANCE DES INCIDENTS | SUIVI AUTOMATISÉ / COLLECTE DE DONNÉES / ANALYSE

L'organisation utilise des mécanismes automatisés lui permettant de suivre les incidents de sécurité et facilitant la collecte et l'analyse de l'information liée à un incident.

Conseils supplémentaires sur l'amélioration : Les mécanismes automatisés visant à suivre les incidents de sécurité et à collecter et analyser l'information liée aux incidents de sécurité comprennent notamment les centres d'intervention aux incidents informatiques et les autres bases de données électroniques d'incidents. Contrôles connexes : AU-7, IR-4.

Références :

SCT, *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* [Référence 7].
SCT, *Plan de gestion des incidents des technologies de l'information du gouvernement du Canada* [Référence 67].

IR-6 SIGNALEMENT DES INCIDENTS

Contrôle :

(A) L'organisation exige que les employés signalent les incidents de sécurité soupçonnés auprès de la capacité d'intervention en cas d'incident organisationnelle [*Affectation : délai défini par l'organisation*].

(B) L'organisation transmet l'information relative à l'incident de sécurité [*Affectation : autorités définies par l'organisation*].

Conseils supplémentaires : Ce contrôle vise à tenir compte à la fois des exigences spécifiques de l'organisation en matière de signalement des incidents et des exigences officielles de signalement des incidents pour les ministères et les organismes du GC ainsi que pour leurs organisations auxiliaires. Les incidents de sécurité soupçonnés comprennent notamment la réception de courriels suspects susceptibles de contenir un programme malveillant. Les types d'incident de sécurité signalés, le contenu et les échéances de production des rapports, de même que la liste des autorités responsables du signalement doivent être conformes aux lois du GC et aux politiques, directives et normes applicables du SCT. Contrôles connexes : IR-4, IR-5, IR-8.

Améliorations du contrôle :

(1) SIGNALEMENT DES INCIDENTS | RAPPORTS AUTOMATISÉS

L'organisation utilise des mécanismes automatisés pour faciliter le signalement des incidents de sécurité.

Conseils supplémentaires sur l'amélioration : Contrôle connexe : IR -7.

(2) SIGNALEMENT DES INCIDENTS | VULNÉRABILITÉS LIÉES AUX INCIDENTS

L'organisation signale [*Affectation : personnes ou rôles définis par l'organisation*] toute vulnérabilité du système d'information associée aux incidents signalés.

(3) SIGNALEMENT DES INCIDENTS | COORDINATION AVEC LA CHAÎNE D'APPROVISIONNEMENT

L'organisation communique l'information sur les incidents de sécurité aux organisations dans la chaîne d'approvisionnement des systèmes d'information ou des composants de systèmes d'information touchés par l'incident.

Conseils supplémentaires sur l'amélioration : Les organisations participant aux activités de la chaîne d'approvisionnement comprennent entre autres les développeurs des produits ou des systèmes et les intégrateurs, les fabricants, les emballeurs, les assembleurs, les distributeurs, les fournisseurs et les revendeurs de ceux-ci. Les incidents liés à la chaîne d'approvisionnement comprennent notamment les compromissions des composants des systèmes d'information, des produits de technologie de l'information, des processus et du personnel de développement, des processus de distribution et des installations d'entreposage, ainsi que les atteintes à ceux-ci. Les organisations doivent déterminer l'information qu'il est approprier d'échanger compte tenu de la valeur ajoutée par les organisations externes et des risques possibles de diffusion d'information sensible aux organisations externes n'ayant pas encore fait preuve de confiance.

Références :

CST, *ITSD-03A, Directive en matière de sécurité des TI sur le contrôle du matériel COMSEC au sein du gouvernement du Canada* [Référence 36].
SCT, *Plan de gestion des incidents des technologies de l'information du gouvernement du Canada* [Référence 67].

IR-7 ASSISTANCE EN CAS D'INCIDENT

Contrôle :

(A) L'organisation fournit une ressource de soutien qui fait partie intégrante de la capacité d'intervention en cas d'incident de l'organisation et qui offre conseils et assistance aux utilisateurs du système d'information pour ce qui touche le traitement et le signalement des incidents de sécurité.

Conseils supplémentaires : Les ressources d'aide aux interventions en cas d'incident fournies par les organisations comprennent entre autres les bureaux de services, les groupes d'aide et l'accès aux services d'informatique judiciaire. Contrôles connexes : AT-2, IR-4, IR-6, IR-8, SA-9.

Améliorations du contrôle :

(1) ASSISTANCE EN CAS D'INCIDENT | SOUTIEN AUTOMATISÉ CONCERNANT LA DISPONIBILITÉ DE L'INFORMATION ET DU SOUTIEN

L'organisation utilise des mécanismes automatisés pour accroître la disponibilité de l'information et du soutien relativement aux interventions en cas d'incident.

Conseils supplémentaires sur l'amélioration : Les mécanismes automatisés peuvent offrir aux utilisateurs une capacité d'assistance réactive ou proactive lors des interventions en cas d'incident. Par exemple, les utilisateurs peuvent avoir accès à un site Web pour interroger la capacité d'assistance ou, inversement, la capacité peut transmettre de l'information de manière proactive aux utilisateurs (par diffusion

générale ou ciblée) en vue d'accroître leurs connaissances concernant les capacités et le soutien actuels de l'organisation en matière d'intervention.

(2) ASSISTANCE EN CAS D'INCIDENT | COORDINATION AVEC DES FOURNISSEURS EXTERNES

(a) L'organisation établit une relation de coopération directe entre sa capacité d'intervention en cas d'incident et la capacité de protection des systèmes d'information de fournisseurs externes.

(b) L'organisation communique l'identité des membres de son équipe d'intervention en cas d'incident aux fournisseurs externes.

Conseils supplémentaires sur l'amélioration : Les fournisseurs externes participent à la protection, la surveillance, l'analyse et la détection des activités illicites dans les systèmes d'information et les réseaux de l'organisation et interviennent, le cas échéant.

Références :

Aucune

IR-8 PLAN D'INTERVENTION EN CAS D'INCIDENT

Contrôle :

(A) L'organisation développe un plan d'intervention en cas d'incident servant à effectuer ce qui suit :

(a) fournir une feuille de route à l'organisation pour la mise en œuvre de sa capacité d'intervention;

(b) décrire la structure et l'organisation de la capacité d'intervention en cas d'incident;

(c) présenter une approche de haut niveau de la façon dont la capacité d'intervention en cas d'incident est intégrée à l'ensemble de l'organisation;

(d) répondre aux exigences particulières de l'organisation concernant sa mission, sa taille, sa structure et ses fonctions;

(e) définir les incidents qui doivent être signalés;

(f) définir les paramètres de mesure de la capacité d'intervention de l'organisation en cas d'incident;

(g) définir les ressources et le soutien de la direction nécessaires au maintien et à l'évolution de la capacité d'intervention en cas d'incident;

(h) permettre [*Affectation : personnel ou rôles définis par l'organisation*] d'assurer son examen et son approbation.

(B) L'organisation distribue des copies du plan d'intervention en cas d'incident [*Affectation : employés (par nom ou rôle) et éléments organisationnels responsables de l'intervention en cas d'incident définis par l'organisation*].

(C) L'organisation examine le plan d'intervention en cas d'incident [*Affectation : fréquence définie par l'organisation*].

(D) L'organisation met à jour le plan d'intervention en cas d'incident pour tenir compte des changements organisationnels ou du système, ou des problèmes relevés au cours de la mise en œuvre, de l'exécution et des tests du plan.

(E) L'organisation communique les changements apportés au plan d'intervention en cas d'incident [*Affectation : employés (par nom ou rôle) et éléments organisationnels responsables de l'intervention en cas d'incident définis par l'organisation*].

(F) L'organisation protège le plan d'intervention en cas d'urgence contre toute divulgation ou modification non autorisée.

Conseils supplémentaires : Il est important que les organisations élaborent et mettent en œuvre une approche d'intervention coordonnée en cas d'incident. Les missions, les fonctions opérationnelles, les stratégies, les buts et les objectifs des organisations à cet égard aident à déterminer la structure de leur capacité d'intervention en cas d'incident. Dans le cadre de leur capacité globale d'intervention en cas d'incident, les organisations doivent tenir compte de la coordination et de l'échange d'information avec des organisations externes, y compris les fournisseurs de services externes et les organisations liées à la chaîne d'approvisionnement des systèmes d'information organisationnels. Contrôles connexes : MP-2, MP-4, MP-5.

Améliorations du contrôle :

Aucune

Références :

SCT, *Plan de gestion des incidents des technologies de l'information du gouvernement du Canada* [Référence 67].

IR-9 INTERVENTION EN CAS DE FUITE D'INFORMATION

Contrôle :

(A) L'organisation réagit aux fuites d'information en déterminant, de manière précise, quelle information a fait l'objet de la contamination du système d'information.

(B) L'organisation réagit aux fuites d'information en avertissant [*Affectation : employés ou rôles définis par l'organisation*] de la fuite d'information au moyen d'un mode de communication n'étant pas lié à la fuite.

(C) L'organisation réagit aux fuites d'information en isolant le système d'information ou du composant du système contaminé.

(D) L'organisation réagit aux fuites d'information en supprimant l'information du système d'information ou le composant du système contaminé.

(E) L'organisation réagit aux fuites d'information en déterminant si d'autres systèmes d'information ou composants de systèmes auraient pu être contaminés subséquemment.

(F) L'organisation réagit aux fuites d'information en exécutant les mesures suivantes : [*Affectation : mesures définies par l'organisation*].

Conseils supplémentaires : Les fuites d'information sont des situations où de l'information classifiée ou sensible est transmise, par inadvertance, à des systèmes pour lesquels le traitement de ce type d'information n'a pas été autorisé. Ces fuites d'information surviennent souvent lorsqu'on croit faussement que la classification de l'information transmise à un système d'information est moins élevée qu'elle ne l'est réellement et que cette correction est apportée après la transmission. À ce stade, il est nécessaire de mettre en place des mesures correctives. La nature de l'intervention organisationnelle est généralement fondée sur la sensibilité de l'information faisant l'objet de la fuite (p. ex. la catégorie de sécurité ou le niveau de classification), sur les capacités de sécurité du système d'information, sur la nature précise du support de stockage contaminé et sur les autorisations d'accès (p. ex. les habilitations de sécurité) des personnes autorisées à accéder au système contaminé. Les méthodes utilisées pour communiquer l'information relative à la fuite après le coup ne sont pas directement liées à la méthode de transmission de l'information faisant l'objet de la fuite de sorte à réduire le risque d'élargissement de la contamination avant que celle-ci ne soit isolée et l'information supprimée.

Améliorations du contrôle :

(1) INTERVENTION EN CAS DE FUITE D'INFORMATION | EMPLOYÉS RESPONSABLES

Les organisations désignent [*Affectation : employés ou rôles définis par l'organisation*] à titre de personnes responsables de l'intervention cas de fuite d'information.

(2) INTERVENTION EN CAS DE FUITE D'INFORMATION | FORMATION

L'organisation offre une formation sur l'intervention en cas de fuite d'information [*Affectation : fréquence définie par l'organisation*].

(3) INTERVENTION EN CAS DE FUITE D'INFORMATION | OPÉRATIONS À LA SUITE D'UNE FUITE

L'organisation met en œuvre [*Affectation : procédures définies par l'organisation*] afin de veiller à ce que les employés de l'organisation touchés par les fuites d'information puissent continuer d'exécuter leurs fonctions même si les systèmes contaminés sont en cours d'assainissement.

Conseils supplémentaires sur l'amélioration : Les mesures correctives appliquées aux systèmes contaminés par les fuites d'information peuvent exiger beaucoup de temps. Durant ces périodes, les employés pourraient ne pas avoir accès aux systèmes contaminés, ce qui peut nuire à leur capacité d'exécuter leurs fonctions organisationnelles.

(4) INTERVENTION EN CAS DE FUITE D'INFORMATION | EXPOSITION AU PERSONNEL NON AUTORISÉ

L'organisation utilise [*Affectation : mesures de protection de la sécurité définies par l'organisation*] lorsque certains employés sont exposés à de l'information qui dépasse leurs autorisations d'accès.

Conseils supplémentaires sur l'amélioration : Les mesures de protection de la sécurité comprennent notamment la conscientisation des employés exposés à l'information faisant l'objet de la fuite concernant les lois du GC et les politiques, directives et normes du SCT relativement à l'information dont il est question et aux restrictions imposées à la suite de l'exposition à celle-ci.

Références :

SCT, *Plan de gestion des incidents des technologies de l'information du gouvernement du Canada* [Référence 67].

IR-10 ÉQUIPE D'ANALYSE DE LA SÉCURITÉ DE L'INFORMATION INTÉGRÉE

Contrôle :

(A) L'organisation constitue une équipe intégrée d'analystes d'informatique judiciaire et de programmes malveillants, de développeurs d'outils et de personnel affecté aux opérations en temps réel.

Conseils supplémentaires : La constitution d'une équipe intégrée d'intervention en cas d'incident facilite l'échange d'information. Disposer d'une telle capacité permet au personnel de l'organisation, dont notamment les développeurs, les réalisateurs et les opérateurs, de tirer profit des connaissances de l'équipe concernant la menace afin de mettre en œuvre des mesures de défense qui permettront aux organisations de décourager plus efficacement les intrusions. De plus, ce type d'équipe facilite la détection rapide d'intrusions, l'élaboration de mesures d'atténuation appropriées et le déploiement de mesures de défense efficaces. Par exemple, dès qu'une intrusion est détectée, l'équipe d'analyse de la sécurité intégrée peut rapidement développer des mesures que les opérateurs peuvent mettre en œuvre, corréler le nouvel incident à l'information liée aux intrusions précédentes et élargir le développement du renseignement en cours. Ainsi, l'équipe peut identifier les tactiques, techniques et procédures (TTP) liées aux opérations ou à des fonctions opérationnelles et de mission particulières et définir les mesures d'intervention à prendre qui ne perturberont pas les activités opérationnelles et de mission. Idéalement, les équipes d'analyse de la sécurité de l'information sont réparties à l'échelle des organisations afin d'assurer la résilience de cette capacité.

Améliorations du contrôle :

Aucune

Références :

SCT, *Plan de gestion des incidents des technologies de l'information du gouvernement du Canada* [Référence 67].

3.9 FAMILLE : MAINTENANCE

CLASSE : OPÉRATIONNELLE

MA-1 POLITIQUE ET PROCÉDURES DE MAINTENANCE DES SYSTÈMES

Contrôle :

(A) L'organisation élabore, consigne et diffuse aux [*Affectation : personnel ou rôles définis par l'organisation*] :

(a) une politique de maintenance des systèmes qui définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et le respect; et

(b) des procédures visant à faciliter la mise en œuvre de la politique de maintenance des systèmes et des contrôles connexes.

(B) L'organisation examine et met à jour :

(a) la politique de maintenance des systèmes actuelle [*Affectation : fréquence définie par l'organisation*]; et

(b) les procédures de maintenance des systèmes actuelles [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : Ce contrôle porte sur l'établissement de la politique et les procédures nécessaires à la mise en œuvre efficace des contrôles de sécurité et des améliorations dans la famille MA. La politique et les procédures reflètent les lois du GC ainsi que les politiques, directives et normes applicables du SCT. Les politiques et les procédures du programme de sécurité organisationnel peuvent rendre facultatives les politiques et procédures propres au système. La politique peut être intégrée à la politique générale sur la sécurité de l'information des organisations ou, inversement, elle peut être représentée par de multiples politiques compte tenu de la nature complexe de certaines organisations. Les procédures peuvent être établies pour le programme de sécurité général et pour des systèmes d'information particuliers, au besoin. La stratégie organisationnelle de gestion des risques est un facteur clé dans l'établissement de la politique et des procédures.

Améliorations du contrôle :

Aucune

Références :

SCT, *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* [Référence 7].

MA-2 MAINTENANCE CONTRÔLÉE

Contrôle :

(A) L'organisation planifie, exécute, documente et examine les dossiers de maintenance et de réparation des composants de système d'information conformément aux spécifications du fabricant ou du fournisseur ou à ses propres exigences.

(B) L'organisation approuve et surveille toutes les activités de maintenance, qu'elles soient effectuées sur place ou à distance et que l'équipement soit réparé sur les lieux ou dans un autre emplacement.

(C) L'organisation exige que [*Affectation : personnel ou rôles définis par l'organisation*] approuve explicitement le retrait du système d'information, ou de ses composants, de ses installations aux fins de maintenance ou de réparation à l'extérieur de ses locaux.

(D) L'organisation nettoie l'équipement afin de supprimer toutes les données des supports connexes avant de l'expédier à l'extérieur aux fins de maintenance ou de réparation.

(E) L'organisation vérifie tous les contrôles de sécurité potentiellement concernés pour s'assurer qu'ils continuent de fonctionner adéquatement après les activités de maintenance ou de réparation.

(F) L'organisation inclut [*Affectation : information portant sur la maintenance définie par l'organisation*] dans les dossiers de maintenance organisationnels.

Conseils supplémentaires : Ce contrôle traite des aspects du programme de maintenance des systèmes d'information liés à la sécurité et s'applique à tous les types de maintenance réalisée par des entités locales ou non locales (p. ex. à l'interne, en vertu d'un contrat, d'une garantie ou d'une entente de maintenance de logiciel) dont font l'objet les composants du système (y compris les applications). La maintenance des systèmes comporte également trois composantes qui ne sont pas directement associées au traitement de l'information et/ou à la conservation des données et de l'information, notamment les numériseurs, les photocopieurs et les imprimantes. L'information nécessaire à la création de dossiers de maintenance efficaces comprend, notamment : (i) la date et l'heure de la maintenance; (ii) le nom de la personne ou du groupe responsable de la maintenance; (iii) le nom de l'escorte, au besoin; (iv) une description de la maintenance effectuée; et (v) les composants du système d'information ou l'équipement retirés ou remplacés (y compris les numéros d'identification, le cas échéant). Le degré de détail compris dans les dossiers de maintenance peut refléter les catégories de sécurité des systèmes d'information organisationnels. L'organisation tient compte des problèmes liés à la chaîne d'approvisionnement qui concernent le remplacement des composants des systèmes d'information. Contrôles connexes : CM-3, CM-4, MA-4, MP-6, PE-16, SA-12, SI-2.

Améliorations du contrôle :

(1) MAINTENANCE CONTRÔLÉE | CONTENU DES DOSSIERS

[Annulé : intégré au contrôle MA-2]

(2) MAINTENANCE CONTRÔLÉE | ACTIVITÉS DE MAINTENANCE AUTOMATISÉES

(a) L'organisation utilise des mécanismes automatisés pour planifier, exécuter et consigner les maintenances et les réparations; et

(b) L'organisation tient à jour des dossiers précis et complets de toutes les maintenances et réparations exigées, planifiées, en cours et exécutées.

Conseils supplémentaires sur l'amélioration : Contrôles connexes : CA-7, MA-3.

Références :

Aucune

MA-3 OUTILS DE MAINTENANCE

Contrôle :

(A) L'organisation approuve et contrôle les outils de maintenance des systèmes d'information et en surveille l'utilisation.

Conseils supplémentaires : Ce contrôle traite des enjeux liés à la sécurité qui découlent de l'utilisation des outils de maintenance aux fins de diagnostic et de réparation des systèmes d'information organisationnels. Les outils de maintenance comprennent les éléments matériels, logiciels et micrologiciels. Ils peuvent potentiellement servir au

transport intentionnel ou non intentionnel de programmes malveillants à l'intérieur d'une installation et, subséquemment, dans les systèmes d'information organisationnels. Les outils de maintenance comprennent, entre autres, l'équipement matériel et logiciel de diagnostic et de test ainsi que les renifleurs de paquets matériels et logiciels. Ce contrôle ne concerne pas les composants matériels et logiciels qui servent à la maintenance des systèmes d'information, bien qu'ils fassent partie de ces derniers (p. ex. logiciel utilisé pour exécuter les fonctions ping, ls ou ipconfig, ou matériel et logiciel mettant en œuvre le port de surveillance d'un commutateur Ethernet). Contrôles connexes : MA-2, MA-5, MP-6.

Améliorations du contrôle :

(1) OUTILS DE MAINTENANCE | INSPECTION DES OUTILS

L'organisation inspecte les outils de maintenance introduits dans une installation par le personnel de maintenance aux fins de détection de modifications inappropriées ou non autorisées.

Conseils supplémentaires sur l'amélioration : Lors de l'inspection, si l'organisation détermine que les outils de maintenance ont été modifiés de manière inappropriée ou non autorisée, ou qu'ils contiennent un programme malveillant, elle gérera l'incident conformément à ses politiques et procédures organisationnelles en matière de traitement des incidents. Contrôle connexe : SI-7.

(2) OUTILS DE MAINTENANCE | INSPECTION DES SUPPORTS

L'organisation vérifie que les supports qui contiennent des programmes de diagnostic et de test sont exempts de code malveillant avant qu'ils ne soient utilisés dans le système d'information.

Conseils supplémentaires sur l'amélioration : Lors de l'inspection des supports contenant des programmes diagnostic et de test de la maintenance, si l'organisation détermine que les supports contiennent un programme malveillant, elle gérera l'incident conformément à ses politiques et procédures organisationnelles en matière de traitement des incidents. Contrôle connexe : SI-3.

(3) OUTILS DE MAINTENANCE | PRÉVENTION DES RETRAITS NON AUTORISÉS

L'organisation prévient les retraits non autorisés de l'équipement de maintenance qui contient l'information organisationnelle; à cette fin, elle :

(a) vérifie que l'équipement ne contient aucune information organisationnelle;

(b) nettoie ou détruit l'équipement;

(c) conserve l'équipement dans l'installation; ou

(d) obtient une exemption de [*Affectation : personnel ou rôles définis par l'organisation*] autorisant explicitement le retrait de l'équipement de l'installation.

Conseils supplémentaires sur l'amélioration : L'information organisationnelle comprend toute information appartenant spécifiquement à l'organisation et celle fournie aux organisations qui gèrent l'information de cette dernière.

(4) OUTILS DE MAINTENANCE | UTILISATION RESTREINTE DES OUTILS

Le système d'information restreint l'utilisation des outils de maintenance au personnel autorisé uniquement.

Conseils supplémentaires sur l'amélioration : Cette amélioration du contrôle s'applique aux systèmes d'information qui sont utilisés pour effectuer des fonctions de maintenance. Contrôles connexes : AC-2, AC-3, AC-5, AC-6.

Références :

Aucune

MA-4 TÉLÉMAINTENANCE

Contrôle :

(A) L'organisation approuve et surveille les activités de télémaintenance et de télédiagnostic.

(B) L'organisation permet l'utilisation des outils de télémaintenance et de télédiagnostic seulement si elle est conforme à sa politique et consignée dans le plan de sécurité du système d'information.

(C) L'organisation utilise des authentifiants robustes lors de l'établissement des sessions de télémaintenance et de télédiagnostic.

(D) L'organisation tient à jour des enregistrements des activités de télémaintenance et de télédiagnostic.

Conseils supplémentaires : Les activités de télémaintenance et de télédiagnostic sont des activités exécutées par des personnes communiquant au moyen d'un réseau externe (p. ex. Internet) ou interne. Les activités de maintenance et de diagnostic locales sont effectuées par des employés situés dans les locaux qui hébergent le système d'information ou ses composants et qui ne communiquent pas au moyen d'une connexion réseau. Les techniques d'authentification utilisées lors de l'établissement des sessions de télémaintenance et de télédiagnostic reflètent les exigences d'accès aux réseaux énoncées dans le contrôle IA-2. Généralement, une authentification robuste exige des authentifiants résistant aux attaques par réinsertion et l'utilisation de l'authentification à facteurs multiples. Les authentifiants robustes comprennent, par exemple, l'infrastructure à clé publique (ICP) dont les certificats sont stockés dans un jeton protégé par mot de passe, une phrase passe ou des données biométriques. L'application des exigences énoncées dans le contrôle MA-4 est effectuée en partie par d'autres contrôles. Contrôles connexes : AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, MP-6, PL-2, SC-7, SC-10 et SC-17.

Améliorations du contrôle :

(1) TÉLÉMAINTENANCE | VÉRIFICATION ET EXAMEN

(a) L'organisation vérifie les sessions de télémaintenance et de télédiagnostic [*Affectation : événements de vérification définis par l'organisation*];

(b) L'organisation examine les enregistrements de sessions de maintenance et de diagnostic.

Conseils supplémentaires sur l'amélioration : Contrôles connexes : AU-2, AU-6 et AU-12.

(2) TÉLÉMAINTENANCE | ENREGISTREMENT DES ACTIVITÉS DE TÉLÉMAINTENANCE

L'organisation consigne, dans le plan de sécurité du système d'information, les politiques et procédures relatives à l'établissement et à l'utilisation des connexions de télémaintenance et de télédiagnostic.

(3) TÉLÉMAINTENANCE | SÉCURITÉ ET NETTOYAGE COMPARABLE

(a) L'organisation exige que les services de télémaintenance et de télédiagnostic soient effectués à partir d'un système d'information qui applique une capacité de sécurité comparable à celle du système cible; ou

(b) l'organisation retire le composant en question du système d'information avant l'exécution des activités de télémaintenance et de télédiagnostic, le nettoie (en supprime toute information organisationnelle) avant de l'expédier à l'extérieur et, une fois la réparation effectuée, l'inspecte et le nettoie à nouveau (pour en éliminer tout logiciel malveillant) avant de le reconnecter au système d'information.

Conseils supplémentaires sur l'amélioration : L'application d'une capacité de sécurité comparable sur les systèmes d'information, les outils de diagnostic et l'équipement fournissant des services de maintenance signifie que les contrôles de sécurité mis en œuvre sur ces systèmes, outils et équipement sont aussi étendus que ceux sur le système cible. Contrôles connexes : MA-3, SA-12, SI-3 et SI-7.

(4) TÉLÉMAINTENANCE | AUTHENTIFICATION ET SÉPARATION DES SESSIONS DE MAINTENANCE

(a) L'organisation protège les sessions de télémaintenance au moyen des [*Affectation : authentifiants résistant aux attaques par réinsertion définis par l'organisation*];

(b) L'organisation protège les sessions de télémaintenance en les isolant des autres sessions réseau du système d'information, comme suit :

- elle sépare physiquement les voies de communication; ou
- elle sépare logiquement les voies de communication à l'aide d'une méthode de chiffrement conforme aux exigences du contrôle SC-13.

Conseils supplémentaires sur l'amélioration : Contrôle connexe : SC-13.

(5) TÉLÉMAINTENANCE | APPROBATIONS ET AVIS

(a) L'organisation exige l'approbation de chacune des sessions de télémaintenance par [*Affectation : membres du personnel ou rôles définis par l'organisation*];

(b) L'organisation avise [*Affectation : membres du personnel ou rôles définis par l'organisation*] de la date et de l'heure à laquelle la télémaintenance est prévue.

Conseils supplémentaires sur l'amélioration : Le personnel de maintenance peut se charger des avis. Les sessions de télémaintenance doivent être approuvées par des membres du personnel ayant suffisamment de connaissances des systèmes d'information et de la sécurité de l'information pour déterminer la pertinence de la maintenance proposée.

(6) TÉLÉMAINTENANCE | PROTECTION CYPTOGRAPHIQUE

Le système d'information applique des mécanismes cryptographiques pour protéger l'intégrité et la confidentialité des communications liées à la télémaintenance et au télédiagnostic.

Conseils supplémentaires sur l'amélioration : Contrôles connexes SC-8 et SC-13.

(7) TÉLÉMAINTENANCE | VÉRIFICATION DE LA DÉCONNEXION À DISTANCE

Le système d'information vérifie la déconnexion à distance à la fin des sessions de télémaintenance et de télédiagnostic.

Conseils supplémentaires sur l'amélioration : La vérification de la déconnexion à distance permet de s'assurer que les connexions à distance à la fin des sessions de télémaintenance ont été interrompues et qu'elles ne peuvent plus être utilisées. Contrôle connexe : SC-13. Les activités de télémaintenance et de télédiagnostic sont des activités exécutées par des personnes communiquant au moyen d'un réseau externe (p. ex. Internet) ou interne. Elles sont effectuées par des employés situés dans les locaux qui hébergent le système d'information ou ses composants et qui ne communiquent pas au moyen d'une connexion réseau. Les techniques d'identification et d'authentification utilisées lors de l'établissement des sessions de télémaintenance et de télédiagnostic sont conformes aux exigences d'accès aux réseaux énoncées dans le contrôle IA-2. Les authentifiants robustes comprennent, par exemple, l'ICP dont les certificats sont stockés dans un jeton protégé par mot de passe, une phrase passe ou des données biométriques. L'application des exigences énoncées dans le contrôle MA-4 est effectuée en partie par d'autres contrôles. Contrôles connexes : AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-8, MA-5, MP-6 et SC-7.

Références :

CST, *ITSG-31, Guide sur l'authentification des utilisateurs pour les systèmes TI* [référence 18].

MA-5 PERSONNEL DE MAINTENANCE

Contrôle :

(A) L'organisation établit un processus d'autorisation du personnel de maintenance et tient à jour une liste des organisations et des employés autorisés à effectuer les activités de maintenance.

(B) L'organisation veille à ce que le personnel non accompagné effectuant les activités de maintenance sur le système d'information possède les autorisations d'accès requises.

(C) L'organisation désigne certains de ses employés qui possèdent les autorisations d'accès et les compétences techniques nécessaires pour superviser les activités de maintenance effectuées par le personnel qui ne possède pas les autorisations d'accès appropriées.

Conseils supplémentaires : Ce contrôle s'applique aux personnes effectuant la maintenance matérielle ou logicielle sur les systèmes d'information organisationnels, tandis que le contrôle PE-2 s'applique à l'accès physique des personnes dont les tâches de maintenance les obligent à être à l'intérieur du périmètre de protection des systèmes (p. ex. personnel de garde, personnel d'entretien des installations). Les compétences techniques des superviseurs sont liées à la maintenance effectuée sur les systèmes d'information, tandis que la possession des autorisations d'accès appropriées est liée à la maintenance sur et près des systèmes. Les personnes non identifiées au préalable comme étant des membres du personnel autorisés, tels que les fabricants de technologies d'information, les fournisseurs, les intégrateurs de système et les experts-conseils, peuvent demander un accès privilégié aux systèmes d'information organisationnels, par exemple pour mener des activités de maintenance avec court préavis ou sans préavis. Selon les évaluations organisationnelles des risques, les organisations peuvent octroyer des justificatifs d'identité temporaires à ces personnes. Ces justificatifs peuvent être octroyés pour un accès unique ou pour une période de temps très limitée. Contrôles connexes : AC-2, IA-8, MP-2, PE-2, PE-3, PE-4 et RA-3.

Améliorations du contrôle :

(1) PERSONNEL DE MAINTENANCE | PERSONNES NE DÉTENANT PAS L'ACCÈS APPROPRIÉ

(a) L'organisation met en œuvre des procédures pour les membres du personnel de maintenance qui ne possèdent pas l'habilitation de sécurité appropriée ou qui ne sont pas citoyens canadiens; ces procédures comprennent les exigences suivantes :

- les membres du personnel de maintenance qui ne possèdent pas les autorisations d'accès, l'habilitation de sécurité ou les approbations officielles d'accès requises sont escortés et surveillés durant l'exécution des activités de maintenance et de diagnostic sur le système d'information par des employés de l'organisation qui sont pleinement habilités, qui possèdent les autorisations d'accès appropriées et qui sont qualifiés sur le plan technique;
- avant que des membres du personnel qui ne possèdent pas les autorisations d'accès, l'habilitation de sécurité ou les approbations officielles d'accès requises puissent entreprendre les activités de maintenance ou de diagnostic, tous les composants de stockage d'information volatile du système d'information sont nettoyés, et les supports d'information non volatile sont enlevés ou physiquement déconnectés du système puis rangés dans un endroit sûr.

(b) L'organisation développe et met en œuvre d'autres mesures de protection dans l'éventualité où un composant du système d'information ne peut être nettoyé, retiré ou déconnecté du système.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle interdit, aux personnes qui ne possèdent pas l'habilitation de sécurité appropriée (c.-à-d. qui ne possèdent pas d'habilitation ou dont l'habilitation est inférieure au niveau de sécurité requis) ou qui ne sont pas citoyens canadiens, tout accès visuel et électronique à toute information classifiée ou protégée contenue dans les systèmes d'information organisationnels. Les procédures concernant le personnel de maintenance peuvent être consignées dans les plans de sécurité des systèmes d'information. Contrôles connexes : MP-6 et PL-2.

(2) PERSONNEL DE MAINTENANCE | HABILITATIONS DE SÉCURITÉ POUR LES SYSTÈMES CLASSIFIÉS

L'organisation veille à ce que les personnes qui effectuent des activités de maintenance et de diagnostic sur un système d'information qui traite, stocke et transmet de l'information classifiée possèdent l'habilitation de sécurité et les approbations d'accès officiels au moins équivalant au niveau de sécurité le plus élevé de l'information contenue dans le système et équivalant à tous les compartiments de cette information.

Conseils supplémentaires sur l'amélioration : Contrôle connexe : PS-3.

(3) PERSONNEL DE MAINTENANCE | EXIGENCES DE CITOYENNETÉ POUR LES SYSTÈMES CLASSIFIÉS

L'organisation veille à ce que les personnes qui effectuent des activités de maintenance et de diagnostic sur un système d'information qui traite, stocke et transmet de l'information classifiée sont des citoyens canadiens.

Conseils supplémentaires sur l'amélioration : Contrôle connexe : PS-3.

(4) PERSONNEL DE MAINTENANCE | RESSORTISSANTS ÉTRANGERS

(a) L'organisation s'assure que des ressortissants étrangers habilités (c.-à-d. possédant l'habilitation de sécurité appropriée) exécutent les activités de maintenance et de diagnostic sur les systèmes d'information seulement lorsque ceux-ci appartiennent et sont exploités à la fois par le gouvernement canadien et des gouvernements étrangers alliés, ou uniquement par des gouvernements étrangers alliés.

(b) L'organisation s'assure que les approbations, les consentements et les modalités opérationnelles détaillées concernant le recours à de ressortissants étrangers pour mener des activités de maintenance et de diagnostic sur les systèmes d'information sont bien consignés dans des protocoles d'entente.

Conseils supplémentaires sur l'amélioration : Contrôle connexe : PS-3.

(5) PERSONNEL DE MAINTENANCE | MAINTENANCE NON LIÉE AUX SYSTÈMES

L'organisation s'assure que les personnes non accompagnées exécutant des activités de maintenance qui ne sont pas directement liées au système d'information, mais qui sont réalisées à proximité du système, détiennent les autorisations d'accès appropriés.

Conseils supplémentaires sur l'amélioration : Les personnes exécutant des activités de maintenance qui ne sont pas directement liées au système d'information comprennent, par exemple, le personnel d'entretien des installations et le personnel de nettoyage.

Références :

CST, *ITSA-23 – Services de soutien des produits de sécurité offerts par les fournisseurs* [référence 30].

MA-6 MAINTENANCE OPPORTUNE

Contrôle :

(A) L'organisation obtient des services de maintenance et/ou des pièces de rechange pour les [*Affectation : composants du système d'information définis par l'organisation*] dans les [*Affectation : durée définie par l'organisation*] qui suivent la panne.

Conseils supplémentaires : L'organisation précise les composants du système d'information qui représentent un risque accru pour les activités et les biens de l'organisation, les personnes, les autres organisations ou le Canada lorsque les fonctionnalités de ces composants ne sont pas opérationnelles. Les mesures que prend l'organisation pour obtenir des services de maintenance comprennent généralement la mise en place de contrats appropriés. Contrôles connexes : CM-8, CP-2, CP-7, SA-14 et SA-15.

Améliorations du contrôle :

(1) MAINTENANCE OPPORTUNE | MAINTENANCE PRÉVENTIVE

L'organisation effectue la maintenance préventive des [*Affectation : composants du système d'information définis par l'organisation*] tous les [*Affectation : intervalles définis par l'organisation*].

Conseils supplémentaires sur l'amélioration : La maintenance préventive comprend l'entretien courant des composants des systèmes d'information organisationnels afin de s'assurer que l'équipement et les installations fonctionnent de façon satisfaisante. Cette maintenance permet systématiquement d'inspecter, de tester, de mesure et d'ajuster l'équipement, de remplacer des pièces ainsi que de détecter et de corriger les pannes avant qu'elles se produisent ou avant qu'elles se transforment en problèmes majeurs. La maintenance préventive vise principalement à éviter ou à atténuer les conséquences des pannes d'équipement. Elle est conçue afin de préserver et de rétablir la fiabilité de l'équipement grâce au remplacement de vieux composants avant qu'ils cessent de fonctionner. Les méthodes à appliquer permettant de déterminer les politiques de gestion préventive des pannes (ou autre) comprennent, par exemple, les recommandations du constructeur (OEM), les enregistrements statistiques de panne, les exigences du code, les lois ou les règlements sans juridiction, l'opinion d'un spécialiste, la maintenance réalisée sur de l'équipement similaire ou les valeurs mesurées et les indicateurs de rendement.

(2) MAINTENANCE OPPORTUNE | MAINTENANCE PRÉVISIONNELLE

L'organisation effectue la maintenance prévisionnelle des [*Affectation : composants du système d'information définis par l'organisation*] tous les [*Affectation : intervalles définis par l'organisation*].

Conseils supplémentaires sur l'amélioration : La maintenance prévisionnelle sert à évaluer l'état de l'équipement en surveillant l'état de façon périodique ou continue (en ligne). Elle vise à effectuer la maintenance au moment prévu où les activités de maintenance sont les plus efficaces et avant que le rendement de l'équipement diminue dans un seuil. La composante prévisionnelle découle de l'objectif selon lequel il faut prédire la tendance future en ce qui a trait à l'état de l'équipement. Cette approche utilise des principes de contrôle statistique du processus en vue de déterminer le moment où les activités de maintenance future seront appropriées. Les inspections de maintenance les plus prévisionnelles sont réalisées lorsque l'équipement est en service, ce qui réduit la perturbation des opérations normales du système. La maintenance prévisionnelle peut entraîner des économies considérables ainsi qu'une meilleure fiabilité système. Elle a tendance à inclure la mesure du composant. Afin d'évaluer l'état de l'équipement, la maintenance prévisionnelle emploie des technologies de mise à l'essai non destructives telles que l'infrarouge, l'acoustique (décharge partielle et ultrason aéroporté), la détection de l'effet couronne, l'analyse des vibrations, la mesure du niveau sonore, l'analyse de l'huile et d'autres tests en ligne précis.

(3) MAINTENANCE OPPORTUNE | SOUTIEN AUTOMATISÉ POUR LA MAINTENANCE PRÉVISIONNELLE

L'organisation utilise des mécanismes automatisés pour transférer les données de maintenance prévisionnelle à un système informatisé de gestion des activités de maintenance.

Conseils supplémentaires sur l'amélioration : Un système informatisé de gestion des activités de maintenance tient une base de données informatique de l'information sur les activités de maintenance des organisations et automatise le traitement des données sur l'état de l'équipement afin de déclencher la planification, l'exécution et les rapports des activités de maintenance.

Références :

Aucune

3.10 FAMILLE : PROTECTION DES SUPPORTS

CLASSE : OPÉRATIONNELLE

MP-1 POLITIQUE ET PROCÉDURES DE PROTECTION DES SUPPORTS

Contrôle :

(A) L'organisation élabore et consigne, ainsi que diffuse aux [*Affectation : personnel ou rôles définis par l'organisation*] :

(a) une politique officielle et documentée qui définit les divers aspects de la protection des supports (but, portée, rôles, responsabilité, engagement de la direction, coordination entre les entités organisationnelles et conformité);

(b) les procédures susceptibles de faciliter la mise en œuvre de la politique de protection des supports et des contrôles connexes.

(B) L'organisation examine et met à jour :

(a) la politique de protection des supports actuelle [*Affectation : fréquence définie par l'organisation*];

(b) les procédures de protection des supports actuelles [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : Ce contrôle concerne l'élaboration des politiques et procédures nécessaires à la mise en œuvre efficace des contrôles de sécurité et des améliorations de contrôle sélectionnés dans la famille MP. La politique et les procédures de protection des supports reflètent les lois du GC et les politiques, directives et normes applicables du SCT. Les politiques et les procédures du programme de sécurité mises en place à l'échelle de l'organisation peuvent rendre inutile toute politique et procédure propre à un système. La politique peut être incorporée à la politique générale sur la sécurité de l'information de l'organisation ou, à l'inverse, faire l'objet de plusieurs politiques reflétant la nature complexe de certaines organisations. Les procédures peuvent être établies pour le programme de sécurité général et pour des systèmes d'information particuliers, au besoin. La stratégie organisationnelle de gestion des risques est un facteur clé dans l'établissement de la politique et des procédures.

Améliorations du contrôle :

Aucune

Références :

SCT, *Norme opérationnelle sur la sécurité matérielle* [Référence 6].
SCT, *Norme opérationnelle de sécurité — Gestion de la sécurité des technologies de l'information* [Référence 7].
CST, *ITSD-03A, Directive sur le contrôle du matériel COMSEC au sein du gouvernement du Canada* [Référence 36].
SCT, *Avis de mise en œuvre de la Politique sur la technologie de l'information 2014-01*[Référence 68].

MP-2 ACCÈS AUX SUPPORTS

Contrôle :

(A) L'organisation restreint l'accès des [*Affectation : types de support numérique et non numérique définis par l'organisation*] aux [*Affectation : personnel ou rôles définis par l'organisation*].

Conseils supplémentaires : Les supports utilisés pour les systèmes d'information incluent autant les supports numériques que les supports non numériques. Les supports numériques comprennent, par exemple, les disquettes, les bandes magnétiques, les disques durs externes ou amovibles, les clés USB, les disques compacts et les vidéodisques numériques. Les supports non numériques comprennent le papier et les microfilms. Par restriction des accès aux supports non numériques, on entend, entre autres, refuser l'accès aux dossiers médicaux des patients d'une communauté à des personnes autres que les professionnels de soins de santé autorisés à accéder à de tels dossiers. Par restriction des accès aux supports numériques, on entend, notamment, limiter l'accès aux spécifications de conception stockées sur les disques compacts d'une bibliothèque de supports au chef de projet et aux membres de l'équipe de développement. Contrôles connexes : AC-3, IA-2, MP-4, PE-2, PE-3, PL-2.

Améliorations du contrôle :

(1) ACCÈS AUX SUPPORTS | ACCÈS LIMITÉ AUTOMATISÉ

[Annulé : Intégré au contrôle MP-4 (2)]

(2) ACCÈS AUX SUPPORTS | PROTECTION CRYPTOGRAPHIQUE

[Annulé : Intégré au contrôle SC-28 (1)]

Références :

Aucune

MP-3 MARQUAGE DES SUPPORTS

Contrôle :

(A) L'organisation indique sur les supports du système d'information les limites de distribution, les mises en garde concernant la manutention et les mentions de sécurité (le cas échéant) de l'information.

(B) L'organisation exempte les [*Affectation : types de supports du système d'information définis par l'organisation*] de tout marquage pour autant qu'ils demeurent dans [*Affectation : zones contrôlées définies par l'organisation*].

Conseils supplémentaires : L'expression « *marquage de sécurité* » désigne l'application ou l'utilisation d'attributs de sécurité lisibles par des humains. L'expression « *étiquetage de sécurité* » désigne l'application ou l'utilisation d'attributs de sécurité liés aux structures de données internes du système (voir le contrôle AC-16). Les supports utilisés pour les systèmes d'information incluent autant les supports numériques que les supports non numériques. Les supports numériques comprennent, par exemple, les disquettes, les bandes magnétiques, les disques durs externes ou amovibles, les clés USB, les disques compacts et les vidéodisques numériques. Les supports non numériques comprennent, notamment, le papier et les microfilms. Le marquage de sécurité n'est généralement pas requis dans le cas des supports qui contiennent de l'information qui, selon l'organisation, est du domaine public ou peut être diffusée publiquement. Certaines organisations peuvent toutefois exiger le marquage de l'information publique pour indiquer qu'elle peut être diffusée publiquement. Le marquage des supports du système d'information reflète les lois du GC ainsi que les politiques, directives et normes applicables du SCT. Contrôles connexes : AC-16, PL-2, RA-3.

Améliorations du contrôle :

Aucune

Références :

SCT, *Norme de sécurité relative à l'organisation et l'administration* [Référence 13].

MP-4 ENTREPOSAGE DES SUPPORTS

Contrôle :

(A) L'organisation contrôle physiquement et entrepose de manière sécurisée les [*Affectation : types de support numérique et/ou non numérique définis par l'organisation*] dans [*Affectation : zones contrôlées définies par l'organisation*], conformément au *Guide d'équipement de sécurité* (G1-001) de la GRC [Référence 15].

(B) L'organisation protège l'information contenue sur les supports du système d'information jusqu'à ce qu'ils soient détruits ou nettoyés avec de l'équipement, des techniques et des procédures approuvés.

Conseils supplémentaires : Les supports utilisés pour les systèmes d'information incluent autant les supports numériques que les supports non numériques. Les supports numériques comprennent, par exemple, les disquettes, les bandes magnétiques, les disques durs externes ou amovibles, les clés USB, les disques compacts et les vidéodisques numériques. Les supports non numériques comprennent, notamment, le papier et les microfilms. Le contrôle physique des supports du système d'information comporte entre autres la tenue d'inventaires, la mise en place de procédures afin que les utilisateurs soient en mesure de réserver et retourner les supports dans la bibliothèque de support et la préservation de la responsabilisation pour tous les supports stockés. On entend par entreposage sécurisé un tiroir, un bureau et une armoire verrouillés, ou une bibliothèque de supports contrôlés. Le type d'entreposage de supports dépend de la catégorie de sécurité et/ou de la classification de l'information qui se trouve sur les supports. Les zones contrôlées sont des zones à l'intérieur desquelles les organisations mettent en place les mesures de sécurité matérielle et de protection suffisantes pour respecter les exigences liées à la protection de l'information et des systèmes d'information. Moins de mesures de protection sont requises dans le cas des supports qui contiennent de l'information qui, selon les organisations, relève du domaine public, peut être diffusée publiquement ou dont l'accès par du personnel non autorisé n'a aucune ou peu d'incidence négative sur les activités et les biens de l'organisation, sur les personnes, les autres organisations ou le Canada. Dans de tels cas, les contrôles d'accès physique procurent une protection adéquate. Contrôles connexes : CP-6, CP-9, MP-2, MP-7, PE-3.

Améliorations du contrôle :

(1) ENTREPOSAGE DES SUPPORTS | PROTECTION CRYPTOGRAPHIQUE

[Annulé : Intégré au contrôle SC-28 (1)]

(2) ENTREPOSAGE DES SUPPORTS | ACCÈS LIMITÉ AUTOMATISÉ

L'organisation utilise des mécanismes automatisés pour restreindre l'accès aux aires d'entreposage des supports de même que pour vérifier les tentatives d'accès et l'accès accordé.

Conseils supplémentaires sur l'amélioration : Les mécanismes automatisés comprennent notamment les pavés numériques sur les entrées externes des zones d'entreposage des supports. Contrôles connexes : AU-2, AU-9, AU-6, AU-12.

Références :

GRC, G1-001, *Guide d'équipement de sécurité* [Référence 15].
CST, ITSG-06, *Effacement et déclassification des supports d'information électroniques* [Référence 16].
GRC, G1-029, *Pièces sécuritaires* [Référence 23].
SCT, *Avis de mise en œuvre de la Politique sur la technologie de l'information 2014-01* [Référence 68].
CST, ITSB-112, *Questions de sécurité relatives à l'utilisation de supports amovibles pour les renseignements Protégé C et classifiés* [Référence 69].

MP-5 TRANSPORT DES SUPPORTS

Contrôle :

(A) L'organisation protège et contrôle [*Affectation : types de supports de système d'information définis par l'organisation*] durant leur transport hors des zones contrôlées en utilisant [*Affectation : mesures de sécurité définies par l'organisation*] conformément à la *Norme opérationnelle sur la sécurité matérielle du SCT* [Référence 6] et au document *Transport et transmission de renseignements protégés ou classifiés* (G1-009) de la GRC [Référence 17].

(B) L'organisation demeure responsable des supports du système d'information durant leur transport hors des zones contrôlées.

(C) L'organisation documente les activités associées au transport des supports du système d'information.

(D) L'organisation réserve les activités associées au transport des supports du système d'information au personnel autorisé.

Conseils supplémentaires : Les supports utilisés pour les systèmes d'information incluent autant les supports numériques que les supports non numériques. Les supports numériques comprennent, par exemple, les disquettes, les bandes magnétiques, les disques durs externes ou amovibles, les clés USB, les disques compacts et les vidéodisques numériques. Les supports non numériques comprennent, notamment, le papier et les microfilms. Ce contrôle s'applique également aux dispositifs mobiles dotés d'une capacité de stockage (p. ex. les téléphones intelligents, les tablettes, les liseuses électroniques) qui sont transportés hors des zones contrôlées. Les zones contrôlées sont des zones ou aires à l'intérieur desquelles les organisations mettent en place les mesures de sécurité matérielle et/ou de protection suffisantes pour respecter les exigences liées à la protection de l'information et des systèmes d'information.

Les mesures de protection matérielles et techniques des supports dépendent de la catégorie de sécurité ou de la classification de l'information qui se trouve sur les supports, conformément aux lois du GC ainsi qu'aux politiques, aux directives et aux normes applicables du SCT. Les mesures visant à protéger les supports lors du transport comprennent notamment les contenants verrouillés et la cryptographie. Certains mécanismes cryptographiques peuvent protéger la confidentialité et l'intégrité de l'information. Les activités associées au transport incluent le transport réel ainsi que les autres activités exercées en vue de remettre les supports aux fins de transport et de s'assurer qu'ils soient soumis à un processus de transport adéquat. En ce qui a trait au transport réel, le personnel autorisé responsable du transport et de la messagerie peut inclure des personnes de l'extérieur de l'organisation (p. ex. Postes Canada ou un service de transport ou de livraison commercial). Préserver la responsabilisation des supports durant leur transport implique notamment limiter les activités de transport au personnel autorisé, de même que faire le suivi et/ou obtenir des enregistrements formels des activités de transport à mesure que les supports se déplacent à travers le système de transport afin d'éviter et de détecter toute perte, destruction ou tentative de trafiquage. Les organisations établissent les exigences de documentation des activités associées au transport des supports du système d'information conformément à l'évaluation organisationnelle des risques. Ces exigences peuvent comprendre la capacité de définir différentes méthodes de tenue des dossiers pour les différents types de supports dans le contexte d'un système global de dossiers afférents au transport. Contrôles connexes : AC-19, CP-9, MP-3, MP-4, RA-3, SC-8, SC-13, SC-28.

Améliorations du contrôle :

(1) TRANSPORT DES SUPPORTS | PROTECTION HORS DES ZONES CONTRÔLÉES

[Annulé : Intégré au contrôle MP-5]

(2) TRANSPORT DES SUPPORTS | DOCUMENTATION DES ACTIVITÉS

[Annulé : Intégré au contrôle MP-5]

(3) TRANSPORT DES SUPPORTS | GARDIENS

L'organisation fait appel à un gardien désigné durant le transport des supports du système d'information à l'extérieur des zones contrôlées.

Conseils supplémentaires sur l'amélioration : Les gardiens désignés fournissent à l'organisation des points de contact durant le processus de transport des supports et facilitent la comptabilité individuelle. Les responsabilités qui incombent au gardien peuvent être transférées d'une personne à une autre pour autant qu'il n'y ait aucune ambiguïté quant à l'identité du gardien.

(4) TRANSPORT DES SUPPORTS | PROTECTION CRYPTOGRAPHIQUE

Le système d'information met en œuvre des mécanismes cryptographiques conformes aux exigences du contrôle SC-13 pour protéger la confidentialité et l'intégrité de l'information stockée dans des supports numériques durant leur transport hors des zones contrôlées.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle s'applique aux dispositifs de stockage portatifs (p. ex. clés USB, disques compacts, vidéodisques, disques durs externes/amovibles) et aux dispositifs mobiles dotés d'une capacité de stockage (p. ex. téléphones intelligents, tablettes, liseuses électroniques). Contrôle connexe : SC-13.

Références :

SCT, *Norme opérationnelle sur la sécurité matérielle* [Référence 6].
GRC, G1-009, *Transport et transmission de renseignements protégés ou classifiés* [Référence 17].
CST, ITSA-11, *Algorithmes cryptographiques approuvés par le CST pour la protection des renseignements protégés* [Référence 8].
CST, ITSB-40A, *Politique du gouvernement du Canada pour la protection de l'information classifiée à l'aide d'algorithmes Suite B* [Référence 28].
CST, ITSD-03A, *Directive sur le contrôle du matériel COMSEC au sein du gouvernement du Canada* [Référence 36].
SCT, *Avis de mise en œuvre de la Politique sur la technologie de l'information 2014-01* [Référence 68].

MP-6 NETTOYAGE DES SUPPORTS

Contrôle :

(A) L'organisation nettoie les [*Affectation : supports du système d'information définis par l'organisation*] avant leur élimination ou leur transfert hors de son contrôle ou à des fins de réutilisation. Elle utilise des [*Affectation : techniques et procédures de nettoyage définies par l'organisation*], conformément à ses normes et politiques applicables ainsi que celles du GC.

(B) L'organisation utilise des mécanismes de nettoyage dont la robustesse et l'intégrité correspondent à la catégorie de sécurité ou à la classification de l'information.

Conseils supplémentaires : Ce contrôle s'applique à tous les supports numériques et non numériques du système d'information susceptibles d'être éliminés ou réutilisés, qu'ils soient amovibles ou non. Comme exemples, citons les supports retrouvés dans les appareils de numérisation, les photocopieurs, les imprimantes, les ordinateurs bloc-notes, les postes de travail, les composants de réseau et les dispositifs mobiles. Le processus de nettoyage supprime l'information sur les supports de manière à ce qu'il soit impossible de la récupérer ou de la reconstituer. Les techniques de nettoyage, notamment l'effacement, l'épuration, l'effacement cryptographique et la destruction de l'information contenue dans les supports, empêchent la divulgation d'information à des personnes non autorisées lorsque les supports sont réutilisés ou transférés aux fins d'élimination. L'organisation détermine les méthodes de nettoyage appropriées tout en sachant qu'il est parfois nécessaire de détruire les supports si ces derniers ne peuvent être soumis à aucune autre méthode de nettoyage. L'organisation utilise à sa discrétion les techniques et procédures approuvées de nettoyage des supports qui contiennent de l'information du domaine public, ou qui peut être diffusée publiquement, ou dont le transfert à des fins de réutilisation ou d'élimination n'a

pas d'incidence négative sur l'organisation ou les personnes. Le nettoyage des supports non numériques comprend notamment la suppression d'une annexe classifiée dans un document autrement non classifié ou la rédaction de certaines sections ou de certains mots tirés d'un document en masquant les sections ou mots triturés aussi efficacement que s'ils avaient été supprimés du document. Les normes et politiques du CST contrôlent le processus de nettoyage des supports qui contiennent de l'information classifiée. Contrôles connexes : MA-2, MA-4, RA-3, SC-4.

Améliorations du contrôle :

(1) NETTOYAGE DES SUPPORTS | EXAMEN / APPROBATION / SUIVI / DOCUMENTATION / VÉRIFICATION

L'organisation examine, approuve, suit, documente et vérifie le nettoyage des supports et les activités d'élimination.

Conseils supplémentaires sur l'amélioration : L'organisation examine et approuve les supports à nettoyer pour en assurer la conformité aux politiques de conservation des dossiers. Les mesures de suivi/documentation comprennent, notamment, dresser la liste du personnel ayant passé en revue et approuvé les activités de nettoyage et d'élimination, les types de supports nettoyés, les fichiers spécifiques enregistrés sur le support, les méthodes de nettoyage employées, la date et l'heure des activités de nettoyage, le personnel ayant procédé au nettoyage, les activités de vérification qui ont été menées, le personnel ayant procédé à la vérification et les activités d'élimination qui ont été prises. L'organisation s'assure que le nettoyage des supports a bien été fait avant l'élimination. Contrôle connexe : SI-12.

(2) NETTOYAGE DES SUPPORTS | MISE À L'ESSAI DU MATÉRIEL

L'organisation teste les procédures et l'équipement de nettoyage [*Affectation : fréquence définie par l'organisation*] en vue de s'assurer que le nettoyage prévu a bien été réalisé.

Conseils supplémentaires sur l'amélioration : La mise à l'essai de l'équipement et des procédures de nettoyage peut être réalisée par des entités externes qualifiées et autorisées (p. ex. d'autres ministères, organismes ou fournisseurs de services externes du GC).

(3) NETTOYAGE DES SUPPORTS | TECHNIQUES NON DESTRUCTIVES

L'organisation nettoie les dispositifs de stockage portatifs au moyen de techniques de nettoyage non destructives avant de les connecter au système d'information dans les situations suivantes : [*Affectation : liste définie par l'organisation des circonstances où les dispositifs de stockage portatifs doivent être nettoyés*].

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle s'applique aux supports numériques qui contiennent de l'information classifiée et protégée. Les dispositifs de stockage portatifs peuvent être la source d'insertions de code malveillant dans les systèmes d'information organisationnels. Plusieurs de ces dispositifs proviennent de sources inconnues et potentiellement douteuses. Ils peuvent contenir du code malveillant susceptible d'être transmis aux systèmes d'information par des ports USB ou d'autres portails d'entrée. On recommande de toujours analyser ces dispositifs de stockage; toutefois, le nettoyage offre une assurance supplémentaire qu'ils sont exempts de tout code malveillant, y compris le code capable de lancer des attaques de jour zéro. Les organisations jugent utile de nettoyer ces dispositifs de stockage portatifs de façon non destructrice, par exemple, au moment de l'achat chez un fabricant ou un fournisseur et avant leur utilisation, ou lorsqu'il y a interruption de leur chaîne de possession. Contrôle connexe : SI-3.

(4) NETTOYAGE DES SUPPORTS | INFORMATION NON CLASSIFIÉE CONTRÔLÉE

[Annulé : Intégré au contrôle MP-6]

(5) NETTOYAGE DES SUPPORTS | INFORMATION CLASSIFIÉE

[Annulé : Intégré au contrôle MP-6]

(6) NETTOYAGE DES SUPPORTS | DESTRUCTION DES SUPPORTS

[Annulé : Intégré au contrôle MP-6]

(7) NETTOYAGE DES SUPPORTS | DOUBLE AUTORISATION

L'organisation fait appel à une double autorisation pour ce qui est du nettoyage des [*Affectation : supports du système d'information définis par l'organisation*].

Conseils supplémentaires sur l'amélioration : L'organisation fait appel à une double autorisation pour s'assurer que le nettoyage des supports du système d'information ne puisse être effectué que sous la supervision de deux personnes qualifiées sur le plan technique. Les personnes qui procèdent au nettoyage des supports du système d'information possèdent les compétences et l'expertise suffisantes pour déterminer si le nettoyage proposé respecte les normes, les politiques et les procédures du GC et de l'organisation. Une double autorisation permet également de s'assurer que le nettoyage s'effectue comme prévu, tout en évitant les erreurs et de fausses indications que des mesures de nettoyage ont été réalisées. La double autorisation est également appelée le contrôle par deux personnes. Contrôles connexes : AC-3 et MP-2.

(8) NETTOYAGE DES SUPPORTS | PURGE ET NETTOYAGE À DISTANCE DE L'INFORMATION

L'organisation fournit la capacité de purger et nettoyer l'information qui se trouve sur les [*Affectation : systèmes d'information, composants système ou dispositifs définis par l'organisation*] à distance ou en vertu des conditions suivantes : [*Affectation : conditions définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle protège les données et l'information stockées sur les systèmes d'information, les composants système ou les dispositifs (p. ex. les dispositifs mobiles) de l'organisation si ces systèmes, composants ou dispositifs se retrouvent entre les mains de personnes non autorisées. Les commandes de purge et nettoyage à distance exigent une authentification forte afin d'atténuer les risques que des personnes non autorisées ne procèdent à la purge ou au nettoyage du système, du composant ou du dispositif. La fonction de purge et de nettoyage peut être mise en œuvre de différentes façons, notamment en remplaçant les données ou l'information à plusieurs reprises ou en détruisant la clé nécessaire au déchiffrage des données chiffrées.

Références :

GRC, G1-001, *Guide d'équipement de sécurité* [Référence 15].
CST, ITSG-06, *Effacement et déclassification des supports d'information électroniques* [Référence 16].
GRC, B2-002, *Produits de réécriture des supports de TI et d'effacement sécurisé* [Référence 44].
GRC, G2-003, *Lignes directrices sur l'élimination et la destruction des renseignements protégés sur disques durs* [Référence 54].
CST, ITSD-03A, *Directive sur le contrôle du matériel COMSEC au sein du gouvernement du Canada* [Référence 36].
SCT, *Avis de mise en œuvre de la Politique sur la technologie de l'information 2014-01* [Référence 68].

MP-7 UTILISATION DES SUPPORTS

Contrôle :

(A) L'organisation [*Sélection : limite, interdit*] l'utilisation de [*Affectation : types de supports de support d'information définis par l'organisation*] sur les [*Affectation : systèmes d'information ou composants système définis par l'organisation*] au moyen de [*Affectation : mesures de protection définies par l'organisation*].

Conseils supplémentaires : Les supports utilisés pour les systèmes d'information incluent autant les supports numériques que les supports non numériques. Les supports numériques comprennent, par exemple, les disquettes, les bandes magnétiques, les disques durs externes ou amovibles, les clés USB, les disques compacts et les vidéodisques numériques. Les supports non numériques comprennent, notamment, le papier et les microfilms. Ce contrôle s'applique également aux dispositifs mobiles dotés d'une capacité de stockage d'information (p. ex.

téléphones intelligents, tablettes, liseuses). Contrairement au contrôle MP-2, qui restreint l'accès des utilisateurs aux supports, ce contrôle limite l'utilisation de certains types de supports sur les systèmes d'information comme, entre autres, restreindre/interdire l'utilisation de clés USB ou de lecteurs de disques durs externes. L'organisation peut employer des mesures de protection techniques et non techniques (p. ex. des politiques, des procédures, des règles de conduite) pour restreindre l'utilisation de supports de système d'information. Elle peut restreindre l'utilisation de dispositifs de stockage portatifs en mettant notamment en place des cages sur les postes de travail pour interdire l'accès à certains ports externes ou en désactivant la fonction qui permet d'insérer, de lire ou d'écrire sur de tels dispositifs. L'organisation peut de plus limiter l'utilisation des dispositifs de stockage portatifs de manière à n'autoriser que les dispositifs approuvés comme, par exemple, ceux fournis par l'organisation, ceux fournis par d'autres organisations approuvées et ceux qui n'appartiennent pas au personnel. Elle peut enfin restreindre l'utilisation de dispositifs de stockage portatifs en fonction du type de dispositif, notamment en interdisant l'utilisation de dispositifs de stockage portatifs inscriptibles et en désactivant la fonction qui permet d'écrire sur de tels dispositifs. Contrôles connexes : AC-19, PL-4.

Améliorations du contrôle :

(1) UTILISATION DES SUPPORTS | INTERDIRE L'UTILISATION SANS PROPRIÉTAIRE

L'organisation interdit dans ses systèmes d'information l'utilisation de dispositifs de stockage portatifs dont le propriétaire est inconnu.

Conseils supplémentaires sur l'amélioration : Exiger que les dispositifs de stockage portatifs soient attribuables à des propriétaires identifiables (p. ex. des personnes, des organisations ou des projets) pour réduire le risque d'utilisation de ces technologies, car on sait à qui attribuer la responsabilité de régler les vulnérabilités connues des dispositifs (p. ex. insertion de code malveillant). Contrôle connexe : PL-4.

(2) UTILISATION DES SUPPORTS | INTERDIRE L'UTILISATION DE SUPPORTS RÉSISTANT AU NETTOYAGE

L'organisation interdit l'utilisation des supports résistant au nettoyage dans ses systèmes d'information.

Conseils supplémentaires sur l'amélioration : La résistance au nettoyage touche la capacité à nettoyer l'information qui se trouve sur les supports. Certains types de supports ne prennent pas en charge les commandes de nettoyage ou, si c'est le cas, n'emploient pas d'interfaces communes à chacun. Les supports résistant au nettoyage comprennent notamment les cartes flash compactes, les lecteurs flash intégrés aux cartes et aux dispositifs, les disques électroniques et les supports amovibles USB. Contrôle connexe : MP-6.

Références :

SCT, *Avis de mise en œuvre de la Politique sur la technologie de l'information 2014-01 [Référence 68]*.

MP-8 DÉCLASSEMENT DES SUPPORTS

Contrôle :

(A) L'organisation définit le [*Affectation : processus de déclassement des supports de système d'information défini par l'organisation*] associé notamment à l'utilisation de mécanismes de déclassement avec [*Affectation : force et intégrité définies par l'organisation*].

(B) L'organisation veille à ce que le processus de déclassement des supports de système d'information corresponde à la catégorie de sécurité et/ou au niveau de classification de l'information à supprimer et des autorisations d'accès des potentiels destinataires de l'information déclassée.

(C) L'organisation identifie les [*Affectation : supports de système d'information à déclasser définis par l'organisation*].

(D) L'organisation emploie le processus établi pour déclasser les supports de système d'information.

Conseils supplémentaires : Ce contrôle s'applique à tous les supports numériques et non numériques de système d'information susceptibles d'être diffusés à l'extérieur de l'organisation, qu'ils soient amovibles ou non. Lorsqu'il est appliqué aux supports du système, le processus de déclassement supprime l'information des supports, généralement selon la catégorie de sécurité ou le niveau de classification, de manière à rendre l'information irrécupérable et impossible à reconstituer. Le déclassement des supports comprend la rédaction de l'information aux fins de divulgation et de distribution à un plus vaste public. Le déclassement des supports permet également de s'assurer que l'espace libre qui se trouve sur les supports (p. ex. les espaces vides dans les fichiers) est dépourvu d'information.

Améliorations du contrôle :

(1) DÉCLASSEMENT DES SUPPORTS | DOCUMENTATION DU PROCESSUS

L'organisation documente les mesures de déclassement des supports de système d'information.

Conseils supplémentaires sur l'amélioration : L'organisation peut documenter le processus de déclassement des supports en fournissant de l'information comme la technique de déclassement employée, le numéro d'identification des supports déclassés et l'identité des personnes qui ont autorisé et/ou effectué le déclassement.

(2) DÉCLASSEMENT DES SUPPORTS | MISE À L'ESSAI DU MATÉRIEL

L'organisation emploie des [*Affectation : tests définis par l'organisation*] de déclassement de l'équipement et des procédures pour s'assurer de leur bon rendement [*Affectation : fréquence définie par l'organisation*].

(3) DÉCLASSEMENT DES SUPPORTS | INFORMATION NON CLASSIFIÉE CONTRÔLÉE

L'organisation déclasse les supports de système d'information qui contiennent [*Affectation : information protégée définie par l'organisation*] avant de les rendre publics conformément aux normes et politiques du GC et de l'organisation.

(4) DÉCLASSEMENT DES SUPPORTS | INFORMATION CLASSIFIÉE

Conformément aux normes et aux politiques, l'organisation déclasse les supports de système d'information qui contiennent de l'information classifiée avant de les remettre à des personnes qui ne disposent pas des droits d'accès requis.

Conseils supplémentaires sur l'amélioration : Le déclassement de l'information classifiée s'effectue au moyen d'outils, de techniques et de procédures de nettoyage approuvés et vise à transférer l'information confirmée non classifiée des systèmes d'information classifiés à des supports non classifiés.

Références :

SCT, *Avis de mise en œuvre de la Politique sur la technologie de l'information 2014-01* [Référence 68].
CST, ITSG-06, *Effacement et déclassification des supports d'information électroniques* [Référence 16].

3.11 FAMILLE : PROTECTION PHYSIQUE ET ENVIRONNEMENTALE

CLASSE : OPÉRATIONNELLE

PE-1 POLITIQUE ET PROCÉDURES DE PROTECTION PHYSIQUE ET ENVIRONNEMENTALE

Contrôle :

(A) L'organisation élabore et consigne, ainsi que diffuse aux [*Affectation : personnel ou rôles définis par l'organisation*] :

(a) une politique officielle et documentée qui définit les divers aspects de la protection physique et environnementale (but, portée, rôles, responsabilité, engagement de la direction, coordination entre les entités organisationnelles et conformité);

(b) des procédures visant à faciliter la mise en œuvre de la politique en matière de protection physique et environnementale, et des contrôles connexes.

(B) L'organisation examine et met à jour :

(a) la politique de protection physique et environnementale [*Affectation : fréquence définie par l'organisation*];

(b) les procédures de protection physique et environnementale [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : Ce contrôle porte sur l'établissement de la politique et les procédures nécessaires à la mise en œuvre efficace des contrôles de sécurité et des améliorations dans la famille PE. La politique et les procédures de protection physique et environnementale reflètent les lois du GC et les politiques, directives et normes applicables du SCT. Les politiques et les procédures du programme de sécurité mises en place à l'échelle de l'organisation peuvent rendre inutile toute politique et procédure propre à un système. La politique peut être intégrée à la politique générale sur la sécurité de l'information de l'organisation ou, inversement, elle peut être représentée par de multiples politiques compte tenu de la nature complexe de certaines organisations. Les procédures peuvent être établies pour le programme de sécurité général et pour des systèmes d'information particuliers, au besoin. La stratégie organisationnelle de gestion des risques est un facteur clé dans l'établissement de la politique et des procédures.

Améliorations du contrôle :

Aucune

Références :

SCT, *Norme opérationnelle sur la sécurité matérielle* [Référence 6].
SCT, *Norme opérationnelle de sécurité — Gestion de la sécurité des technologies de l'information* [Référence 7].
GRC, G1-025, *Protection, détection et intervention* [Référence 51].

PE-2 AUTORISATIONS D'ACCÈS PHYSIQUE

Contrôle :

(A) L'organisation élabore, approuve et maintient une liste des personnes autorisées à accéder aux installations où se trouve le système d'information.

(B) L'organisation délivre des justificatifs d'autorisation pour accéder aux installations.

(C) L'organisation passe en revue la liste d'accès qui fournit les détails quant aux personnes autorisées à accéder aux installations [*Affectation : fréquence définie par l'organisation*].

(D) L'organisation retire de la liste d'accès le nom des personnes qui n'ont plus à accéder aux installations.

Conseils supplémentaires : Ce contrôle s'applique aux employés et aux visiteurs de l'organisation. Les personnes (employés, entrepreneurs et autres) qui possèdent des justificatifs d'autorisation permanents pour accéder physiquement à l'installation ne sont pas considérées des visiteurs. Les justificatifs d'autorisation comprennent notamment les laissez-passer, les cartes d'identité et les cartes à puce. L'organisation détermine la robustesse des justificatifs d'autorisation nécessaires (y compris le niveau des laissez-passer, cartes à puce ou cartes d'identification anti-falsification) en vertu des directives, des normes, des politiques et des procédures du GC. Ce contrôle ne s'applique qu'aux zones de l'installation qui n'ont pas été désignées comme publiques. Contrôles connexes : PE-3, PE-4 et PS-3.

Améliorations du contrôle :

(1) AUTORISATIONS D'ACCÈS PHYSIQUE | ACCÈS PAR POSTE / RÔLE

L'organisation autorise, selon le poste ou le rôle de l'employé, l'accès physique à l'installation qui héberge le système d'information.

Conseils supplémentaires sur l'amélioration : Contrôles connexes : AC-2, AC-3 et AC-6.

(2) AUTORISATIONS D'ACCÈS PHYSIQUE | DEUX FORMES D'IDENTIFICATION

L'organisation exige deux formes d'identification de [*Affectation : liste des formes acceptables d'identification définie par l'organisation*] pour permettre l'accès des visiteurs à l'installation qui héberge le système d'information.

Conseils supplémentaires sur l'amélioration : Les formes de documents d'identification avec photo délivrés par le gouvernement comprennent notamment les passeports, les cartes de vérification d'identité personnelle (VIP) et les permis de conduire. Pour obtenir accès à l'installation au moyen de mécanismes automatisés, l'organisation peut avoir recours à des cartes VIP, des cartes-clés, des numéros d'identification personnels et à la biométrie. Contrôles connexes : IA-2, IA-3, IA-5.

(3) AUTORISATIONS D'ACCÈS PHYSIQUE | ACCÈS RESTREINT SANS ESCORTE

L'organisation restreint les accès sans escorte à l'installation qui héberge le système d'information au personnel qui [*Sélection (une ou plusieurs) : possède les habilitations de sécurité pour toute l'information contenue dans le système; est formellement autorisé à accéder à toute l'information contenue dans le système; nécessite un accès à toute l'information contenue dans le système; [Affectation : justificatifs d'identification définis par l'organisation*]].

Conseils supplémentaires sur l'amélioration : En raison de la nature hautement sensible de l'information classifiée stockée dans certaines installations, il est important que des personnes possédant les habilitations adéquates escortent les visiteurs non habilités, non autorisés à accéder aux installations ou ne répondant pas au besoin de connaître afin d'éviter que l'information ne sont exposée ou compromise. Contrôles connexes : PS-2, PS-6.

(100) L'organisation émet à chaque membre de son personnel une carte d'identité qui inclut, au minimum, le nom de l'organisation, la photo et le nom du titulaire, un numéro de carte unique et une date d'expiration.

Références :

SCT, *Norme opérationnelle sur la sécurité matérielle* [Référence 6].
CST, *ITSD-03A, Directive sur le contrôle du matériel COMSEC au sein du gouvernement du Canada* [Référence 36].
GRC, *G1-005, Guide pour la préparation d'un énoncé de sécurité matérielle* [Référence 45].
GRC, *G1-006, Cartes d'identité / Insignes d'accès* [Référence 46].

GRC, *G1-024, Contrôle de l'accès* [Référence 50].
GRC, *G1-025, Protection, détection et intervention* [Référence 51].

PE-3 CONTRÔLE D'ACCÈS PHYSIQUE

Contrôle :

(A) L'organisation applique les autorisations d'accès physique à [*Affectation : points d'entrée/de sortie à l'installation qui héberge le système d'information définis par l'organisation*] de la façon suivante :

(a) en vérifiant les autorisations d'accès individuelles avant d'accorder l'accès à l'installation;

(b) en contrôlant l'entrée et la sortie de l'installation au moyen [*Sélection (une ou plusieurs) : [Affectation : systèmes/dispositifs de contrôle d'accès physique définis par l'organisation]; de gardiens*].

(B) L'organisation maintient des registres de vérification des accès physiques aux [*Affectation : points d'entrée/de sortie définis par l'organisation*].

(C) L'organisation met en place des [*Affectation : mesures de sécurité définies par l'organisation*] afin de contrôler l'accès aux zones officiellement désignées comme étant accessibles au public au sein de l'installation.

(D) L'organisation escorte les visiteurs et surveille leurs activités [*Affectation : circonstances définies par l'organisation qui requièrent l'escorte et la surveillance des visiteurs*].

(E) L'organisation protège les clés, les combinaisons et autres dispositifs de contrôle d'accès physique.

(F) L'organisation fait l'inventaire des [*Affectation : dispositifs d'accès physique définis par l'organisation*] tous les [*Affectation : fréquence définie par l'organisation*].

(G) L'organisation modifie les combinaisons et les clés [*Affectation : fréquence définie par l'organisation*] lorsque des clés sont perdues, lorsque des combinaisons sont compromises ou lorsque des employés sont transférés ou quittent leur poste.

Conseils supplémentaires : Le contrôle de l'accès aux zones d'accès restreint et autres locaux de l'organisation doit être effectué de manière à ne pas contrevenir aux exigences relatives à la sécurité des personnes énoncées dans le *Code national du bâtiment (CNB) 2010* [Référence 19], le *Code national de prévention des incendies (CNPI) 2005* [Référence 20] et autres codes, normes et lignes directrices connexes. Se reporter au document intitulé *Éléments du Code national du bâtiment 1995 touchant la sécurité (G1-007)* de la GRC [Référence 21] pour plus de détails.

Ce contrôle s'applique aux employés et aux visiteurs de l'organisation. Les personnes (employés, entrepreneurs et autres) qui possèdent des justificatifs d'autorisation permanents pour accéder physiquement à l'installation ne sont pas considérées des visiteurs. L'organisation détermine les types d'agent de sécurité appropriés, par exemple, des professionnels de la sécurité physique ou autres personnes tels des employés de l'administration ou des utilisateurs du système d'information. Les dispositifs de contrôle d'accès physique comprennent notamment les clés, les cadenas, les combinaisons et les lecteurs de cartes. Les mesures de protection applicables aux zones accessibles au public au sein des installations de l'organisation comprennent, entre autres, des caméras, une surveillance menée par des gardes et l'isolement des systèmes d'information et/ou des composants système sélectionnés dans les zones sécurisées. Les systèmes de contrôle d'accès physique sont conformes aux lois du GC ainsi qu'aux politiques, aux directives et aux normes applicables du SCT. Les organisations peuvent employer les types de journaux de vérification de leur choix. Les journaux de vérification peuvent être basés sur les procédures (p. ex. un registre permettant de consigner le nom des personnes qui accèdent à l'installation ainsi que l'heure et la date de l'accès en question), autorisés (p. ex. générer l'identifiant inscrit sur une carte VIP) ou une

combinaison des deux options. Les points d'accès physique peuvent comprendre les points d'accès à l'installation, les points d'accès intérieur aux systèmes d'information et/ou aux composants qui exigent des contrôles d'accès supplémentaires, ou les deux. Les composants des systèmes d'information organisationnels (p. ex. les postes de travail, les terminaux) peuvent être situés dans des zones désignées comme étant accessibles au public si l'organisation protège l'accès à ces dispositifs. Contrôles connexes : AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3.

Améliorations du contrôle :

(1) CONTRÔLE D'ACCÈS PHYSIQUE | ACCÈS AU SYSTÈME D'INFORMATION

L'organisation applique les autorisations d'accès physique au système d'information en plus des contrôles d'accès physique à l'installation qui se trouve dans [*Affectation : espaces physiques définis par l'organisation qui contiennent un ou plusieurs composants du système d'information*].

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle offre une plus grande sécurité physique dans ces secteurs de l'installation où se retrouvent la plupart des composants du système d'information (p. ex. salles de serveurs, aires d'entreposage des supports, centres de données et de communications). Contrôle connexe : PS-2.

(2) CONTRÔLE D'ACCÈS PHYSIQUE | FRONTIÈRES DE L'INSTALLATION / DU SYSTÈME D'INFORMATION

L'organisation effectue des vérifications de sécurité [*Affectation : fréquence définie par l'organisation*] au périmètre physique de l'installation ou du système d'information pour détecter toute exfiltration non autorisée d'information ou retrait de composant de système d'information.

Conseils supplémentaires sur l'amélioration : L'organisation détermine la portée, la fréquence et/ou le caractère aléatoire des vérifications de sécurité pour atténuer de manière adéquate les risques associés aux exfiltrations. Contrôles connexes : AC-4, SC-7.

(3) CONTRÔLE D'ACCÈS PHYSIQUE | GARDE CONTINUE / ALARMES / SURVEILLANCE

L'organisation emploie des gardes pour surveiller, 24 heures par jour et 7 jours par semaine, tous les points d'accès physique de l'installation qui héberge le système d'information et émet des alarmes, le cas échéant.

Conseils supplémentaires sur l'amélioration : Contrôles connexes : CP-6, CP-7.

(4) CONTRÔLE D'ACCÈS PHYSIQUE | CONTENANTS VERROUILLABLES

L'organisation utilise des contenants verrouillables pour protéger [*Affectation : composants de système d'information définis par l'organisation*] contre les accès physiques non autorisés.

(5) CONTRÔLE D'ACCÈS PHYSIQUE | PROTECTION ANTITRAFIQUAGE

L'organisation emploie des [*Affectation : mesures de protection de sécurité définies par l'organisation*] pour [*Sélection (un ou plusieurs) : détecter; empêcher*] le trafiquage physique ou la modification des [*Affectation : composants matériels définis par l'organisation*] du système d'information.

Conseils supplémentaires sur l'amélioration : L'organisation peut mettre en place des mesures de détection et de prévention du trafiquage sur les composants matériels sélectionnés, ou encore des mesures de détection sur certains et des mesures de prévention sur d'autres. Les activités de détection et de prévention du trafiquage peuvent utiliser plusieurs types de mécanismes d'inviolabilité, notamment des étiquettes et des revêtements d'inviolabilité. Les programmes antitrafiquage permettent de détecter les modifications apportées au matériel à la suite d'un acte de contrefaçon et d'autres risques liés à la chaîne d'approvisionnement. Contrôle connexe : SA-12.

(6) CONTRÔLE D'ACCÈS PHYSIQUE | TEST DE PÉNÉRATION DES INSTALLATIONS

L'organisation utilise un processus de test de pénétration qui comprend [*Affectation : fréquence définie par l'organisation*] tentatives inopinées de contournement des contrôles de sécurité associés aux points d'accès physique de l'installation.

Conseils supplémentaires sur l'amélioration : Contrôles connexes : CA-2, CA-7.

Références :

TPSGC, *Manuel de la sécurité industrielle* [Référence 2].
SCT, *Norme opérationnelle sur la sécurité matérielle* [Référence 6].
Code national du bâtiment (CNB) 2010 [Référence 19].
Code national de prévention des incendies (CNPI) 2010 [Référence 20].
GRC, G1-010, *Éléments du Code national du bâtiment 1995 touchant la sécurité* [Référence 21].
CST, *ITSD-03A, Directive sur le contrôle du matériel COMSEC au sein du gouvernement du Canada* [Référence 36].
GRC, *G1-005, Guide pour la préparation d'un énoncé de sécurité matérielle* [Référence 45].
GRC, *G1-007, Scellage de protection des clés d'urgence et passe-partout ou des serrures à code d'immeubles* [Référence 47].
GRC, *G1-008, Lignes directrices visant les services de gardiens* [Référence 48].
GRC, *G1-016, Les systèmes de clés maîtresses* [Référence 49].
GRC, *G1-024, Contrôle de l'accès* [Référence 50].
GRC, *G1-025, Protection, détection et intervention* [Référence 51].
GRC, *G1-026, Guide pour l'établissement des zones de sécurité matérielle* [Référence 52].
GRC, *G1-029, Pièces sécuritaires* [Référence 23].
GRC, *G1-031, Protection matérielle des serveurs informatiques* [Référence 53].

PE-4 CONTRÔLE D'ACCÈS AUX SUPPORTS DE TRANSMISSION

Contrôle :

(A) L'organisation contrôle l'accès physique aux [*Affectation : lignes de distribution et de transmission du système d'information définies par l'organisation*] dans ses installations utilisant les [*Affectation : mesures de protection de sécurité définies par l'organisation*].

Conseils supplémentaires : Les mesures de protection de sécurité appliquées aux lignes de distribution et de transmission du système d'information permettent de prévenir les dommages accidentels, les interruptions et le trafiquage physique. Elles pourraient de plus s'avérer nécessaires pour aider à prévenir l'écoute clandestine ou la modification en transit des transmissions non chiffrées. Les mesures de protection de sécurité utilisées pour contrôler l'accès physique aux lignes de distribution et de transmission du système comprennent entre autres : (i) le verrouillage des armoires de câblage, (ii) la déconnexion ou le verrouillage des connecteurs non utilisés et (iii) la protection du câblage par des conduits ou des chemins de câbles. Contrôles connexes : MP-2, MP-4, PE-2, PE-3, PE-5, SC-7, SC-8.

Améliorations du contrôle :

Aucune

Références :

GRC, *G1-005, Guide pour la préparation d'un énoncé de sécurité matérielle* [Référence 45].
GRC, *G1-026, Guide pour l'établissement des zones de sécurité matérielle* [Référence 52].

PE-5 CONTRÔLE D'ACCÈS AUX DISPOSITIFS DE SORTIE

Contrôle :

(A) L'organisation contrôle l'accès physique aux dispositifs de sortie du système d'information pour empêcher les personnes non autorisées d'obtenir les sorties.

Conseils supplémentaires : Le contrôle de l'accès physique aux dispositifs de sortie peuvent comprendre, en autres, la mise en place des dispositifs de sortie dans des salles verrouillées ou d'autres zones sécurisées auxquelles seules les personnes autorisées sont mesure d'accéder, et la mise en place des dispositifs de sortie dans des lieux où ils peuvent être surveillés par le personnel de l'organisation. Les dispositifs de sortie du système d'information comprennent notamment les moniteurs, les imprimantes, les photocopieurs, les numériseurs, les télécopieurs et autres dispositifs audio. Contrôles connexes : PE-2, PE-3, PE-4, PE-18.

Améliorations du contrôle :

(1) CONTRÔLE D'ACCÈS AUX DISPOSITIFS DE SORTIE | ACCÈS AUX DONNÉES DE SORTIE ACCORDÉ AUX PERSONNES AUTORISÉES

(a) L'organisation contrôle l'accès physique aux données transmises par les [*Affectation : dispositifs de sortie définis par l'organisation*];

(b) L'organisation veille à ce que seules les personnes autorisées reçoivent les données transmises par le dispositif.

Conseils supplémentaires sur l'amélioration : Le contrôle de l'accès physique aux dispositifs de sortie sélectionnés peut comprendre, en autres, la mise en place des imprimantes, des photocopieurs et des télécopieurs dans des zones contrôlées au moyen d'un pavé numérique ou la limitation de l'accès à certains types de laissez-passer.

(2) CONTRÔLE D'ACCÈS AUX DISPOSITIFS DE SORTIE | ACCÈS AUX DONNÉES DE SORTIE ACCORDÉ EN FONCTION DES IDENTITÉS DES INDIVIDUS

(a) Le système d'information contrôle l'accès physique aux données transmises par les [*Affectation : dispositifs de sortie définis par l'organisation*];

(b) Le système d'information associe l'identité des individus aux données transmises par le dispositif.

Conseils supplémentaires sur l'amélioration : Le contrôle de l'accès physique aux dispositifs de sortie sélectionnés peut comprendre, en autres, la mise en place de fonctions de sécurité sur les imprimantes, les photocopieurs et les télécopieurs permettant à l'organisation d'authentifier les utilisateurs (p. ex. au moyen d'un NIP ou d'un jeton matériel) sur les dispositifs de sortie avant de leur transmettre les données de sortie.

(3) CONTRÔLE D'ACCÈS AUX DISPOSITIFS DE SORTIE | MARQUAGE DES DISPOSITIFS DE SORTIE

L'organisation appose sur les [*Affectation : dispositifs de sortie du système d'information définis par l'organisation*] la classification appropriée de l'information pouvant être tirées du dispositif.

Conseils supplémentaires sur l'amélioration : Les dispositifs de sortie comprennent notamment les imprimantes, les moniteurs, les télécopieurs, les numériseurs, les photocopieurs et les dispositifs audio. Cette amélioration de contrôle vise généralement les dispositifs de sortie du système d'information autres que les dispositifs mobiles.

Références :

GRC, *G1-026, Guide pour l'établissement des zones de sécurité matérielle* [Référence 52].

PE-6 SURVEILLANCE DE L'ACCÈS PHYSIQUE

Contrôle :

(A) L'organisation surveille l'accès physique à l'installation qui héberge le système d'information afin de détecter les incidents de sécurité physique et d'y répondre.

(B) L'organisation examine les journaux d'accès physique [*Affectation : fréquence définie par l'organisation*] et advenant [*Affectation : événements ou indications potentielles d'événements définis par l'organisation*].

(C) L'organisation coordonne les résultats des examens et des enquêtes avec sa capacité d'intervention en cas d'incident.

Conseils supplémentaires : La capacité d'intervention de l'organisation comprend les enquêtes et les interventions liées aux incidents de sécurité physique. Les incidents de sécurité comprennent notamment les atteintes à la sécurité apparentes et les activités suspectes, à savoir, (i) les accès hors des heures normales de travail; (ii) les accès répétés aux zones auxquelles on n'accède généralement pas; (iii) les accès qui durent plus longtemps que d'habitude; et (iv) les accès hors fréquence. Contrôles connexes : CA-7, IR-4, IR-8.

Améliorations du contrôle :

(1) SURVEILLANCE DE L'ACCÈS PHYSIQUE | ALARMES DE DÉTECTION D'INTRUSION / ÉQUIPEMENT DE SURVEILLANCE

L'organisation surveille les alarmes de détection d'intrusion physique et l'équipement de surveillance.

(2) SURVEILLANCE DE L'ACCÈS PHYSIQUE | RECONNAISSANCE DES INTRUSIONS / INTERVENTIONS

L'organisation fait appel à des mécanismes automatisés pour reconnaître [*Affectation : classes ou types d'intrusions définis par l'organisation*] et appliquer [*Affectation : mesures d'intervention définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Contrôle connexe : SI-4.

(3) SURVEILLANCE DE L'ACCÈS PHYSIQUE | SURVEILLANCE VIDÉO

L'organisation fait appel à la surveillance vidéo des [*Affectation : zones opérationnelles définies par l'organisation*] et conserve les enregistrements vidéo pendant [*Affectation : période définie par l'organisation*].

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle vise l'enregistrement de la surveillance vidéo aux fins d'examen ultérieur, si les circonstances le justifient (p. ex. une tentative d'infraction détectée par d'autres moyens). À moins que l'organisation ne l'exige, aucune supervision de la surveillance vidéo n'est requise. Il pourrait être nécessaire de tenir compte de certaines considérations juridiques au moment de procéder à la surveillance vidéo et d'en conserver les enregistrements, tout particulièrement si une telle surveillance est réalisée dans un lieu public.

(4) SURVEILLANCE DE L'ACCÈS PHYSIQUE | SURVEILLANCE DE L'ACCÈS PHYSIQUE AUX SYSTÈMES D'INFORMATION

L'organisation surveille l'accès physique au système d'information en plus de surveiller l'installation qui se trouve dans [*Affectation : espaces physiques définis par l'organisation qui contiennent un ou plusieurs composants du système d'information*].

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle offre une plus grande surveillance des secteurs de l'installation où se retrouvent la plupart des composants du système d'information (p. ex. salles de serveurs, aires d'entreposage des supports, centres de communications). Contrôles connexes : PS-2, PS-3.

Références :

GRC, *G1-025, Protection, détection et intervention* [Référence 51].

PE-7 CONTRÔLE DES VISITEURS

[Annulé : Intégré aux contrôles PE-2 et PE-3]

PE-8 REGISTRE DES ACCÈS

Contrôle :

(A) L'organisation tient un registre des visiteurs qui accèdent à l'installation qui héberge le système d'information pendant [*Affectation : période définie par l'organisation*];

(B) L'organisation examine le registre des accès des visiteurs [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : Le registre des accès des visiteurs comprend, par exemple, le nom du visiteur et son organisation, sa signature, les formes d'identification, la date de l'accès, les heures d'arrivée et de départ, le but de la visite, et le nom et l'organisation de la personne visitée. Un tel registre n'est pas requis dans les lieux publics.

Améliorations du contrôle :

(1) REGISTRE DES VISITEURS | TENUE ET EXAMEN AUTOMATISÉS DU REGISTRE

L'organisation fait appel à des mécanismes automatisés pour faciliter la tenue et l'examen du registre des accès des visiteurs.

(2) REGISTRE DES VIAnuléSITEURS | REGISTRE DES ACCÈS PHYSIQUES

[Annulée : Intégrée au contrôle PE-2]

Références :

Aucune

PE-9 ÉQUIPEMENT ET CÂBLAGE D'ALIMENTATION

Contrôle :

(A) L'organisation protège l'équipement et le câblage d'alimentation du système d'information contre les dommages et la destruction.

Conseils supplémentaires : L'organisation détermine les types de protection nécessaires à l'équipement et au câble d'alimentation dans différents emplacements internes et externes de l'installation et de l'environnement opérationnel de l'organisation. Ceci comprend notamment les génératrices et le câblage d'alimentation à l'extérieur de l'édifice, le câblage interne et les sources d'alimentation sans coupure à l'intérieur d'un bureau ou d'un centre de données, et les sources d'alimentation provenant d'entités autonomes comme des véhicules et des satellites. Contrôle connexe : PE-4.

Améliorations du contrôle :

(1) ÉQUIPEMENT ET CÂBLAGE D'ALIMENTATION | CÂBLAGE REDONDANT

L'organisation emploie des chemins de câblage d'alimentation redondant, installés à une distance de [*Affectation : distance définie par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les câbles d'alimentation redondants distants permettent d'assurer une alimentation continue si l'un des câbles est coupé ou endommagé.

(2) ÉQUIPEMENT ET CÂBLAGE D'ALIMENTATION | CONTRÔLES DE TENSION AUTOMATISÉS

L'organisation utilise des contrôles de tension automatisés pour [*Affectation : composants essentiels du système d'information définis par l'organisation*].

Références :

Aucune

PE-10 ARRÊT D'URGENCE

Contrôle :

(A) L'organisation peut, en situation d'urgence, couper l'alimentation du système d'information ou des composants individuels connexes.

(B) L'organisation place des interrupteurs ou des dispositifs d'arrêt d'urgence dans [*Affectation : liste définie par l'organisation des emplacements par système d'information ou composant*] pour offrir au personnel un accès sûr et facile.

(C) L'organisation protège sa capacité d'interruption d'urgence de l'alimentation contre toute activation non autorisée.

Conseils supplémentaires : Ce contrôle s'applique principalement aux installations qui contiennent des concentrations de ressources de système d'information, notamment les centres de données, les salles de serveurs et les salles d'ordinateurs centraux. Contrôle connexe : PE-15.

Améliorations du contrôle :

(1) ARRÊT D'URGENCE | ACTIVATION NON AUTORISÉE

[Annulée : Intégrée au contrôle PE-10]

Références :

Aucune

PE-11 ALIMENTATION D'URGENCE

Contrôle :

(A) L'organisation prévoit une alimentation électronique interruptible à court terme pour faciliter [*Sélection (un ou plusieurs) : l'arrêt ordonné du système d'information; le réacheminement du système d'information vers une source d'alimentation de secours à long terme*] dans l'éventualité d'une perte de la source d'alimentation principale.

Conseils supplémentaires : Contrôles connexes : AT-3, CP-2, CP-7.

Améliorations du contrôle :

(1) ALIMENTATION D'URGENCE | SOURCE D'ALIMENTATION DE SECOURS À LONG TERME — CAPACITÉ OPÉRATIONNELLE MINIMALE

L'organisation prévoit pour le système d'information une source d'alimentation de secours à long terme capable de maintenir la capacité opérationnelle minimale requise dans l'éventualité d'une perte prolongée de la source d'alimentation principale.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle peut être réalisée, par exemple, par l'utilisation d'un bloc d'alimentation commercial secondaire ou d'une autre source

d'alimentation externe. Les sources d'alimentation de secours à long terme du système d'information peuvent être activées manuellement ou automatiquement.

(2) ALIMENTATION D'URGENCE | SOURCE D'ALIMENTATION DE SECOURS À LONG TERME — AUTONOME

L'organisation procure au système d'information une source d'alimentation de secours à long terme à la fois :

(a) autonome;

(b) indépendante de toute source d'alimentation externe;

(c) capable de maintenir [*Sélection : la capacité opérationnelle minimale requise; une capacité opérationnelle totale*] dans l'éventualité d'une perte prolongée de la source d'alimentation principale.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle peut être réalisée, par exemple, par l'utilisation d'une ou plusieurs génératrices possédant la capacité suffisante pour répondre aux besoins de l'organisation. Les sources d'alimentation de secours à long terme des systèmes d'information de l'organisation peuvent être activées manuellement ou automatiquement.

Références :

Aucune

PE-12 ÉCLAIRAGE DE SÉCURITÉ

Contrôle :

(A) L'organisation utilise et entretient, pour le système d'information, un système automatique d'éclairage de sécurité qui entre en fonction lorsqu'il y a coupure ou interruption de courant et qui éclaire les sorties d'urgence et les chemins d'évacuation dans l'installation.

Conseils supplémentaires : Ce contrôle s'applique principalement aux installations qui contiennent des concentrations de ressources de système d'information, notamment les centres de données, les salles de serveurs et les salles d'ordinateurs centraux. Contrôles connexes : CP-2, CP-7.

Améliorations du contrôle :

(1) ÉCLAIRAGE DE SÉCURITÉ | FONCTIONS OPÉRATIONNELLES ET DE MISSION ESSENTIELLES

L'organisation prévoit l'éclairage de sécurité de toutes les zones de l'installation prenant en charge les fonctions opérationnelles et de mission essentielles.

Références :

Aucune

PE-13 PROTECTION CONTRE L'INCENDIE

Contrôle :

(A) L'organisation utilise et maintient, pour le système d'information, des dispositifs et systèmes de détection et d'extinction d'incendie alimentés par une source d'énergie indépendante.

Conseils supplémentaires : Ce contrôle s'applique principalement aux installations qui contiennent des concentrations de ressources de système d'information, notamment les centres de données, les salles de serveurs et les salles d'ordinateurs centraux. Les dispositifs ou systèmes de détection et d'extinction d'incendie

comprennent, par exemple, les systèmes de gicleurs, les extincteurs manuels, les boyaux d'arrosage fixes et les détecteurs de fumée.

Améliorations du contrôle :

(1) PROTECTION CONTRE L'INCENDIE | DISPOSITIFS ET SYSTÈMES DE DÉTECTION

L'organisation utilise, pour le système d'information, des dispositifs ou systèmes de détection d'incendie qui s'activent automatiquement et informent [*Affectation : personnel ou rôles définis par l'organisation*] et [*Affectation : intervenants d'urgence définis par l'organisation*] dans l'éventualité d'un incendie.

Conseils supplémentaires sur l'amélioration : L'organisation peut préciser le personnel, les rôles et les intervenants d'urgence advenant le cas où les personnes se trouvant sur la liste de notifications sont tenues d'avoir les autorisations d'accès et les habilitations de sécurité appropriées pour accéder aux installations où s'effectuent les opérations classifiées et où résident les systèmes d'information qui contiennent l'information classifiée.

(2) PROTECTION CONTRE L'INCENDIE | DISPOSITIFS ET SYSTÈMES D'EXTINCTION

L'organisation utilise, pour le système d'information, des dispositifs ou systèmes d'extinction d'incendie qui informent automatiquement [*Affectation : personnel ou rôles définis par l'organisation*] et les [*Affectation : intervenants d'urgence définis par l'organisation*] dès qu'ils sont activés.

Conseils supplémentaires sur l'amélioration : L'organisation peut préciser le personnel, les rôles et les intervenants d'urgence advenant le cas où les personnes se trouvant sur la liste de notifications sont tenues d'avoir les autorisations d'accès et les habilitations de sécurité appropriées pour accéder aux installations où s'effectuent les opérations classifiées et où résident les systèmes d'information qui contiennent l'information classifiée.

(3) PROTECTION CONTRE L'INCENDIE | EXTINCTION AUTOMATIQUE D'INCENDIE

L'organisation utilise, pour le système d'information, une capacité d'extinction automatique d'incendie lorsque l'installation n'a pas de personnel affecté de façon continue.

(4) PROTECTION CONTRE L'INCENDIE | INSPECTIONS

L'organisation s'assure que l'installation est [*Affectation : fréquence définie par l'organisation*] inspectée par des inspecteurs autorisés et qualifiés, et remédie aux problèmes relevés dans les [*Affectation : période définie par l'organisation*] suivants.

Références :

Aucune

PE-14 CONTRÔLE DE LA TEMPÉRATURE ET DE L'HUMIDITÉ

Contrôle :

(A) L'organisation maintient à [*Affectation : niveaux acceptables définis par l'organisation*] les niveaux de température et d'humidité dans l'installation qui héberge le système d'information.

(B) L'organisation surveille les niveaux de température et d'humidité [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : Ce contrôle s'applique principalement aux installations qui contiennent des concentrations de ressources de système d'information, notamment les centres de données, les salles de serveurs et les salles d'ordinateurs centraux. Contrôle connexe : AT-3.

Améliorations du contrôle :

(1) CONTRÔLE DE LA TEMPÉRATURE ET DE L'HUMIDITÉ | CONTRÔLES AUTOMATIQUES

L'organisation utilise des contrôles automatiques de la température et de l'humidité pour empêcher toute fluctuation potentiellement préjudiciable au système d'information.

(2) CONTRÔLE DE LA TEMPÉRATURE ET DE L'HUMIDITÉ | SURVEILLANCE AVEC ALARMES OU AVIS

L'organisation utilise un processus de surveillance de la température et de l'humidité qui déclenche une alarme ou un avis en cas de changements potentiellement préjudiciables au personnel ou à l'équipement.

Références :

Aucune

PE-15 PROTECTION CONTRE LES DÉGÂTS D'EAU

Contrôle :

(A) L'organisation protège le système d'information contre tout dommage causé par une fuite d'eau en recourant à des robinets d'arrêt ou d'isolement accessibles qui fonctionnent adéquatement et dont le personnel concerné connaît l'emplacement.

Conseils supplémentaires : Ce contrôle s'applique principalement aux installations qui contiennent des concentrations de ressources de système d'information, notamment les centres de données, les salles de serveurs et les salles d'ordinateurs centraux. Les robinets d'isolement peuvent être employés en plus ou à la place de robinets d'arrêt pour fermer l'approvisionnement en eau dans des zones données sans que toute l'organisation ne soit touchée. Contrôle connexe : AT-3.

Améliorations du contrôle :

(1) PROTECTION CONTRE LES DÉGÂTS D'EAU | SOUTIEN AUTOMATISÉ

L'organisation fait appel à des mécanismes automatisés pour détecter la présence d'eau à proximité du système d'information et en informer [*Affectation : personnel ou rôles définis par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les mécanismes automatisés comprennent notamment les détecteurs d'eau, les alarmes et les systèmes de notifications.

Références :

Aucune

PE-16 LIVRAISON ET RETRAIT

Contrôle :

(A) L'organisation autorise, surveille et contrôle l'entrée dans l'installation et la sortie de cette dernière des [*Affectation : types de composant de système d'information définis par l'organisation*] et tient à jour les dossiers pertinents.

Conseils supplémentaires : L'application réelle des autorisations d'entrée et de sortie des composants de système d'information peut exiger une restriction de l'accès aux aires de livraison et, éventuellement, leur isolation du système d'information et des bibliothèques de supports. Contrôles connexes : CM-3, MA-2, MA-3, MP-5, SA-12.

Améliorations du contrôle :

Aucune

Références :

GRC, *G1-024, Contrôle de l'accès* [Référence 50].

PE-17 AUTRES LIEUX DE TRAVAIL

Contrôle :

(A) L'organisation utilise [Affectation : *contrôles de sécurité définis par l'organisation*] dans les autres lieux de travail.

(B) L'organisation évalue dans la mesure du possible l'efficacité des contrôles de sécurité dans les autres lieux de travail.

(C) L'organisation permet aux employés de communiquer avec le personnel chargé de la sécurité de l'information en cas d'incidents ou de problèmes liés à la sécurité.

Conseils supplémentaires : Les autres lieux de travail peuvent comprendre, par exemple, des installations du gouvernement ou la résidence privée d'employés. Bien qu'ils se distinguent des autres sites de traitement, les autres lieux de travail peuvent constituer des alternatives facilement accessibles dans le cadre des opérations d'urgence. L'organisation peut définir différents ensembles de contrôles de sécurité pour des lieux de travail ou des types de site précis selon les activités professionnelles qui y sont menées. Contrôles connexes : AC-17, CP-7.

Améliorations du contrôle :

Aucune

Références :

SCT, *Norme opérationnelle sur la sécurité matérielle* [Référence 6].

PE-18 EMPLACEMENT DES COMPOSANTS DU SYSTÈME D'INFORMATION

Contrôle :

(A) L'organisation installe les composants du système d'information de manière à réduire au minimum les dommages que pourraient causer [*Affectation : risques physiques et environnementaux définis par l'organisation*], de même que les possibilités d'accès non autorisé.

Conseils supplémentaires : Les risques physiques et environnementaux comprennent, par exemple, les inondations, les incendies, les tornades, les tremblements de terre, les ouragans, les actes terroristes, le vandalisme, les impulsions électromagnétiques, les interférences électriques et d'autres formes de radiations électromagnétiques. De plus, l'organisation choisit l'emplacement des points d'entrée physique de manière à ce qu'aucune personne non autorisée, même si l'accès lui est interdit, ne puisse s'approcher du système d'information et, par conséquent, accéder illégalement aux communications (p. ex. à l'aide de renifleurs ou de microphones sans fil). Contrôles connexes : CP-2, PE-19, RA-3.

Améliorations du contrôle :

(1) EMPLACEMENT DES COMPOSANTS DU SYSTÈME D'INFORMATION | SITE DE L'INSTALLATION

L'organisation planifie l'emplacement ou le site de l'installation qui hébergera le système en tenant compte des dangers physiques et environnementaux et, dans le cas des installations existantes, tient compte de ces dangers dans sa stratégie d'atténuation des risques.

Références :

CST, *ITSG-02, Critères pour la conception, la fabrication, l'approvisionnement, l'installation et les essais de réception des enceintes blindées contre les radiofréquences* [Référence 35].
GRC, *G1-026, Guide pour l'établissement des zones de sécurité matérielle* [Référence 52].

PE-19 FUITES D'INFORMATION

Contrôle :

(A) L'organisation protège le système d'information contre les fuites d'information dues à l'émission de signaux électromagnétiques.

Conseils supplémentaires : On entend par fuite d'information toute divulgation intentionnelle ou non intentionnelle d'information à un environnement non fiabilisé due à l'émission de signaux électromagnétiques. La catégorisation ou la classification de sécurité des systèmes d'information (en ce qui a trait à la confidentialité) et les politiques de sécurité organisationnelles permettent de sélectionner les contrôles de sécurité employés pour protéger les systèmes contre les fuites d'information liées à l'émission de signaux électromagnétiques.

Améliorations du contrôle :

(1) FUITES D'INFORMATION | POLITIQUES ET PROCÉDURES NATIONALES EN MATIÈRE D'ÉMISSIONS / TEMPEST

L'organisation s'assure que les composants du système d'information, les communications de données connexes et les réseaux sont protégés conformément aux politiques et procédures nationales en ce qui a trait aux émissions et à la norme TEMPEST en tenant compte de la catégorie de sécurité ou de la classification de l'information.

Références :

CST, *ITSD-01A, Directives pour l'application de la sécurité des communications au sein du gouvernement du Canada*, [Référence 14].
CST, *ITSG-11, Planification des installations COMSEC – Conseils et critères TEMPEST* [Référence 37].
CST, *ITSG-12, Procédures d'évaluation des installations du gouvernement du Canada* [Référence 38].

PE-20 SURVEILLANCE ET SUIVI DES ACTIFS

Contrôle :

(A) L'organisation utilise [*Affectation : technologies associées à l'emplacement des actifs définies par l'organisation*] pour procéder au suivi et à la surveillance de l'emplacement et des déplacements des [*Affectation : actifs définis par l'organisation*] dans [*Affectation : zones contrôles définies par l'organisation*].

(B) L'organisation s'assure que les technologies associées à l'emplacement des actifs sont employées conformément à la législation du GC et aux politiques, aux directives et aux normes applicables du SCT.

Conseils supplémentaires : Grâce aux technologies associées à l'emplacement des actifs, l'organisation peut veiller à ce que les actifs essentiels, comme les véhicules ou les composants fondamentaux du système d'information, demeurent dans les emplacements autorisés. Elle consulte également le Bureau de l'avocat général et le chef de la protection des renseignements personnels (CPRP) au sujet du déploiement et de l'utilisation des technologies associées à l'emplacement des actifs afin de discuter de possibles préoccupations en matière de protection des renseignements personnels. Contrôle connexe : CM-8.

Améliorations du contrôle :

Aucune

Références :

SCT, *Cadre de politique sur la gestion des actifs et services acquis* [Référence 75]

3.12 FAMILLE : PLANIFICATION

CLASSE : GESTION

PL-1 POLITIQUE ET PROCÉDURES DE PLANIFICATION DE LA SÉCURITÉ

Contrôle :

(A) L'organisation élabore et consigne, ainsi que diffuse aux [*Affectation : personnel ou rôles définis par l'organisation*] :

(a) une politique de planification de la sécurité qui définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et le respect;

(b) des procédures pour faciliter la mise en œuvre de la politique de planification de la sécurité et des contrôles de planification de la sécurité connexes.

(B) L'organisation examine et met à jour :

(a) la politique de planification de la sécurité actuelle [*Affectation : fréquence définie par l'organisation*];

(b) les procédures de planification de la sécurité actuelles [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : Ce contrôle porte sur l'établissement de la politique et les procédures nécessaires à la mise en œuvre efficace des contrôles de sécurité et des améliorations dans la famille PL. La politique et les procédures de planification de la sécurité reflètent les lois du GC et les politiques, directives et normes applicables du SCT. Les politiques et les procédures du programme de sécurité mises en place à l'échelle de l'organisation peuvent rendre inutile toute politique et procédure propre à un système. La politique peut être intégrée à la politique générale sur la sécurité de l'information des organisations ou, inversement, elle peut être représentée par de multiples politiques compte tenu de la nature complexe de certaines organisations. Les procédures peuvent être établies pour le programme de sécurité général et pour des systèmes d'information particuliers, au besoin. La stratégie organisationnelle de gestion des risques est un facteur clé dans l'établissement de la politique et des procédures.

Améliorations du contrôle :

Aucune

Références :

SCT, *Norme opérationnelle de sécurité — Gestion de la sécurité des technologies de l'information* [Référence 7].

PL-2 PLAN DE SÉCURITÉ DU SYSTÈME

Contrôle :

(A) L'organisation développe pour le système d'information un plan de sécurité qui :

(a) est conforme à l'architecture d'entreprise de l'organisation;

(b) définit explicitement les limites d'autorisation pour le système;

(c) décrit le contexte opérationnel du système d'information sur le plan de la mission et des processus opérationnels;

(d) définit la catégorisation de sécurité du système d'information, y compris la justification à l'appui;

(e) décrit l'environnement opérationnel du système d'information de même que les relations ou les connexions avec les autres systèmes d'information;

(f) donne un aperçu des exigences en matière de sécurité pour le système d'information;

(g) détermine tous les compléments pertinents, le cas échéant;

(h) décrit les contrôles de sécurité existants ou prévus pour répondre à ces exigences, y compris la justification des décisions concernant l'adaptation des contrôles;

(i) est examiné et approuvé par l'autorité responsable ou un représentant désigné avant sa mise en œuvre.

(B) L'organisme distribue des copies du plan de sécurité et communique les changements qui y sont apportés par la suite aux [*Affectation : personnel ou rôles définis par l'organisation*].

(C) L'organisation examine le plan de sécurité du système d'information [*Affectation : fréquence définie par l'organisation*].

(D) L'organisation met le plan à jour pour tenir compte des changements apportés au système d'information ou à l'environnement d'exploitation, ou des problèmes soulevés lors de la mise en œuvre du plan ou des évaluations des contrôles de sécurité.

(E) L'organisation protège le plan de sécurité contre toute divulgation et modification non autorisées.

Conseils supplémentaires : Les plans de sécurité associent les exigences en matière de sécurité à un ensemble de contrôles de sécurité et d'améliorations de contrôle. Les plans de sécurité décrivent également, de façon générale, en quoi les contrôles de sécurité et les améliorations de contrôle satisfont aux exigences en matière de sécurité, sans pour autant fournir des descriptions détaillées et techniques de la conception ou la mise en œuvre de ces contrôles ou de ces améliorations. Ils contiennent suffisamment d'information (y compris la spécification explicite ou par référence des paramètres d'affectation et de sélection) pour permettre une conception et mise en œuvre clairement conforme à ses objectifs et la détermination subséquente des risques qu'il représente, s'il est appliqué, pour les activités et les biens de l'organisation, les personnes, les autres organisations et le Canada. L'organisation peut de plus appliquer l'orientation de personnalisation des contrôles de sécurité de base stipulés dans l'annexe 4 en vue de développer des compléments qui seront utilisés à l'échelle de la collectivité ou de se conformer à des exigences, des technologies, des missions ou des environnements d'opération spécialisés (p. ex. des tactiques du MDN, l'infrastructure à clé publique du GC ou ICAM).

Les plans de sécurité ne doivent pas être des documents uniques, mais plutôt une collection de différents documents, y compris ceux qui existent déjà. Des plans de sécurité efficaces renvoient largement aux politiques, aux procédures et à des documents additionnels (p. ex. les spécifications liées à la conception et à la mise en œuvre) dans lesquels il est possible d'obtenir de plus amples détails. Il est ainsi possible de réduire la documentation afférente aux programmes de sécurité et de conserver l'information relative à la sécurité dans d'autres secteurs opérationnels et de gestion établis en lien avec l'architecture d'entreprise, le cycle de développement des systèmes, l'ingénierie des systèmes et l'acquisition. Par exemple, les plans de sécurité ne comportent aucune information détaillée sur le plan de secours ou le plan d'intervention en cas d'incident. Ils fournissent plutôt suffisamment d'information, que ce soit explicitement et en référence, pour établir quels objectifs ces plans visent à atteindre. Contrôles connexes : AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-2, MP-4, MP-5, PL-7, SA-5, SA-17.

Améliorations du contrôle :

(1) PLAN DE SÉCURITÉ DU SYSTÈME | CONCEPT DES OPÉRATIONS

[Annulé : intégré au contrôle PL-7]

(2) PLAN DE SÉCURITÉ DU SYSTÈME | ARCHITECTURE FONCTIONNELLE

[Annulé : intégré au contrôle PL-8]

(3) PLAN DE SÉCURITÉ DU SYSTÈME | PLANIFIER ET COORDONNER AVEC D'AUTRES ENTITÉS ORGANISATIONNELLES

L'organisation planifie et coordonne les activités liées à la sécurité du système d'information avec [*Affectation : personnes ou groupes définis par l'organisation*] avant de les effectuer afin de réduire leur incidence sur les activités des autres entités organisationnelles.

Conseils supplémentaires sur l'amélioration : Les activités liées à la sécurité comprennent, par exemple, les évaluations de la sécurité, les vérifications, la maintenance matérielle et logicielle, la gestion des correctifs et les tests liés au plan d'urgence. La planification préliminaire et la coordination englobent les situations urgentes et celles qui ne le sont pas (c.-à-d. planifiées ou non urgentes et non planifiées). Le processus défini par l'organisation en vue de planifier et de coordonner les activités liées à la sécurité peut être ajouté aux plans de sécurité mis en place pour les systèmes d'information ou à d'autres documents, le cas échéant. Contrôles connexes : CP-4, IR-4.

Références :

SCT, *Guide de vérification – Sécurité des technologies de l'information* [Référence 29].
SCT, *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* [Référence 7].

PL-3 MISE À JOUR DU PLAN DE SÉCURITÉ DES SYSTÈMES

[Annulé : intégré au contrôle PL-2]

PL-4 RÈGLES DE CONDUITE

Contrôle :

(A) L'organisation établit et rend facilement accessibles les règles qui décrivent les responsabilités et le comportement attendu des personnes qui doivent accéder au système d'information concernant l'utilisation de l'information et du système d'information.

(B) Avant de les autoriser à accéder à l'information et au système d'information, l'organisation reçoit de ces personnes une attestation signée indiquant qu'ils ont lu et compris les règles de conduite et qu'ils acceptent de s'y conformer.

(C) L'organisation examine et met à jour les règles de conduite [*Affectation : fréquence définie par l'organisation*].

(D) L'organisation exige que les personnes ayant déjà signé des versions antérieures des règles de conduite lisent et signent de nouveau ces règles de conduite après leur révision ou leur mise à jour.

Conseils supplémentaires : Cette amélioration de contrôle s'applique aux utilisateurs de l'organisation. L'organisation prévoit les règles de conduite selon les rôles et les responsabilités des utilisateurs en faisant une distinction, par exemple, entre les règles appliquées aux utilisateurs privilégiés et celles appliquées aux utilisateurs généraux. Il est souvent difficile d'établir des règles de conduite pour certains types d'utilisateurs non organisationnels, notamment des personnes qui ne font que recevoir des renseignements et des données de systèmes d'information fédéraux, étant donné le grand nombre de ces utilisateurs et la nature limitée de leurs interactions sur les systèmes. Les règles de conduite des utilisateurs organisationnels et non organisationnels peuvent également être établies sous le contrôle AC-8, Avis d'utilisation système. Pour satisfaire au contrôle PL-4 b (l'attestation signée de ce contrôle), l'organisation peut offrir de la formation sur la sensibilisation à la sécurité et des programmes de formation à la sécurité axée sur les rôles, si de telles formations traitent des règles de conduite. L'organisation peut faire appel aux signatures électroniques pour l'attestation liée

aux règles de conduite. Contrôles connexes : AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5.

Améliorations du contrôle :

(1) RÈGLES DE CONDUITE | RESTRICTIONS ASSOCIÉES AUX MÉDIAS ET RÉSEAUX SOCIAUX

L'organisation inclut dans les règles de conduite des restrictions explicites concernant l'utilisation des sites de médias et réseaux sociaux et l'affichage d'information organisationnelle sur des sites Web publics.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle traite des règles de conduite liées à l'utilisation des sites de médias et réseaux sociaux : (i) lorsque le personnel de l'organisation utilise de tels sites dans l'exercice de ses fonctions officielles ou dans le cadre de ses activités officielles; (ii) lorsque l'information organisationnelle fait partie d'une transaction sur des médias ou réseaux sociaux; et (iii) lorsque le personnel utilise des systèmes d'information de l'organisation pour accéder aux sites de médias ou réseaux sociaux. L'organisation prévoit également des règles particulières pour empêcher que des entités non autorisées utilisent les sites de médias ou réseaux sociaux pour obtenir et/ou déduire de l'information non publique sur l'organisation (p. ex. de l'information permettant d'identifier un compte du système ou une personne).

Références :

SCT, *Politique sur l'utilisation acceptable des dispositifs et des réseaux* [Référence 70].
CST, ITSB-66, *Les risques à la cybersécurité associés à l'utilisation de médias sociaux* [Référence 71].

PL-5 ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE

[Annulé].

PL-6 PLANIFICATION DES ACTIVITÉS RELATIVES À LA SÉCURITÉ

[Annulé : intégré au contrôle PL-2]

PL-7 CONCEPTS D'OPÉRATION DE SÉCURITÉ

Contrôle :

(A) L'organisation élabore un concept des opérations (CONOPS) de sécurité pour le système d'information. Celui-ci doit à tout le moins définir comment l'organisation prévoit opérer le système du point de vue de la sécurité d'information.

(B) L'organisation examine et tient à jour le CONOPS [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : Le CONOPS de sécurité peut être intégré au plan de sécurité du système d'information ou à d'autres documents traitant du cycle de développement du système, le cas échéant. Les changements apportés au CONOPS se reflètent en permanence dans les mises à jour du plan de sécurité, l'architecture de sécurité de l'information et d'autres documents organisationnels appropriés (p. ex. les spécifications relatives à la sécurité aux fins d'approvisionnement ou d'acquisition, les documents relatifs au cycle de développement du système et les documents liés à l'ingénierie des systèmes ou de la sécurité). Contrôle connexe : PL-2.

Améliorations du contrôle :

Aucune

Références :

Aucune

PL-8 ARCHITECTURE DE SÉCURITÉ DE L'INFORMATION

Contrôle :

(A) L'organisation développe pour le système d'information une architecture de sécurité de l'information qui :

(a) décrit la philosophie, les exigences et l'approche générales qui devront être respectées pour protéger la confidentialité, l'intégralité et la disponibilité de l'information de l'organisation;

(b) détermine comment l'architecture de sécurité de l'information s'intègre à l'architecture d'entreprise et la prend en charge;

(c) définit toutes les hypothèses sous-jacentes à la sécurité de l'information en lien avec les services externes et les interdépendances.

(B) L'organisation examine et met à jour l'architecture de sécurité de l'information [*Affectation : fréquence définie par l'organisation*] de manière à tenir compte des mises à jour apportées à l'architecture d'entreprise.

(C) L'organisation s'assure que les modifications prévues à l'architecture de sécurité de l'information sont reflétées dans le plan de sécurité, le concept des opérations (CONOPS) de sécurité, de même que l'approvisionnement et les acquisitions organisationnels.

Conseils supplémentaires : Ce contrôle porte sur les mesures prises par l'organisation dans le cadre de la conception et du développement des systèmes d'information. Sur le plan du système d'information individuel, l'architecture de sécurité de l'information est conforme et complémentaire à l'architecture de sécurité d'information plus globale utilisée à l'échelle de l'organisation, laquelle fait d'ailleurs partie intégrante et est développée dans le cadre de l'architecture d'entreprise. L'architecture de sécurité de l'information comprend une description de l'architecture, le placement ou l'affectation des fonctions de sécurité (y compris les contrôles de sécurité), l'information relative à la sécurité des interfaces externes, l'information échangée entre les interfaces et les mécanismes de protection associés à chacun des interfaces. L'architecture de sécurité peut de plus comprendre d'autres renseignements importants sur la sécurité comme, par exemple, les rôles des utilisateurs et les privilèges d'accès associés à chacun de ces rôles, des exigences propres à la sécurité, les types de renseignements traités, stockés et transmis par le système d'information, les priorités de restauration de l'information et les services du système d'information, ainsi que tout autre besoin de protection particulier.

Dans l'architecture moderne, de moins en moins d'organisations contrôlent l'ensemble des ressources d'information. L'organisation dépendra fortement des services d'information externes et des fournisseurs de services. Il est important de décrire ces dépendances dans l'architecture de sécurité de l'information pour mettre en place une stratégie de protection exhaustive pour ce qui est de la mission et des opérations. La mise en œuvre et le maintien d'une architecture de sécurité de l'information passent essentiellement par l'élaboration, le développement, la documentation et le maintien d'une configuration de base pour les systèmes d'information de l'organisation dans le cadre du contrôle des configurations. Ce développement de l'architecture de sécurité de l'information est coordonné avec le chef de la protection des renseignements personnels (CPRP) en vue d'assurer la détermination et la mise en œuvre des contrôles de sécurité nécessaires au respect des exigences en matière de protection des renseignements. Le contrôle PL-8 concerne principalement l'organisation (c.-à-d. axé sur le fonctionnement interne). Il vise à s'assurer que l'organisation met en place une architecture de sécurité de l'information pour le système d'information, et que cette architecture de sécurité s'intègre étroitement ou complémente l'architecture d'entreprise à l'échelle de l'entreprise. À l'opposé, le contrôle SA-17 concerne principalement les développeurs et intégrateurs de produits ou systèmes externes de TI (bien que l'organisation

puisse utiliser le contrôle SA-17 pour développer des systèmes internes). L'organisation sélectionne le contrôle SA-17, qui est complémentaire au contrôle PL-8, lorsqu'elle externalise le développement des systèmes d'information ou des composants connexes à des entités externes, puisqu'il sera dès lors nécessaire d'assurer l'uniformité avec l'architecture d'entreprise et l'architecture de sécurité de l'information de l'organisation. Contrôles connexes : CM-2, CM-6, PL-2, SA-5, SA-17.

Améliorations du contrôle :

(1) ARCHITECTURE DE SÉCURITÉ DE L'INFORMATION | DÉFENSE EN PROFONDEUR

(a) L'organisation élabore son architecture de sécurité selon une approche basée sur une défense en profondeur qui affecte [*Affectation : mesures de protection de sécurité définies par l'organisation*] aux [*Affectation : emplacements et couches d'architecture définis par l'organisation*];

(b) l'organisation élabore son architecture de sécurité selon une approche basée sur une défense en profondeur qui permet de s'assurer que les mesures de protection de sécurité affectées fonctionnent de façon coordonnée et se renforcent mutuellement.

Conseils supplémentaires sur l'amélioration : L'organisation affecte stratégiquement les mesures de protection (administratives, techniques ou les deux) dans l'architecture de sécurité de manière à ce que les adversaires ne puissent atteindre leur objectif sans être confrontés à plusieurs mesures de protection. Forcer les adversaires à mettre en échec plusieurs mécanismes les empêche d'attaquer trop facilement les ressources d'information essentielles (et complique sa tâche du même coup) et augmente les chances que leurs activités soient détectées. Il est essentiel de bien coordonner les mesures de protection affectées de manière à éviter qu'une attaque visant l'une de ces mesures n'ait des conséquences néfastes imprévues (p. ex. verrouillage, alertes successives) et aille à l'encontre d'une autre mesure. Le déploiement des mesures de protection est une activité capitale. Plus grande sera la criticité des actifs ou la valeur de l'information, plus importante sera la superposition des contrôles de sécurité. Conséquemment, une organisation peut opter d'installer un antivirus sur les couches frontières, les serveurs Web et de messagerie, les ordinateurs portables et les postes de travail pour maximiser le nombre de mesures de protection que les adversaires devront traverser pour en arriver à compromettre l'information et les systèmes d'information. Contrôles connexes : SC-29, SC-36.

(2) ARCHITECTURE DE SÉCURITÉ DE L'INFORMATION | DIVERSITÉ DES FOURNISSEURS

L'organisation exige que les [*Affectation : mesures de protection de sécurité définies par l'organisation*] affectées aux [*Affectation : emplacements et couches d'architecture définis par l'organisation*] soient obtenues de différents fournisseurs.

Conseils supplémentaires sur l'amélioration : Les différents produits de TI présentent des forces et des faiblesses diverses. C'est en combinant un large éventail de produits qu'il est possible de renforcer chacune des solutions. Par exemple, les fournisseurs de mécanismes de protection contre les programmes malveillants mettent généralement à jour leurs produits à différents moments et développent souvent des solutions aux virus, aux chevaux de Troie ou aux vers connus en fonction de leurs priorités et de leurs calendriers de développement. Installer différents produits dans divers emplacements (p. ex. sur des serveurs, aux frontières du système, sur un poste de travail) permet d'augmenter les chances que le programme malveillant soit détecté par l'un ou l'autre de ces composants. Contrôle connexe : SA-12.

Références :

Aucune

PL-9 GESTION CENTRALISÉE

Contrôle :

(A) L'organisation centralise la gestion des [*Affectation : contrôles de sécurité et processus connexes définis par l'organisation*].

Conseils supplémentaires : La gestion centralisée renvoie à la gestion et à la mise en œuvre des contrôles de sécurité sélectionnés et des processus connexes à l'échelle de l'organisation. Elle comprend la planification, la mise en œuvre, l'évaluation, l'autorisation et la surveillance des contrôles et processus de sécurité définis par l'organisation et gérés de façon centralisée par celle-ci. Comme la gestion centralisée des contrôles de sécurité est généralement synonyme de contrôles communs, ce type de gestion favorise et facilite la normalisation de la mise en œuvre des contrôles de sécurité, de leur gestion, et d'une utilisation judicieuse des ressources de l'organisation. Des contrôles et processus de sécurité gérés centralement peuvent également répondre aux exigences d'autonomie associées aux évaluations qui visent à appuyer les autorisations initiales et permanentes d'opérer dans le cadre de la surveillance continue de l'organisation. En vertu du processus de sélection des contrôles de sécurité, l'organisation détermine quels seront les contrôles susceptibles d'être gérés centralement en tenant compte de ses ressources et de ses capacités. L'organisation tient compte du fait qu'il n'est pas toujours possible de gérer centralement chacun des aspects d'un contrôle de sécurité. Dans de tels cas, le contrôle de sécurité est traité comme un contrôle hybride : il est géré et mis en œuvre centralement ou au niveau du système d'information. Les contrôles et les améliorations de contrôle qui se prêtent à une gestion centralisée complète ou partielle comprennent, sans s'y limiter : AC-2 (1) (2) (3) (4); AC-17 (1) (2) (3) (9); AC-18 (1) (3) (4) (5); AC-19 (4); AC-22; AC-23; AT-2 (1) (2); AT-3 (1) (2) (3); AT-4; AU-6 (1) (3) (5) (6) (9); AU-7 (1) (2); AU-11, AU-13, AU-16, CA-2 (1) (2) (3); CA-3 (1) (2) (3); CA-7 (1); CA-9; CM-2 (1) (2); CM-3 (1) (4); CM-4; CM-6 (1); CM-7 (4) (5); CM-8 (tous); CM-9 (1); CM-10; CM-11; CP-7 (tous); CP-8 (tous); SC-43; SI-2; SI-3; SI-7 et SI-8.

Améliorations du contrôle :

Aucune

Références :

Aucune

3.13 FAMILLE : SÉCURITÉ DU PERSONNEL

CLASSE : OPÉRATIONNELLE

PS-1 POLITIQUE ET PROCÉDURES DE SÉCURITÉ DU PERSONNEL

Contrôle :

(A) L'organisation élabore et consigne, ainsi que diffuse aux [*Affectation : personnel ou rôles définis par l'organisation*] :

(a) une politique de sécurité du personnel qui définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et le respect;

(b) des procédures visant à faciliter la mise en œuvre de la politique de sécurité du personnel et des contrôles qui y sont associés.

(B) L'organisation examine et met à jour :

(a) la politique de sécurité du personnel actuelle [*Affectation : fréquence définie par l'organisation*];

(b) les procédures de sécurité du personnel actuelles [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : Ce contrôle porte sur l'établissement de la politique et les procédures nécessaires à la mise en œuvre efficace des contrôles de sécurité et des améliorations dans la famille PS. La politique et les procédures de sécurité du personnel reflètent les lois du GC et les politiques, directives et normes applicables du SCT. Les politiques et les procédures du programme de sécurité mises en place à l'échelle de l'organisation peuvent rendre inutile toute politique et procédure propre à un système. La politique peut être intégrée à la politique générale sur la sécurité de l'information des organisations ou, inversement, elle peut être représentée par de multiples politiques compte tenu de la nature complexe de certaines organisations. Les procédures peuvent être établies pour le programme de sécurité général et pour des systèmes d'information particuliers, au besoin. La stratégie organisationnelle de gestion des risques est un facteur clé dans l'établissement de la politique et des procédures.

Améliorations du contrôle :

Aucune

Références :

SCT, *Norme opérationnelle de sécurité — Gestion de la sécurité des technologies de l'information* [Référence 7].

PS-2 CATÉGORISATION DES POSTES

Contrôle :

(A) L'organisation catégorise tous les postes en fonction des préjudices que les titulaires peuvent causer en commettant des actes malveillants découlant de l'exercice des privilèges associés au poste.

(B) L'organisation choisit la catégorie de sécurité appropriée (p. ex. vérification approfondie de la fiabilité [VAF], I, II, III) pour les personnes occupant ces postes.

(C) L'organisation examine et révise la catégorisation des postes [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires :

Aucun

Améliorations du contrôle :

Aucune

Références :

SCT, *Norme sur le filtrage de sécurité* [Référence 9].

PS-3 ENQUÊTE DE SÉCURITÉ SUR LE PERSONNEL

Contrôle :

(A) L'organisation soumet les personnes à une enquête de sécurité avant de leur autoriser l'accès au système d'information, conformément à la *Norme sur le filtrage de sécurité du SCT* [Référence 9].

(B) L'organisation effectue une nouvelle enquête de sécurité lorsque [*Affectation : liste définie par l'organisation des conditions qui exigent une nouvelle enquête de sécurité et fréquence de cette enquête, le cas échéant*].

Conseils supplémentaires : Les activités liées aux deux types d'enquête reflètent les lois du GC, les politiques, les directives et les normes applicables du SCT, ainsi que les critères établis pour la désignation des risques associés au poste concerné. L'organisation peut définir différentes conditions et fréquences pour une nouvelle enquête des employés qui accèdent aux systèmes d'information selon le type d'information traitée, stockée ou transmise. Contrôles connexes : AC-4, IA-2, PE-2, PS-2.

Améliorations du contrôle :

(1) ENQUÊTE DE SÉCURITÉ SUR LE PERSONNEL | INFORMATION CLASSIFIÉE

L'organisation s'assure que chaque utilisateur d'un système d'information qui traite, stocke ou transmet de l'information classifiée a une habilitation et un endoctrinement au plus haut niveau de classification de l'information à laquelle ils ont accès dans le système.

Conseils supplémentaires sur l'amélioration : Contrôles connexes : AC-3, AC-4.

(2) ENQUÊTE DE SÉCURITÉ SUR LE PERSONNEL | ENDOCTRINEMENT OFFICIEL

L'organisation s'assure que chaque utilisateur d'un système d'information qui traite, stocke ou transmet des types d'information classifiée pour lesquels il faut suivre une séance d'endoctrinement officielle est officiellement endoctriné pour tous les types d'information pertinents auxquels il a accès sur le système.

Conseils supplémentaires sur l'amélioration : Les informations sensibles cloisonnées sont un exemple de type d'information pour lequel il faut suivre une séance d'endoctrinement officielle.

(3) ENQUÊTE DE SÉCURITÉ SUR LE PERSONNEL | INFORMATION VISÉE PAR DES MESURES DE PROTECTION SPÉCIALES

L'organisation veille à ce que les utilisateurs puissent accéder à un système d'information qui traite, stocke ou transmet de l'information nécessitant une protection spéciale :

(a) avec des autorisations d'accès valides attestées par les responsabilités gouvernementales officielles qui leur ont été assignées;

(b) conforme aux [*Affectation : critères d'enquête de sécurité supplémentaires définis par l'organisation*].

Conseils supplémentaires sur l'amélioration : L'information organisationnelle nécessitant une protection spéciale comprend notamment l'information protégée et l'information sur les sources et les méthodes. Les

critères de sécurité du personnel comprennent, par exemple, les exigences de vérification des antécédents en fonction de la sensibilité du poste.

Références :

TPSGC, *Manuel de la sécurité industrielle* [Référence 2].
SCT, *Norme sur le filtrage de sécurité* [Référence 9].

PS-4 CESSATION D'EMPLOI

Contrôle :

(A) L'organisation, lors de la cessation d'emploi d'un employé, met un terme à l'accès au système d'information dans les [*Affectation : période définie par l'organisation*].

(B) L'organisation, lors de la cessation d'emploi d'un employé, met fin ou annule les authentifiants et les justificatifs d'identité associés à l'employé.

(C) L'organisation, lors de la cessation d'emploi d'un employé, effectue une entrevue de fin d'emploi et mène une discussion sur [*Affectation : sujets liés à la sécurité de l'information définis par l'organisation*].

(D) L'organisation, lors de la cessation d'emploi d'un employé, retire tous les biens liés au système d'information organisationnel associés à la sécurité.

(E) L'organisation, lors de la cessation d'emploi d'un employé, conserve l'accès à l'information et aux systèmes d'information organisationnels précédemment contrôlés par l'employé concerné.

(F) L'organisation, lors de la cessation d'emploi d'un employé, informe les [*Affectation : personnel ou rôles définis par l'organisation*] dans les [*Affectation : période définie par l'organisation*].

Conseils supplémentaires : Les biens associés au système d'information comprennent, par exemple, les jetons matériels d'authentification, les manuels techniques d'administration du système, les clés, les cartes d'identité et les laissez-passer. Les entrevues de fin d'emploi permettent de s'assurer que les personnes concernées comprennent les contraintes de sécurité auxquelles elles doivent se soumettre à titre d'anciens employés et leurs responsabilités à l'égard des biens associés au système d'information. Lors des entrevues de fin d'emploi, la sécurité veille notamment à rappeler aux employés leur acceptation des ententes de non-divulgation et les éventuelles limitations professionnelles dont ils pourraient faire l'objet. Il peut arriver qu'il soit impossible de procéder à ces entrevues pour certains employés, par exemple, dans le cas d'un abandon de poste, d'une maladie et de la non-disponibilité des superviseurs. Les entrevues de fin d'emploi sont importantes dans le cas des personnes qui possèdent une habilitation de sécurité. L'exécution opportune de ces mesures de fin d'emploi est importante dans le cas d'employés licenciés. Dans certaines situations, l'organisation peut opter de désactiver les comptes de système d'information des employés licenciés avant même qu'ils ne soient informés. Contrôles connexes : AC-2, IA-4, PE-2, PS-5, PS-6.

Améliorations du contrôle :

(1) CESSATION D'EMPLOI | EXIGENCES RÉGISSANT L'APRÈS-MANDAT

(a) L'organisation informe les employés qui quittent leur emploi des exigences applicables à l'après-mandat qui ont valeur juridique contraignante et concernent la protection de l'information organisationnelle;

(b) l'organisation exige que les employés qui quittent leur emploi attestent par écrit des exigences d'après-mandat dans le cadre du processus organisationnel de cessation d'emploi.

Conseils supplémentaires sur l'amélioration : L'organisation consulte le Bureau de l'avocat général au sujet des questions liées aux exigences d'après-mandat des employés qui quittent leur emploi.

(2) CESSATION D'EMPLOI | NOTIFICATION AUTOMATIQUE

L'organisation fait appel à des mécanismes automatisés pour informer [*Affectation : personnel ou rôles définis par l'organisation*] lors de la cessation d'emploi d'un employé.

Conseils supplémentaires sur l'amélioration : Dans les organisations qui comptent un grand nombre d'employés, le personnel qui doit être mis au courant des mesures associées à la cessation d'emploi d'un employé ne reçoit pas toujours les notifications appropriées ou ne les reçoit pas dans des délais opportuns. Il est possible de mettre en place des mécanismes automatisés afin d'envoyer des alertes ou notifications automatiques à des membres du personnel ou des rôles particuliers (p. ex. les membres de la direction, les superviseurs, les agents de la sécurité interne, les administrateurs système ou les administrateurs des TI) lorsqu'un employé quitte son emploi. Ces alertes ou notifications peuvent être acheminées de différentes façons, que ce soit par téléphone, par courrier électronique, par message texte ou par le biais d'un site Web.

Références :

SCT, *Norme sur le filtrage de sécurité* [Référence 9].

PS-5 TRANSFERT DU PERSONNEL

Contrôle :

(A) L'organisation examine et confirme les exigences opérationnelles liées aux autorisations d'accès physique et logique existantes aux systèmes d'information et aux installations lorsque des employés sont réaffectés ou transférés à d'autres postes au sein de l'organisation.

(B) L'organisation entreprend des [*Affectation : mesures de transfert ou de réaffectation définies par l'organisation*] dans les [*Affectation : période définie par l'organisation conformément à la Norme sur le filtrage de sécurité* du SCT *[Référence 9]*].

(C) L'organisation modifie au besoin les autorisations d'accès afin de tenir compte de toute modification apportée aux exigences opérationnelles en raison d'une réaffectation ou d'un transfert.

(D) L'organisation informe [*Affectation : personnel ou rôles définis par l'organisation*] dans les [*Affectation : période définie par l'organisation*].

Conseils supplémentaires : Ce contrôle s'applique dans les cas où la réaffectation ou le transfert d'un employé est permanents ou d'une durée qui justifie les mesures requises. De plus, l'organisation définit les mesures appropriées pour le type de réaffectation ou de transfert, qu'il soit permanent ou prolongé. Ces mesures comprennent notamment (i) le retour et le remplacement des anciens laissez-passer, cartes d'identité et clés, (ii) la fermeture des comptes de système d'information et l'établissement de nouveaux, (iii) la modification des autorisations d'accès aux systèmes d'information (c.-à-d. les privilèges) et (iv) la fourniture de l'accès aux dossiers officiels auxquels l'employé avait accès dans les lieux de travail précédents et avec les comptes de système d'information précédents. Contrôles connexes : AC-4, IA-2, PE-2, PS-4.

Améliorations du contrôle :

Aucune

Références :

SCT, *Norme sur le filtrage de sécurité* [Référence 9].

PS-6 ENTENTES D'ACCÈS

Contrôle :

(A) L'organisation élabore et documente les ententes d'accès aux systèmes d'information organisationnels.

(B) L'organisation examine et met à jour les ententes d'accès [*Affectation : fréquence définie par l'organisation*].

(C) L'organisation s'assure que les personnes qui ont besoin d'accéder à l'information et aux systèmes d'information organisationnels :

(a) signent les ententes d'accès appropriées avant que l'accès ne leur soit accordé;

(b) signent des nouvelles ententes d'accès pour maintenir l'accès aux systèmes d'information organisationnels lorsque les ententes d'accès sont mises à jour ou [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : Les ententes d'accès comprennent notamment les ententes de non-divulgation, les ententes d'utilisation acceptable, les règles de conduite et les ententes régissant les conflits d'intérêts. Une entente d'accès signée comprend une attestation que la personne a lu et compris les contraintes associées aux systèmes d'information organisationnels auxquels on lui a accordé l'accès et qu'elle accepte de s'y conformer. Les signatures électroniques sont admises pour l'acceptation d'ententes d'accès, à moins d'être expressément interdites par les politiques de l'organisation. Contrôles connexes : PL-4, PS-2, PS-3, PS-4, PS-8.

Améliorations du contrôle :

(1) ENTENTES D'ACCÈS | INFORMATION NÉCESSITANT UNE PROTECTION SPÉCIALE

[Annulée : Intégrée au contrôle PS-3]

(2) ENTENTES D'ACCÈS | INFORMATION CLASSIFIÉE NÉCESSITANT UNE PROTECTION SPÉCIALE

L'organisation s'assure que l'accès à l'information classifiée nécessitant une protection spéciale est accordé uniquement aux personnes qui :

(a) possèdent une autorisation d'accès valide attestée par les responsabilités gouvernementales officielles qui leur ont été assignées;

(b) satisfont aux critères connexes de sécurité du personnel;

(c) ont lu, compris et signé une entente de non-divulgation.

Conseils supplémentaires sur l'amélioration : Les informations sensibles cloisonnées sont un exemple de type d'information pour lequel il faut suivre une séance d'endoctrinement officielle. Les critères de sécurité du personnel sont conformes aux lois du GC et aux politiques, directives et normes applicables du SCT.

(3) ENTENTES D'ACCÈS | EXIGENCES RÉGISSANT L'APRÈS-MANDAT

(a) L'organisation informe les employés des exigences applicables à l'après-mandat qui ont valeur juridique contraignante et concernent la protection de l'information organisationnelle;

(b) l'organisation exige que les employés attestent par écrit de ces exigences, le cas échéant, au moment d'accorder accès à l'information concernée.

Conseils supplémentaires sur l'amélioration : L'organisation consulte son conseiller juridique au sujet des questions liées aux exigences d'après-mandat des employés qui quittent leur emploi.

Références :

Aucune

PS-7 SÉCURITÉ DU PERSONNEL DE TIERCES PARTIES

Contrôle :

(A) L'organisation définit les exigences en matière de contrôle de sécurité liées à la sécurité du personnel, y compris les rôles et responsabilités des fournisseurs tiers.

(B) L'organisation exige que les fournisseurs tiers se conforment aux politiques et procédures en matière de contrôle de la sécurité du personnel qu'elle a mises en place.

(C) L'organisation documente les exigences en matière de sécurité du personnel.

(D) L'organisation exige que les fournisseurs tiers informent [*Affectation : personnel ou rôles définis par l'organisation*] du transfert ou de la cessation d'emploi de tout employé de tierces parties qui possède des justificatifs d'identité et/ou des laissez-passer de l'organisation, ou dispose de privilèges d'accès au système d'information dans les [*Affectation : période définie par l'organisation*].

(E) L'organisation surveille la conformité des fournisseurs.

(AA) L'organisation veille à ce que les organisations et les personnes du secteur privé qui ont accès à l'information et aux biens protégés et classifiés fassent l'objet d'une enquête de sécurité, conformément à la *Norme sur le filtrage de sécurité du SCT* [Référence 9].

(BB) L'organisation définit explicitement la surveillance gouvernementale et les rôles et responsabilités d'utilisateur final relativement aux services fournis par des tiers, conformément à la *Norme de sécurité et de gestion des marchés du SCT* [Référence 25].

Conseils supplémentaires : Les fournisseurs tiers comprennent, par exemple, les sociétés de services informatiques, les entrepreneurs et autres organisations qui offrent des services de développement de système d'information et de technologie de l'information, des applications imparties et la gestion des réseaux et de la sécurité. L'organisation inclut explicitement les exigences en matière de contrôle de sécurité liées à la sécurité du personnel dans les documents d'approvisionnement. Le personnel de fournisseurs tiers peut travailler dans les installations de l'organisation si cette dernière lui remet des justificatifs d'identité, des laissez-passer ou des privilèges d'accès aux systèmes d'information. Les avis envoyés advenant des changements au niveau du personnel de tierces parties permettent d'assurer l'annulation opportune des privilèges d'accès et des justificatifs d'identité. L'organisation détermine quels seront les transferts et les cessations d'emploi à signaler en fonction de caractéristiques de sécurité comme, par exemple, les fonctions, les rôles et la nature des justificatifs d'identité et privilèges associés à la personne qui fait l'objet du transfert ou de la cessation d'emploi. Contrôles connexes : PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21.

Améliorations du contrôle :

Aucune

Références :

SCT, *Norme sur le filtrage de sécurité* [Référence 9].
SCT, *Norme de sécurité et de gestion des marchés* [Référence 25].

PS-8 SANCTIONS IMPOSÉES AU PERSONNEL

Contrôle :

(A) L'organisation utilise un processus formel de sanctions pour le personnel qui ne se conforme pas aux politiques et procédures établies de sécurité de l'information.

(B) L'organisation informe [*Affectation : personnel ou rôles définis par l'organisation*] dans les [*Affectation : période définie par l'organisation*] lorsque le processus formel de sanctions est amorcé et indique qui est l'employé sanctionné et les motifs de la sanction.

Conseils supplémentaires : Les processus de sanctions de l'organisation reflètent les lois du GC ainsi que les politiques, les directives et les normes applicables du SCT. Les processus de sanctions sont décrits dans des ententes d'accès et peuvent être incorporés aux politiques et procédures générales sur le personnel de l'organisation. L'organisation demande l'avis de son conseiller juridique pour les questions liées aux sanctions des employés. Contrôles connexes : PL-4, PS-6.

Améliorations du contrôle :

Aucune

Références :

Aucune

3.14 FAMILLE : ÉVALUATION DES RISQUES

CLASSE : GESTION

RA-1 POLITIQUE ET PROCÉDURES D'ÉVALUATION DES RISQUES

Contrôle :

(A) L'organisation élabore, consigne et diffuse auprès de [*Affectation : personnel ou rôles définis par l'organisation*] :

(a) une politique d'évaluation des risques qui définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité;

(b) des procédures visant à faciliter la mise en œuvre de la politique d'évaluation des risques et des contrôles connexes visant l'évaluation des risques.

(B) L'organisation examine et met à jour :

(a) la politique d'évaluation des risques tous les [*Affectation : fréquence définie par l'organisation*];

(b) les procédures d'évaluation des risques tous les [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : Ce contrôle porte sur l'application de la politique et des procédures afférentes, qui ont pour objet de mettre en œuvre les divers contrôles ainsi que les améliorations se rapportant à la famille « évaluation des risques » (RA). La politique et les procédures répondent aux lois du GC ainsi qu'aux politiques, directives et normes applicables du SCT. Les politiques et les procédures du programme de sécurité organisationnel peuvent rendre facultatives les politiques et procédures propres au système. La politique peut être intégrée à la politique générale sur la sécurité de l'information des organisations ou, inversement, elle peut être représentée par de multiples politiques, compte tenu de la nature complexe de certaines organisations. Les procédures peuvent être établies pour le programme de sécurité général et pour des systèmes d'information particuliers, le cas échéant. La stratégie organisationnelle de gestion des risques est un facteur clé dans l'établissement de la politique et des procédures.

Améliorations du contrôle :

Aucune

Références :

SCT, *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* [Référence 7].

RA-2 CATÉGORISATION DE SÉCURITÉ

Contrôle :

(A) L'organisation catégorise l'information et les systèmes d'information conformément aux lois du GC et aux prescriptions du SCT.

(B) L'organisation documente les résultats de la catégorisation (y compris les justifications) dans le plan de sécurité du système d'information.

(C) L'organisation s'assure que la décision concernant la catégorisation de sécurité est examinée et approuvée par l'autorité responsable ou par son représentant désigné.

Conseils supplémentaires : Des limites d'autorisation clairement définies constituent un préalable aux décisions devant mener à une catégorisation de sécurité efficace. Les catégories de sécurité décrivent les incidences négatives potentielles sur les activités et les biens organisationnels, de même que sur les personnes dans les cas où l'information organisationnelle ou les systèmes d'information sont compromis à la suite d'une entorse à la confidentialité, à l'intégrité ou à la disponibilité. Les organisations engagent le processus de catégorisation de la sécurité comme une activité globale à laquelle participent les dirigeants principaux de l'information, les agents principaux de sécurité de l'information, les propriétaires des systèmes d'information, les propriétaires de la mission ou des activités, de même que les propriétaires ou les gardiens de l'information. Les organisations devraient également prendre en compte les impacts négatifs sur les autres organisations à l'échelle nationale. Les processus de catégorisation de la sécurité qui sont mis en œuvre par les organisations permettent de réaliser les inventaires des biens d'information et, de concert avec le contrôle CM-8, facilitent le mappage à certains composants des systèmes d'information où de l'information est traitée, stockée ou transmise. Contrôles connexes : CM-8, MP-4, RA-3, SC-7.

Améliorations du contrôle :

Aucune

Références :

CST, *ITSG-33, Annexe 2 – Activités de gestion des risques liés aux systèmes d'information* [Référence 58].

RA-3 ÉVALUATION DES RISQUES

Contrôle :

(A) L'organisation effectue une évaluation des risques, y compris la probabilité et l'ampleur des préjudices, qui sont associés à l'utilisation, à la divulgation, à l'interruption, à la modification et à l'accès non autorisés ou encore à la destruction du système d'information ou de l'information qu'il traite, stocke et transmet.

(B) L'organisation documente les résultats de l'évaluation des risques dans [*Sélection : plan de sécurité; rapport d'évaluation des risques;* [*Affectation : document défini par l'organisation*]].

(C) L'organisation examine les résultats de l'évaluation des risques [*Affectation : fréquence définie par l'organisation*].

(D) L'organisation communique les résultats de l'évaluation des risques aux [*Affectation : personnel ou rôles définis par l'organisation*].

(E) L'organisation effectue une mise à jour de l'évaluation des risques [*Affectation : fréquence définie par l'organisation*] ou chaque fois que des changements importants sont apportés au système d'information ou à l'environnement d'exploitation (y compris l'identification de nouvelles menaces et vulnérabilités), ou encore lorsque d'autres conditions sont susceptibles d'influer sur l'état de sécurité du système.

Conseils supplémentaires : Des limites d'autorisation clairement définies constituent un préalable aux décisions devant mener à une évaluation efficace des risques. Toute évaluation des risques doit prendre en compte les menaces, les vulnérabilités, les probabilités ainsi que les impacts sur activités et les biens organisationnels, sur les employés, sur d'autres organisations, et sur le Canada en se fondant sur l'exploitation et l'utilisation des systèmes d'information. Les évaluations des risques doivent également tenir compte des risques provenant d'intervenants externes (p. ex. fournisseurs de services, entrepreneurs qui exploitent les systèmes d'information au nom de l'organisation, personnes qui accèdent aux systèmes d'information de l'organisation, sous-traitants).

Qu'elles soient formelles ou informelles, les évaluations des risques peuvent être menées à chacun des trois niveaux hiérarchiques de la gestion des risques (c.-à-d. le niveau organisationnel, le niveau du processus lié à une mission/une activité ou le niveau du système d'information) ainsi qu'à chacune des phases du cycle de

développement des systèmes. Les évaluations peuvent également être effectuées à divers stades du cadre de gestion des risques de l'ITSG-33, notamment la catégorisation des systèmes d'information, la sélection des contrôles de sécurité, la mise en œuvre des contrôles, l'évaluation des contrôles de sécurité, l'autorisation des systèmes d'information et la surveillance des contrôles de sécurité. Au reste, le RA-3 se distingue en ce qu'il doit être en partie appliqué avant la mise en œuvre des autres contrôles, de façon à permettre l'achèvement des deux premières étapes du cadre de gestion des risques. Les évaluations des risques peuvent jouer un rôle important dans les processus de sélection des contrôles de sécurité, particulièrement pendant la mise en application des directives de personnalisation, lesquelles comprennent un complément en matière de contrôle de sécurité.
Contrôle connexe : RA-2.

Améliorations du contrôle :

Aucune

Références :

CST, *ITSG-33, Annexe 2 – Activités de gestion des risques liés aux systèmes d'information* [Référence 58].
CST et GRC, *Méthodologie harmonisée d'évaluation des menaces et des risques* [Référence 3].
SCT, *Norme de sécurité relative à l'organisation et l'administration* [Référence 13].

RA-4 MISE À JOUR DE L'ÉVALUATION DES RISQUES

[Annulé : Intégré au contrôle RA-3]

RA-5 ANALYSE DES VULNÉRABILITÉS

Contrôle :

(A) L'organisation soumet le système d'information et les applications hébergées à une analyse des vulnérabilités [*Affectation : fréquence définie par l'organisation ou de manière aléatoire conformément au processus défini par l'organisation*] et lorsque de nouvelles vulnérabilités susceptibles d'influer sur le système ou sur les applications sont identifiées et signalées.

(B) L'organisation utilise des outils et des techniques d'analyse des vulnérabilités qui facilitent l'interopérabilité et automatisent les composantes du processus de gestion des vulnérabilités. À cette fin, elle applique des normes sur les aspects suivants :

(a) relevé des plateformes, des lacunes logicielles et des configurations inappropriées;

(b) formatage de listes de vérification et de procédures de test;

(c) mesure de l'incidence des vulnérabilités.

(C) L'organisation examine les rapports d'analyse des vulnérabilités et les résultats des évaluations des contrôles de sécurité.

(D) L'organisation corrige les vulnérabilités légitimes [*Affectation : temps de réponse définis par l'organisation*] conformément à son évaluation des risques.

(E) L'organisation communique l'information découlant du processus d'analyse des vulnérabilités et des évaluations des contrôles de sécurité à [*Affectation : rôles ou membres du personnel définis par l'organisation*] pour faciliter l'élimination de vulnérabilités semblables (c.-à-d. les faiblesses ou les lacunes systémiques) dans les autres systèmes d'information.

Conseils supplémentaires : La catégorisation de sécurité des systèmes d'information aide à définir la fréquence et le niveau d'exhaustivité des analyses des vulnérabilités. Les organisations définissent l'analyse de vulnérabilité requise pour tous les composants du système d'information tout en veillant à ce que les éventuelles sources de vulnérabilité, notamment les dispositifs réseaux comme les imprimantes, les numériseurs et les photocopieuses, ne soient pas négligées. Les analyses de vulnérabilité visant les applications logicielles sur mesure pourraient nécessiter des mesures additionnelles comme les analyses statiques, les analyses dynamiques, les analyses binaires ou encore des analyses recourant à une combinaison des types d'analyse précités. Les organisations peuvent employer ces types d'analyses dans plusieurs outils (p. ex. analyseurs d'application Web, outils d'analyse statique, analyseurs binaires) ainsi que dans des examens de code source. Voici des exemples d'analyse de vulnérabilité : (i) l'analyse des niveaux de rustines; (ii) la recherche de fonctions, de ports, de protocoles et de services qui ne devraient pas être accessibles aux utilisateurs ni aux dispositifs; (iii) l'identification des mécanismes de contrôle des flux d'information, qui sont mal configurés ou qui fonctionnent inadéquatement.

Améliorations du contrôle :

(1) ANALYSE DES VULNÉRABILITÉS | MISE À NIVEAU DE LA CAPACITÉ DES OUTILS

L'organisation utilise des outils d'analyse des vulnérabilités qui sont en mesure de mettre facilement à jour le registre des vulnérabilités qu'il faudrait analyser par mesure de protection des systèmes d'information.

Conseils supplémentaires sur l'amélioration : Le registre des vulnérabilités à analyser doit être aisément actualisé à mesure que de nouvelles vulnérabilités sont mises au jour et que les méthodes d'analyse sont établies. Ce processus de mise à jour permet d'identifier les éventuelles vulnérabilités auxquelles s'exposent les systèmes d'information et d'intervenir dans les plus brefs délais. Contrôles connexes : SI-3, SI-7.

(2) ANALYSE DES VULNÉRABILITÉS | MISE À JOUR SELON LA FRÉQUANCE / PRÉALABLEMENT À UNE NOUVELLE ANALYSE / AU MOMENT DE L'IDENTIFICATION

L'organisation met à jour le registre des vulnérabilités des systèmes d'information [*Sélection (un ou plusieurs) :* [*Affectation : fréquence définie par l'organisation*]; *avant une nouvelle analyse; lorsque de nouvelles vulnérabilités sont identifiées et signalées*].

Conseils supplémentaires sur l'amélioration : Contrôles connexes – SI-3, SI-5.

(3) ANALYSE DES VULNÉRABILITÉS | AMPLEUR / PROFONDEUR DE LA COUVERTURE

L'organisation utilise des procédures d'analyse des vulnérabilités qui peuvent établir l'ampleur et la profondeur de la couverture (c.-à-d. vulnérabilités vérifiées et composants de système d'information analysés).

(4) ANALYSE DES VULNÉRABILITÉS | INFORMATION DÉCOUVRABLE

L'organisation dresse une liste des informations qui sont enregistrées dans les systèmes d'information et qui sont susceptibles d'être découvertes par des adversaires, puis elle prend les mesures suivantes : [*Affectation : mesures correctives définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Au nombre des informations découvrables, citons notamment celles que les adversaires pourraient obtenir sans directement compromettre ou forcer le système d'information – par exemple, en collectant de l'information que le système expose ou en menant des recherches extensives dans le Web. Les mesures correctives peuvent comprendre, par exemple, le signalement auprès du personnel organisationnel compétent, le retrait de certaines informations, ou l'introduction de modifications du système visant à rendre l'information en question moins pertinente ou moins attrayante pour les parties adverses. Contrôle connexe : AU-13.

(5) ANALYSE DES VULNÉRABILITÉS | ACCÈS PRIVILÉGIÉS

Le système d'information permet un accès privilégié aux [*Affectation : composants du système d'information définis par l'organisation*] pour certaines fonctions comme [*Affectation : opérations d'analyse des vulnérabilités définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Dans certains cas, les analyses des vulnérabilités pourraient s'avérer plutôt intrusives, ou encore, les systèmes d'information faisant l'objet d'une analyse pourraient contenir des renseignements hautement sensibles. L'accès privilégié accordé à certains composants du système d'information permet de procéder à une analyse plus approfondie des vulnérabilités et de protéger la nature sensible d'une telle analyse.

(6) ANALYSE DES VULNÉRABILITÉS | AUTOMATISATION DES ANALYSES DE TENDANCES

L'organisation utilise des mécanismes automatisés conçus pour comparer chronologiquement les résultats des analyses et établir les tendances sur le plan des vulnérabilités du système d'information.

Conseils supplémentaires sur l'amélioration : Contrôles connexes – IR-4, IR-5, SI-4.

(7) ANALYSE DES VULNÉRABILITÉS | AUTOMATISATION DE LA DÉTECTION ET DU SIGNALEMENT DES COMPOSANTS NON AUTORISÉS

[Annulé : Intégré au contrôle CM-8]

(8) ANALYSE DES VULNÉRABILITÉS | EXAMEN DES JOURNAUX DE VÉRIFICATION HISTORIQUES

L'organisation examine les journaux de vérification historiques pour déterminer si une vulnérabilité connue a déjà été exploitée dans le système d'information.

Conseils supplémentaires sur l'amélioration : Contrôle connexe – AU-6.

(9) ANALYSE DES VULNÉRABILITÉS | TESTS ET ANALYSES DE PÉNÉTRATION

[Annulé : Intégré au contrôle CA-8]

(10) ANALYSE DES VULNÉRABILITÉS | CORRÉLATION DES INFORMATIONS TIRÉES DES ANALYSES

L'organisation tente d'établir une corrélation entre les résultats produits par les outils d'analyse des vulnérabilités dans le but de déceler, le cas échéant, la présence de vecteurs d'attaque visant plusieurs vulnérabilités ou se déplaçant sur plusieurs bonds.

Références :

Aucune

RA-6 DÉPISTAGE DES CONTRE-MESURES DE SURVEILLANCE TRECHNIQUE

Contrôle :

(A) L'organisme a recours à un dépistage des contre-mesures de surveillance technique aux [*Affectation : lieux définis par l'organisation*] [*Sélection (une ou plusieurs) :* [*Affectation : fréquence définie par l'organisation*]; [*Affectation : occurrence d'événements ou indicateurs définis par l'organisation*]].

Conseils supplémentaires : Le dépistage des contre-mesures de surveillance technique est exécuté dans le but de détecter la présence de dispositifs/de méthodes de surveillance technique et d'identifier les lacunes de sécurité technique qui pourraient ouvrir le champ aux tentatives de pénétration technique des installations en cause. Les mesures de dépistage fournissent des éléments d'évaluation de la posture de sécurité de l'organisation et des installations; elles comprennent généralement des examens exhaustifs (visuels, électroniques, physiques) des installations et de leurs alentours. Les mesures de dépistage fournissent également des informations pouvant servir aux évaluations des risques et permettant de signaler les brèches que des adversaires pourraient exploiter.

Améliorations du contrôle :

Aucune

Références :

Aucune

3.15 FAMILLE : ACQUISITION DES SYSTÈMES ET DES SERVICES

CLASSE : GESTION

SA-1 POLITIQUE ET PROCÉDURES D'ACQUISITION DES SYSTÈMES ET DES SERVICES

Contrôle :

(A) L'organisation élabore et consigne, puis diffuse auprès de [*Affectation : personnel ou rôles définis par l'organisation*] :

(a) une politique d'acquisition des systèmes et des services, qui définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité;

(b) des procédures visant à faciliter la mise en œuvre de la politique d'acquisition des systèmes et des services ainsi que des contrôles connexes.

(B) L'organisation examine et met à jour :

(a) la politique d'acquisition des systèmes et des services tous les [*Affectation : fréquence définie par l'organisation*];

(b) les procédures relatives à l'acquisition des systèmes et des services tous les [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : Ce contrôle porte sur l'application de la politique et des procédures afférentes, qui ont pour objet de mettre en œuvre les divers contrôles ainsi que les améliorations ayant trait à la famille SA. La politique et les procédures d'acquisition des systèmes et des services répondent aux lois du GC ainsi qu'aux politiques, directives et normes applicables du SCT. Les politiques et les procédures du programme de sécurité organisationnel peuvent rendre facultatives les politiques et les procédures propres au système. La politique peut être intégrée à la politique générale sur la sécurité de l'information des organisations ou, inversement, elle peut être représentée par de multiples politiques compte tenu de la nature complexe de certaines organisations. Les procédures peuvent être établies pour le programme de sécurité général et pour des systèmes d'information particuliers, le cas échéant. La stratégie organisationnelle de gestion des risques est un facteur clé dans l'établissement de la politique et des procédures.

Améliorations du contrôle :

Aucune

Références :

SCT, *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* [Référence 7].

SA-2 AFFECTATION DES RESSOURCES

Contrôle :

(A) L'organisation définit les exigences en matière de contrôle de sécurité de l'information pour le système d'information ou pour les services connexes lors de la planification de la mission ou des processus opérationnels.

(B) L'organisation détermine, documente et affecte les ressources nécessaires pour protéger le système d'information ou les services connexes dans le cadre du processus de planification des immobilisations et de contrôle des investissements.

(C) L'organisation prévoit un poste distinct pour la sécurité de l'information dans sa documentation de programmation et de budgétisation.

Conseils supplémentaires : L'affectation des ressources aux fins de la sécurité de l'information comprend le financement de l'acquisition du système d'information initial ou de services connexes ainsi que le financement des opérations de maintien desdits système ou services.

Améliorations du contrôle :

Aucune

Références :

SCT, *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* [Référence 7].

SA-3 CYCLE DE DÉVELOPPEMENT DE SYSTÈME

Contrôle :

(A) L'organisation gère le système d'information en recourant à [*Affectation : cycle de développement de système défini par l'organisme*] qui intègre les aspects liés à la sécurité de l'information.

(B) L'organisation définit et documente les responsabilités et les rôles associés à la sécurité de l'information, et ce, à tous les stades du cycle de développement du système.

(C) L'organisation identifie les personnes auxquelles sont attribués des responsabilités et des rôles relatifs à la sécurité de l'information.

(D) L'organisation intègre les processus organisationnels de gestion des risques liés à la sécurité de l'information à la planification des activités du cycle de développement du système.

Conseils supplémentaires : Un cycle de développement des systèmes qui a été adéquatement élaboré constitue une condition essentielle à la réussite des étapes de développement, de mise en œuvre et d'exploitation des systèmes d'information**.** Pour être en mesure d'appliquer adéquatement les contrôles de sécurité pendant le cycle de développement des systèmes, il faut posséder une compréhension élémentaire du domaine de la sécurité de l'information, des menaces, des vulnérabilités, des effets négatifs, et des risques auxquels s'exposent les missions et les activités opérationnelles. Les principes d'ingénierie de sécurité énoncés dans le SA-8 ne peuvent être adéquatement appliqués lorsque les responsables de la conception, du code et des tests menés sur les systèmes d'information ou sur les composants du système (y compris les produits de technologie de l'information) ne sont pas au fait des enjeux liés à la sécurité. Par conséquent, les organisations doivent compter sur du personnel compétent, notamment des dirigeants principaux de la sécurité de l'information, des architectes et des ingénieurs de sécurité, ainsi que des responsables de la sécurité de l'information, pour être en mesure de mener adéquatement les activités ponctuant le cycle de développement des systèmes de façon à concrétiser les exigences de sécurité dans les systèmes organisationnels d'information. Au reste, il est tout aussi important que les développeurs puissent compter sur des intervenants qui possèdent l'expertise et les compétences requises en matière de sécurité, pour parvenir à intégrer comme il se doit les capacités de sécurité dans les systèmes d'information. La sensibilisation à la sécurité ainsi que les programmes de formation peuvent permettre aux intervenants clés en matière de sécurité d'acquérir l'expérience, les compétences et l'expertise nécessaires à la conduite des activités constitutives du cycle de développement des systèmes. La parfaite intégration des exigences de sécurité à l'architecture d'entreprise permet également d'assurer que les enjeux importants en matière de sécurité sont pris en compte dès le début du cycle de développement des systèmes et qu'ils sont

directement liés à la mission ainsi qu'aux processus opérationnels. En outre, le processus facilite l'intégration de l'architecture de sécurité de l'information à l'architecture d'entreprise, conformément aux stratégies organisationnelles de gestion des risques et de sécurité de l'information. Contrôles connexes : AT-3, SA-8.

Améliorations du contrôle :

Aucune

Références :

SCT, *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* [Référence 7].

SA-4 PROCESSUS D'ACQUISITION

Contrôle :

(A) L'organisme inclut, explicitement ou en référence, les exigences, les descriptions et les critères suivants dans le contrat d'acquisition des systèmes d'information, des composants de systèmes ou des services liés aux systèmes d'information, et ce, conformément aux lois applicables du GC, aux politiques, directives et normes du SCT, ainsi qu'aux besoins de la mission et des opérations :

(a) exigences fonctionnelles de sécurité;

(b) exigences relatives à la force de la sécurité;

(c) exigences relatives à l'assurance de la sécurité;

(d) exigences relatives à la documentation portant sur la sécurité;

(e) exigences relatives à la protection de la documentation portant sur la sécurité;

(f) description de l'environnement de développement des systèmes d'information et de l'environnement opérationnel desdits systèmes;

(g) critères d'acceptation.

(AA) L'organisation inclut, explicitement ou en référence, de la documentation sur la sécurité et des exigences ou des spécifications fonctionnelles de sécurité dans les contrats d'acquisition de systèmes d'information, et ce, en fonction des résultats d'une évaluation des risques et conformément à la *Norme de sécurité et de gestion des marchés du SCT* [Référence 25].

(BB) L'organisation inclut, explicitement ou en référence, les exigences ou les spécifications liées au développement et à l'évaluation dans les contrats d'acquisition de systèmes, et ce, en fonction des résultats d'une évaluation des risques et conformément aux lois du GC et aux politiques, directives et normes applicables du SCT.

Conseils supplémentaires : À la fois discrets et identifiables, les composants d'un système d'information (p. ex. le matériel, les logiciels ou les microgiciels) sont des biens de technologie de l'information qui constituent les fondements d'un système d'information. Les composants d'un système d'information comprennent également des produits commerciaux de technologie de l'information. Les exigences fonctionnelles de sécurité comprennent les capacités, les fonctions de sécurité ainsi que les mécanismes de sécurité. Les exigences relatives à la force de la sécurité qui s'appliquent aux capacités, aux fonctions et aux mécanismes énoncent le degré de fonctionnement, d'achèvement, de résistance aux attaques directes et de résistance au trafiquage ou aux contournements. Les exigences d'assurance de sécurité comprennent ce qui suit : (i) les processus, les procédures, les pratiques et la méthodologie de développement; (ii) les preuves tirées des activités de développement et d'évaluation, qui permettent de conclure assurément que les fonctionnalités de sécurité exigées ont été mises en œuvre et que le

niveau de force de la sécurité a été atteint. Les exigences relatives à la documentation sur la sécurité concernent toutes les phases du cycle de développement des systèmes.

Les exigences liées à la fonctionnalité, à l'assurance ainsi qu'à la documentation se traduisent par des contrôles de sécurité et des améliorations de contrôles, qui sont choisis par le biais d'un processus de personnalisation. Le processus de personnalisation des contrôles de sécurité comprend, à titre d'exemple, la définition de valeurs de paramètres par des énoncés d'affectation et de sélection, et par la spécification des dépendances concernant les plateformes et des renseignements sur la mise en œuvre. La documentation de sécurité fournit, aux utilisateurs et aux administrateurs, des conseils sur la mise en œuvre et le fonctionnement des contrôles de sécurité. Le degré de détail requis dans la documentation de sécurité se fonde sur la catégorie de sécurité ou sur le niveau de classification des systèmes d'information, de même que sur l'ampleur de la dépendance à l'égard des capacités, des fonctions ou des mécanismes que les organismes manifestent dans l'exercice de fonctions qui visent notamment à répondre aux attentes globales en matière de réaction aux risques (tel qu'il est défini dans la stratégie organisationnelle de gestion des risques). Les exigences de sécurité peuvent également comporter des paramètres de configuration mandatés pour l'organisation, qui spécifient les fonctions, les ports, les protocoles ainsi que les services qui sont autorisés. Le critère d'acceptation visant les systèmes d'information de même que les composants et les services qui s'y rapportent sont définis de la même façon que les critères visant toute acquisition ou tout approvisionnement organisationnels. Contrôles connexes : CM-6, PL-2, PS-7, SA-3, SA-5, SA-8, SA-11, SA-12.

Améliorations du contrôle :

(1) PROCESSUS D'ACQUISITION | PROPRIÉTÉS FONCTIONNELLES DES CONTRÔLES DE SÉCURITÉ

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe fournisse une description des propriétés fonctionnelles des contrôles de sécurité à employer.

Conseils supplémentaires sur l'amélioration : Les propriétés fonctionnelles des contrôles de sécurité décrivent une fonctionnalité (p. ex. une capacité de sécurité, une fonction ou un mécanisme) qui est visible par l'intermédiaire de l'interface des contrôles. De plus, elles excluent les fonctionnalités et les structures de données qui sont au cœur du fonctionnement des contrôles. Contrôle connexe : SA-5.

(2) PROCESSUS D'ACQUISITION | CONCEPTION / CONTRÔLES DE SÉCURITÉ : RENSEIGNEMENTS RELATIFS À LA MISE EN ŒUVRE

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe fournisse des renseignements sur la conception et la mise en œuvre des contrôles de sécurité à employer, ce qui comprend ce qui suit : [*Sélection (une ou plusieurs) : interfaces de systèmes externes ayant trait à la sécurité; conception de haut niveau; conception de bas niveau; code source ou schémas des composants matériels*; [*Affectation : renseignements produits par l'organisme sur la conception/sur la mise en œuvre*]] selon [*Affectation : degré de détails définit par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les organisations pourraient exiger un degré différent de détail concernant la conception et la mise en œuvre des contrôles de sécurité à employer dans les systèmes organisationnels d'information, les composant de systèmes ou les services connexes en fonction des exigences de la mission ou des opérations, des exigences en matière de fiabilité et de résilience, et des exigences en matière d'analyse et de tests. Les systèmes d'information peuvent être partitionnés en plusieurs sous-systèmes. Chacun de ces sous-systèmes peut également comprendre un ou plusieurs modules. La conception de haut niveau pour les systèmes se traduit par une multiplicité de sous-systèmes interreliés par des interfaces qui fournissent des fonctionnalités de sécurité. La conception de bas niveau pour les systèmes se traduit par la création de modules axés sur les logiciels et les microgiciels (sans exclure le côté matériel pour autant) reliés par des interfaces qui fournissent des fonctionnalités de sécurité. Le code source et les schémas de composants matériels sont principalement considérés comme des représentations de la mise en œuvre d'un système d'information. Contrôle connexe : SA-5.

(3) PROCESSUS D'ACQUISITION | MÉTHODES DE DÉVELOPPEMENT / TECHNIQUES / PRATIQUES

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe montre que le cycle de développement d'un système donné comprenne [*Affectation : méthodes d'ingénierie de système/de sécurité, méthodes de développement de logiciels, et processus relatifs aux tests, à l'évaluation, aux techniques de validation et au contrôle de la qualité, qui sont conformes aux pratiques en vigueur et définis par l'organisme*].

Conseils supplémentaires sur l'amélioration : Le fait de suivre un cycle de développement de système – qui soit adéquatement défini et qui comprenne des méthodes de développement de logiciels conformes aux normes en vigueur, des méthodes d'ingénierie de système et de sécurité, des processus de contrôle de la qualité, ainsi que des techniques de test, d'évaluation et de validation – contribue à réduire le nombre et la sévérité des éventuelles erreurs pouvant survenir dans les systèmes d'information, les composants de systèmes ou les services connexes. La réduction du nombre et de la sévérité de telles erreurs diminue également le nombre des vulnérabilités d'un système donné, de ses composants et de ses services. Contrôle connexe : SA-12.

(4) PROCESSUS D'ACQUISITION | AFFECTATION DES COMPOSANTS AUX SYSTÈMES

[Annulé : Intégré au contrôle CM-8 (9)]

(5) PROCESSUS D'ACQUISITION | SYSTÈME / COMPOSANT / CONFIGURATION DES SERVICES

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe exécute ce qui suit :

(a) produire un système, des composants ou des services dont les [*Affectation : configuration de sécurité définies par l'organisation*] sont mises en œuvre;

(b) utiliser les configurations à titre de valeur par défaut pour tout système, composant ou service devant faire ultérieurement l'objet d'une réinstallation ou d'une mise à niveau.

Conseils supplémentaires sur l'amélioration : Les caractéristiques de sécurité comprennent, notamment, l'exigence selon laquelle tous les mots de passe par défaut doivent avoir été changés. Contrôle connexe : CM-8.

(6) PROCESSUS D'ACQUISITION | UTILISATION DE PRODUITS D'ASSURANCE DE L'INFORMATION

(a) L'organisation utilise uniquement des produits gouvernementaux sur étagère (GOTS) ou des produits commerciaux sur étagère (COTS) de sécurité des TI et de technologie de l'information à sécurité activée, qui sont partie intégrante d'une solution approuvée par le CST dans le but de protéger l'information classifiée lorsque les réseaux servant à transmettre cette information ont un niveau de classification inférieur à celui de l'information transmise.

(b) L'organisation veille à ce que ces produits aient été évalués/validés par le CST ou conformément à des procédures approuvées par le CST.

Conseils supplémentaires sur l'amélioration : Il est possible que les produits de sécurité des TI ou de technologie de l'information à sécurité activée qui sont utilisés pour protéger l'information classifiée par des moyens cryptographiques doivent utiliser une méthode de gestion des clés approuvée par le CST. La cryptographie doit être conforme aux exigences du contrôle de sécurité SC-13. Contrôles connexes : SC-8, SC-12, SC-13.

(7) PROCESSUS D'ACQUISITION | PROFILS DE PROTECTION APPROUVÉS PAR LE NATIONAL INFORMATION ASSURANCE PARTNERSHIP (NIAP)

(a) L'organisation permet l'utilisation de produits de TI commerciaux spécialisés en assurance de l'information ou prenant en charge l'assurance de l'information, à condition que ces derniers aient répondu aux exigences du profil de protection homologué par le CST et correspondant à leur type de technologie, si un tel profil existe.

(b) Si aucun profil de protection homologué par le CST existe pour le type de technologie en question, mais qu'un produit commercial de technologie de l'information s'appuie sur une fonctionnalité cryptographique pour appliquer sa politique de sécurité, l'organisation exige que le module cryptographique soit homologué FIPS.

Conseils supplémentaires sur l'amélioration : Contrôles connexes : SC-12, SC-13.

(8) PROCESSUS D'ACQUISITION | PLAN DE SURVEILLANCE CONTINUE

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe produise un plan de surveillance continue de l'efficacité des contrôles de sécurité, qui contienne [*Affectation : degré de détails défini par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les plans de surveillance continue visent à établir si l'intégralité des contrôles de sécurité qui sont planifiés, exigés et déployés au sein du système d'information, des composants du système ou des services connexes continuent d'être efficaces, en se fondant sur les changements inévitables appelés à survenir. Le développement des plans de surveillance continue produisent un degré de détails tel que l'information fournie peut être intégrée aux stratégies et programmes de surveillance continue mis en œuvre par les organisations. Contrôle connexe : CA-7.

(9) PROCESSUS D'ACQUISITION | FONCTIONS / PORTS / PROTOCOLES / SERVICES UTILISÉS

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe identifie, dès le début du cycle de développement des systèmes, les fonctions, les ports, les protocoles et les services qui seront utilisés dans l'organisation.

Conseils supplémentaires sur l'amélioration : L'identification précoce des fonctions, des ports, des protocoles et des services (p. ex. pendant les phases initiales de définition des besoins et de conception) permet aux organisations d'influer sur la modélisation d'un système d'information, de ses composants ou des services connexes. Cette intervention précoce dans le cycle de développement des systèmes permet aux organisations d'éviter ou de réduire au minimum l'utilisation des fonctions, des ports, des protocoles ou des services pouvant poser des risques tout aussi importants qu'inutiles, et de comprendre les avantages de bloquer l'accès à certains ports, protocoles ou services (ou lorsqu'il s'agit de demander à des fournisseurs de services de systèmes d'information de faire de même). Une identification hâtive des fonctions, des ports, des protocoles et des services évite d'avoir à reconfigurer les contrôles de sécurité après la mise en œuvre d'un système d'information, de ses composants ou des services connexes. Le SA-9 décrit les exigences relatives aux services de systèmes d'information externes des organisations, et identifie les fonctions, les ports, les protocoles et les services qui sont fournis depuis des sources externes. Contrôles connexes : CM-7, SA-9.

Références :

SCT, *Norme de sécurité et de gestion des marchés* [Référence 25].
CST, *ITSA-11, Algorithmes cryptographiques approuvés par le CST pour la protection des renseignements protégés* [Référence 8].
CST, *ITSB-40A, Politique du gouvernement du Canada pour la protection de l'information classifiée à l'aide d'algorithmes Suite B* [Référence 28].

SA-5 DOCUMENTATION RELATIVE AUX SYSTÈMES D'INFORMATION

Contrôle :

(A) L'organisation obtient la documentation du développeur d'un système d'information, d'un composant du système ou d'un service connexe, laquelle décrit ce qui suit :

(a) la configuration, l'installation et l'exploitation sécurisées du système, des composants ou des services;

(b) l'utilisation et la maintenance efficaces des fonctions et mécanismes de sécurité;

(c) les vulnérabilités connues associées à la configuration et à l'utilisation des fonctions administratives (c.-à-d. privilégiées).

(B) L'organisation obtient la documentation de l'utilisateur d'un système d'information, d'un composant du système ou d'un service connexe, laquelle décrit ce qui suit :

(a) les fonctions et mécanismes de sécurité accessibles à l'utilisateur, et la façon de les utiliser efficacement;

(b) les méthodes d'interaction de l'utilisateur qui lui permettent d'utiliser plus sécuritairement le système, ses composants ou les services connexes;

(c) les responsabilités de l'utilisateur concernant le maintien de la sécurité du système, de ses composants ou des services connexes.

(C) L'organisation documente les tentatives visant à obtenir des documents sur le système d'information, sur ses composants ou sur les services connexes, qui n'existent pas ou qui ne sont pas disponibles. Elle réagit en [*Affectation : mesure définie par l'organisation*].

(D) L'organisation protège la documentation en fonction des besoins, conformément à la stratégie de gestion des risques.

(E) L'organisation distribue la documentation aux [*Affectation : personnel ou rôles définis par l'organisation*].

Conseils supplémentaires : Ce contrôle permet au personnel des organisations de bien comprendre la logique de mise en œuvre et de fonctionnement des contrôles de sécurité associés aux systèmes d'information, à leurs composants ou aux services connexes. Les organisations envisagent d'établir des mesures spécifiques visant à définir le degré de qualité/d'achèvement du contenu fourni. L'incapacité d'obtenir les documents requis peut survenir, par exemple, en raison de la désuétude d'un système/d'un composant ou encore du peu de soutien de la part des développeurs et des contractants. Dans ces situations, l'organisation devra peut-être recréer une partie de la documentation, si celle-ci s'avère nécessaire à la mise en œuvre ou à l'exploitation efficaces des contrôles de sécurité. Le niveau de protection s'appliquant à la documentation relative à certains systèmes d'information, à certains composants ou à certains services est proportionnel à la catégorie de sécurité ou à la classification desdits systèmes. La documentation portant sur les vulnérabilités des systèmes d'information pourrait également nécessiter un niveau de protection accru. L'exploitation sécurisée d'un système d'information comprend, par exemple, le démarrage initial du système et la reprise sécuritaire des opérations du système après le signalement d'une anomalie. Contrôles connexes : CM-6, CM-8, PL-2, PL-4, PS-2, SA-3, SA-4.

Améliorations du contrôle :

(1) DOCUMENTATION RELATIVE AU SYSTÈME D'INFORMATION | PROPRIÉTÉS FONCTIONNELLES DES CONTRÔLES DE SÉCURITÉ

[Annulée : Intégrée au contrôle SA-4 (1)]

(2) DOCUMENTATION RELATIVE AU SYSTÈME D'INFORMATION | INTERFACES DE SYSTÈME EXTERNES RELATIVES À LA SÉCURITÉ

[Annulée : Intégrée au contrôle SA-4 (2)]

(3) DOCUMENTATION RELATIVE AU SYSTÈME D'INFORMATION | CONCEPTION DE HAUT NIVEAU

[Annulée : Intégrée au contrôle SA-4 (2)]

(4) DOCUMENTATION RELATIVE AU SYSTÈME D'INFORMATION | CONCEPTION DE BAS NIVEAU

[Annulée : Intégrée au contrôle SA-4 (2)]

(5) DOCUMENTATION RELATIVE AU SYSTÈME D'INFORMATION | CODE SOURCE

[Annulée : Intégrée au contrôle SA-4 (2)]

Références :

Aucune

SA-6 RESTRICTIONS RELATIVES À L'UTILISATION DES LOGICIELS

[Annulé : Intégré aux contrôles CM-10 et SI-7]

SA-7 LOGICIELS INSTALLÉS PAR L'UTILISATEUR

[Annulé : Intégré aux contrôles CM-11 et SI-7]

SA-8 PRINCIPES D'INGÉNIERIE DE SÉCURITÉ

Contrôle :

(A) L'organisation applique les principes de l'ingénierie de sécurité aux spécifications, à la conception, au développement, à la mise en œuvre et à la modification du système d'information.

Conseils supplémentaires sur l'amélioration : Habituellement, les organisations appliquent les principes d'ingénierie de sécurité aux systèmes d'information en développement ou aux systèmes existants faisant l'objet de mises à niveau majeures. Dans le cas des systèmes existants, les organisations appliquent, dans la mesure du possible, les principes d'ingénierie de sécurité aux mises à niveau et aux modifications en tenant compte de l'état actuel du matériel, des logiciels et des micrologiciels des systèmes en question. Les exemples de principes d'ingénierie de sécurité comprennent entre autres : (i) le développement de protections en couches; (ii) l'établissement de politiques, d'architectures et de contrôles de sécurité sains comme base de la conception; (iii) l'intégration des exigences de sécurité au cycle de développement des systèmes; (iv) la délimitation des périmètres de sécurité physiques et logiques; (v) la formation appropriée des développeurs pour leur permettre de créer des logiciels sécurisés; (vi) la personnalisation des contrôles de sécurité en fonction des besoins organisationnels et opérationnels; (vii) la modélisation des menaces dans le but d'identifier les cas types, les sources des menaces, les vecteurs d'attaque ainsi que les schèmes d'attaque, ainsi que l'optimisation des contrôles et des schémas de conception dans le but d'atténuer les risques; et (viii) la réduction du facteur de risque à un niveau acceptable, ce qui facilite la prise de décisions éclairées en matière de gestion des risques. Contrôles connexes : SA-3, SA-4, SA-17, SC-2, SC-3.

Améliorations du contrôle :

(100) L'organisation recourt à des ingénieurs brevetés et agréés en sécurité qui assument la responsabilité des spécifications, de la conception, du développement et de la mise en œuvre de solutions de sécurité du système d'information.

Références :

Aucune

SA-9 SERVICES DE SYSTÈME D'INFORMATION EXTERNES

Contrôle :

(A) L'organisation exige que les fournisseurs de services de système d'information externes respectent ses exigences en matière de contrôle de sécurité de l'information et utilisent [*Affectation : contrôles de sécurité définis et conformes aux besoins de l'organisation*] conformément à la *Norme de sécurité et de gestion des marchés du SCT* [Référence 25].

(B) L'organisation définit et documente la surveillance gouvernementale, de même que les rôles et responsabilités des utilisateurs en ce qui a trait aux services externes de système d'information.

(C) L'organisme utilise des [*Affectation : méthodes, techniques et processus définis par l'organisation*] dans le but de surveiller en tout temps la conformité des fournisseurs de services externes aux contrôles de sécurité.

Conseils supplémentaires : Les systèmes d'information externes sont mis en œuvre à l'extérieur des limites d'autorisation des systèmes organisationnels d'information**.** Ils comprennent notamment les services qui sont utilisés par les systèmes organisationnels d'information sans en faire partie pour autant. Les politiques du SCT exigent que les organisations qui ont recours à des fournisseurs de services externes pour le traitement, le stockage ou la transmission des informations du GC ou pour l'exploitation des systèmes d'information au nom du GC s'assurent que lesdits fournisseurs répondent aux mêmes exigences de sécurité que celles qui sont imposées aux ministères et organismes. Les organisations établissent divers types de relations avec les fournisseurs de services externes, notamment le modèle des coentreprises, les partenariats d'affaires, les accords d'impartition (c.-à-d. contrats, ententes inter-organismes, ententes liées aux secteurs d'activité), les accords de licence ou les échanges de chaîne d'approvisionnement. La responsabilité en matière de gestion des risques pouvant découler du recours à des services de système d'information externes continue d'incomber aux autorités responsables. Dans le cas des services externes, la chaîne de confiance exige que les organisations créent et maintiennent un niveau de confiance en la capacité de chaque fournisseur participant à une relation client-fournisseur potentiellement complexe d'assurer une protection adéquate des services rendus. La portée et la nature de la chaîne de confiance varient en fonction des relations établies entre les organisations et les fournisseurs externes. Les organisations prennent note des bases de la relation de confiance pour que celle-ci puisse faire l'objet d'une surveillance occasionnelle. La documentation des services de système d'information externes comprend les rôles et responsabilités du gouvernement, des fournisseurs de services et des utilisateurs terminaux en matière de sécurité, ainsi que toute entente de niveau de service pertinente. Les ententes de niveau de service définissent les attentes de rendement pour les contrôles de sécurité, décrivent les résultats mesurables et identifient les exigences en matière de solution et d'intervention pour les situations de non-respect relevée. Contrôles connexes : CA-3, IR-7, PS-7.

Améliorations du contrôle :

(1) SYSTÈMES D'INFORMATION EXTERNES | ÉVALUATIONS DES RISQUES / APPROBATIONS ORGANISATIONNELLES

(a) L'organisation effectue une évaluation des risques avant l'acquisition ou l'impartition des services spécialisés de sécurité de l'information.

(b) L'organisation s'assure que l'acquisition ou l'impartition de ces services est approuvée par [*Affectation : personnel ou rôles désignés par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les services spécialisés de sécurité de l'information comprennent, par exemple, la surveillance et l'analyse des incidents de même que les interventions connexes, l'exploitation des dispositifs liés à la sécurité de l'information tels les coupe-feux, ou encore les services de gestion des clés. Contrôles connexes : CA-6, RA-3.

(2) SYSTÈMES D'INFORMATION EXTERNES | IDENTIFICATION DES FONCTIONS / PORTS / PROTOCOLES / SERVICES

L'organisation exige que les fournisseurs de [*Affectation : services de systèmes d'information externes désignés par l'organisation*] identifient les fonctions, les ports, les protocoles et les autres services qui sont requis pour l'utilisation des services en question.

Conseils supplémentaires sur l'amélioration : L'information provenant de fournisseurs de services externes en ce qui a trait aux fonctions, ports, protocoles et services utilisés aux fins de la prestation des services en question peut s'avérer particulièrement utile, lorsqu'il s'agit de comprendre pourquoi il est avantageux d'imposer certaines restrictions à des services ou à des fonctions ou encore de bloquer certains ports ou protocoles. Contrôle connexe : CM-7.

(3) SYSTÈMES D'INFORMATION EXTERNES | ÉTABLIR / MAINTENIR UNE RELATION DE CONFIANCE AVEC LES FOURNISSEURS DE SERVICES

L'organisation établit, documente et maintient une relation de confiance avec les fournisseurs de services externes en se fondant sur [*Affectation : exigences de sécurité, propriétés, facteurs ou conditions définissant ce qui constitue une relation de confiance adéquate]*.

Conseils supplémentaires sur l'amélioration : Le degré de certitude permettant de percevoir comme acceptable le risque découlant du recours à un fournisseur de services externe dépend de la confiance que les organisations témoignent à l'endroit de ces fournisseurs externes ou d'un groupe de ces fournisseurs externes. La relation de confiance permet aux organisations d'accroître le degré de certitude à l'égard de l'aptitude des fournisseurs de services à garantir un rendement adéquat en matière de sécurité. De telles relations peuvent s'avérer compliquées en raison du nombre des intervenants qui interagissent, des relations hiérarchiques et des niveaux de confiance, ainsi que de la nature des interactions entre les divers intervenants. Dans certains cas, le degré fiabilité se fonde sur le nombre des contrôles directs que les organisations sont en mesure d'exercer sur les fournisseurs de services pour ce qui a trait aux contrôles de sécurité qu'il est nécessaire de mettre en place pour assurer la protection du service et de l'information, ainsi que sur les facteurs permettant de prouver l'efficacité des contrôles en place. Le niveau de contrôle est généralement établi selon les termes des contrats ou des ententes de niveau de service et peuvent varier entre les contrôles élémentaires (p. ex. recourir aux contrats ou aux ententes de niveau de service pour obtenir des services auxiliaires comme les services commerciaux de télécommunications) et les contrôles plus rigoureux (p. ex. négociation de contrats ou d'ententes énonçant les exigences de sécurité auxquelles les fournisseurs doivent répondre). Dans d'autres cas, le niveau de fiabilité se fonde sur des facteurs qui convainquent les organisations que les contrôles de sécurité requis ont été employés et sur la preuve de l'efficacité des contrôles en question. Par exemple, des services de système d'information externes autorisés distinctement et fournis à des organisations par l'intermédiaire d'une relation d'affaire bien établie pourraient fournir divers degrés confiance dans les services, et ce, dans un registre de risques acceptable par les organisations utilisatrices desdits services. Les fournisseurs de services externes peuvent, à leur tour, externaliser certains de leurs services à d'autres entreprises, ce qui complexifie la gestion des relations de confiance. Selon la nature des services, les organisations peuvent éprouver passablement de difficulté à accorder leur confiance aux fournisseurs externes. Cette difficulté ne tient pas forcément à une forme de méfiance naturelle à l'égard des fournisseurs, mais au niveau de risque inhérent aux services mêmes.

(4) SYSTÈMES D'INFORMATION EXTERNES | CONCORDANDCE DES INTÉRÊTS DES CLIENTS ET DES FOURNISSEURS

L'organisme emploie [*Affectation : mesures de protection définies par l'organisation*] pour veiller à ce que les intérêts de [*Affectation : fournisseurs de services externes désignés par l'organisation*] répondent aux intérêts de l'organisation.

Conseils supplémentaires sur l'amélioration : Comme les organisations comptent de plus en plus sur les services de fournisseurs externes, la possibilité que les intérêts des organisations et des fournisseurs divergent demeure entière. Dans de telles situations, la simple application de mesures de protection techniques, procédurales ou opérationnelles pourrait s'avérer insuffisante, particulièrement lorsque les fournisseurs responsables de la mise en œuvre et du contrôle de ces mesures de protection fonctionnent selon des modalités qui ne correspondent pas aux intérêts des organisations clientes. Pour résoudre de telles questions, les organisations disposent de diverses mesures, par exemple, l'exigence d'enquêtes de sécurité pour certains membres du personnel des fournisseurs externes, l'examen des registres de propriété, l'embauche exclusive de fournisseurs de services dont la fiabilité est démontrée (p. ex. fournisseurs qui ont satisfait aux exigences d'autres organisations), la visite périodique ou inopinée des installations de fournisseurs de services.

(5) SYSTÈMES D'INFORMATION EXTERNES | LIEUX DE TRAITEMENT, DE STOCKAGE, ET DE TRAITEMENT

Les organisations circonscrivent les lieux de [*Sélection (un ou plusieurs) : services de traitement de l'information; de stockage d'information/de données; de systèmes d'information*] à [*Affectation : lieux désignés par les organisations*] en se fondant sur [*Affectation : exigences ou conditions définies par les organisations*].

Conseils supplémentaires sur l'amélioration : Le choix des lieux de prestation des services essentiels de traitement de l'information, de stockage d'information/de données, ou l'emplacement des systèmes

d'information peuvent avoir une incidence directe sur l'aptitude des organisations à exécuter adéquatement leur mission ou leurs opérations. Ce type de situation se présente lorsque des fournisseurs externes administrent eux-mêmes les lieux de traitement, de stockage ou de service. Les critères que les fournisseurs externes utilisent pour la désignation des lieux de traitement, de stockage ou de service pourraient ne pas correspondre à ceux des organisations. Par exemple, les organisations pourraient souhaiter que les lieux de stockage d'information/de données se limitent à certains sites, de façon à faciliter les activités d'intervention en cas d'incident (p. ex. analyses judiciaires, investigations post-incidents) advenant la compromission/la violation des mesures de sécurité de l'information. De telles activités d'intervention en cas d'incident pourraient être entravées par les lois ou protocoles en vigueur dans les sites où le traitement et le stockage ont lieu ou dans les sites depuis lesquels les services de systèmes fonctionnent.

Références :

SCT, *Norme de sécurité et de gestion des marchés* [Référence 25].

SA-10 GESTION DES CONFIGURATIONS PAR LES DÉVELOPPEURS

Contrôle :

(A) L'organisation exige que le développeur d'un système d'information, de ses composants ou des services connexes se charge de la gestion de configuration pendant [*Sélection (un ou plusieurs) : conception; développement; mise en œuvre; exploitation*] du système, de ses composants ou des services connexes.

(B) L'organisation exige que le développeur d'un système d'information, de ses composants ou des services connexes documente, gère et contrôle l'intégrité des changements apportés à [*Affectation : éléments de configuration faisant partie de la gestion de configuration définie par l'organisation*].

(C) L'organisation exige que le développeur d'un système d'information, de ses composants ou des services connexes mette exclusivement en œuvre les changements approuvés par l'organisme pour les systèmes, composants ou services.

(D) L'organisation exige que le développeur d'un système d'information, de ses composants ou des services connexes documente les changements approuvés par l'organisme (pour les systèmes, composants ou services) ainsi que les répercussions possibles de ces changements sur la sécurité.

(E) L'organisation exige que le développeur d'un système d'information, de ses composants ou des services connexes fasse le suivi des lacunes de sécurité (et des solutions) signalées dans les systèmes, les composants ou les services et qu'il fasse part de ses observations auprès de [*Affectation : personnel désigné par l'organisation*].

Conseils supplémentaires : Ce contrôle s'applique également aux organisations qui procèdent au développement ou à l'intégration de systèmes d'information internes. Les organisations considèrent la qualité et l'achèvement des activités de gestion de configuration menées par les développeurs comme des preuves de l'application efficace des mesures de protection. Les mesures de protection peuvent notamment comprendre la protection contre les modifications ou les destructions non autorisées des copies maîtresses de tout le matériel utilisé pour générer certains aspects de la sécurité matérielle, logicielle ou microgicielle du système. Le maintien de l'intégrité des changements apportés au système d'information, à ses composants ou aux services connexes requiert que le contrôle de configuration, pendant l'intégralité du cycle de développement de système, enregistre les changements autorisés et empêche les changements non autorisés. Les éléments de configuration qui font partie de la gestion de configuration (si les autres contrôles de sécurité en exigent l'existence ou l'utilisation) sont les suivants : le modèle formel; les spécifications de conception fonctionnelles, de haut niveau et de bas niveau; les autres données de conception; la documentation relative à la mise en œuvre; les schémas relatifs au code source et aux composants matériels; la version active du code exécutable; les outils de comparaison des descriptions de nouvelles versions de composants matériels ou de code source de logiciels/de microgiciels avec

les versions précédentes; et les accessoires ainsi que la documentation de test. En fonction des missions et des besoins opérationnels des organisations ou selon la nature des relations contractuelles en vigueur, les développeurs peuvent se charger de la gestion de configuration pendant les phases d'exploitation et de maintenance du cycle de vie. Contrôles connexes : CM-3, CM-4, CM-9, SA-12, SI-2.

Améliorations du contrôle :

(1) GESTION DES CONFIGURATIONS PAR LES DÉVELOPPEURS | VÉRIFICATION DE L'INTÉGRITÉ DES LOGICIELS / MICROGICIELS

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe active la fonction de vérification de l'intégrité des logiciels et des microgiciels.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle permet aux organisations de détecter les changements non autorisés apportés aux logiciels et aux microgiciels par le recours à des outils, des techniques ou des mécanismes fournis par les développeurs. Les mécanismes de vérification de l'intégrité peuvent également détecter la contrefaçon de logiciels et de microgiciels. Les organisations vérifient l'intégrité des logiciels et des microgiciels au moyen, par exemple, du hachage unidirectionnel sécurisé fourni par les développeurs. Les logiciels et microgiciels qui sont produits incluent également les mises à jour/à niveau requises. Contrôle connexe : SI-7.

(2) GESTION DES CONFIGURATIONS PAR LES DÉVELOPPEURS | PROCESSUS DE GESTION DES CONFIGURATIONS DE RECHANGE

L'organisation prévoit un processus de gestion des configurations de rechange auquel participent des membres de son personnel en l'absence d'une équipe de développeurs spécialisés en gestion des configurations.

Conseils supplémentaires sur l'amélioration : Les processus de gestion des configurations de rechange pourraient être requis, par exemple, lorsque des organisations utilisent des produits commerciaux de technologie de l'information (COTS). Les processus de gestion des configurations de rechange comprend le personnel organisationnel répondant aux conditions suivantes : (i) responsable de l'examen/de l'approbation des changements proposés pour les systèmes d'information, pour leurs composants ou pour les services connexes; et (ii) chargé de mener des analyses d'impact sur la sécurité préalablement à la mise en œuvre de tout changement aux systèmes, aux composants ou aux services (p. ex. un comité de contrôle des configurations qui envisage les impacts des changements sur la sécurité pendant le développement et qui se compose de représentants de l'organisation et des développeurs, s'il y a lieu).

(3) GESTION DES CONFIGURATIONS PAR LES DÉVELOPPEURS | VÉRIFICATION DE L'INTÉGRITÉ DU MATÉRIEL

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe active la fonction de vérification de l'intégrité des composants matériels.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle permet aux organisations de détecter les changements non autorisés apportés aux composants matériels par le recours à des outils, des techniques ou des mécanismes fournis par les développeurs. Les organisations vérifient l'intégrité des composants matériels, par exemple, en exigeant des étiquettes irreproductibles et des numéros de série vérifiables fournis par les développeurs et en exigeant la mise en application de mécanismes d'inviolabilité. Les composants matériels qui sont produits incluent également les mises à jour/à niveau requises. Contrôle connexe : SI-7.

(4) GESTION DES CONFIGURATIONS PAR LES DÉVELOPPEURS | GÉNÉRATION FIABLE

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe emploie des outils permettant de comparer les versions nouvellement générées de descriptions de composants matériels de sécurité ou de de code source/de code exécutable de logiciels/de microgiciels avec les versions précédentes.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle résout la question des changements apportés aux composants matériels, aux logiciels et aux microgiciels entre les diverses

version en cours de développement. En revanche, le SA-10 (1) et le SA-10 (3) permettent aux organisations de détecter les changements non autorisés apportés aux composants matériels, aux logiciels et aux microgiciels par le recours à des outils, des techniques ou des mécanismes fournis par les développeurs.

(5) GESTION DES CONFIGURATIONS PAR LES DÉVELOPPEURS | MAPPAGE DE L'INTÉGRITÉ AUX FINS DE CONTRÔLE DES VERSIONS

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe maintienne l'intégrité du mappage entre les données de la version maîtresse (schémas du matériel et code logiciel/micrologiciel) qui décrivent la version en cours du matériel, des logiciels et des micrologiciels servant à la sécurité, d'une part, et d'autre part, la copie maîtresse des données de la version en cours, qui se trouve sur le site.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle résout la question des changements apportés aux composants matériels, aux logiciels et aux microgiciels pendant le développement initial et pendant les mises à jour/à niveau du cycle de vie du système. Le maintien de l'intégrité entre les copies maîtresses des composants matériels, des logiciels et des microgiciels (y compris les éléments de conception et le code source) et les données équivalentes des copies maîtresses sur le site des environnements opérationnels est essentiel, lorsqu'on souhaite garantir la disponibilité des systèmes organisationnels d'information dont dépendent les missions prioritaires ou les fonctions opérationnelles.

(6) GESTION DES CONFIGURATIONS PAR LES DÉVELOPPEURS | DISTRIBUTION FIABLE

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe exécute les procédures visant à garantir que les mises à jour/à niveau des composants matériels, des logiciels et des microgiciels servant à la sécurité, qui sont distribuées à l'organisation sont en tout point conformes aux spécifications des copies maîtresses.

Conseils supplémentaires sur l'amélioration : La distribution en toute confiance des mises à jour/à niveau des composants matériels, des logiciels et des microgiciels permet de garantir que lesdites mises à jour/à niveau constituent des représentations fidèles des copies maîtresses maintenues par le développeur et qu'elles n'ont pas été trafiquées en cours de distribution.

Références :

Aucune

SA-11 TESTS DE SÉCURITÉ EFFECTUÉS PAR LES DÉVELOPPEURS

Contrôle :

(A) L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe crée et mette en œuvre un plan d'évaluation de la sécurité.

(B) L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe exécute des tests/des évaluations de [*Sélection (un ou plusieurs) : unité; intégration; système; régression*] selon [*Affectation : profondeur et couverture définies par l'organisation*].

(C) L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe produise les preuves de l'exécution du plan d'évaluation de la sécurité ainsi que les résultats des tests/de l'évaluation de sécurité.

(D) L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe mette en œuvre un processus vérifiable de correction des lacunes.

(E) L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe corrige les lacunes signalées pendant les tests/les évaluations de sécurité.

Conseils supplémentaires : Les tests et les évaluations de sécurité de développement ont lieu à toutes les phases post-conception du cycle de développement des systèmes. De tels tests et évaluations confirment que les contrôles de sécurité requis ont été adéquatement mis en œuvre, qu'ils fonctionnent selon les attentes, qu'ils permettent d'appliquer la politique de sécurité en vigueur et qu'ils répondent aux exigences de sécurité établies. L'interconnexion des composants de systèmes ou les changements apportés à ces derniers pourraient influer sur les propriétés de sécurité des systèmes d'information. Ces interconnexions ou changements (p. ex. mise à niveau ou remplacement d'applications ou de systèmes d'exploitation) peuvent avoir un effet défavorable sur les contrôles de sécurité mis en œuvre précédemment. Ce contrôle fournit des modalités de test/d'évaluation complémentaires que les développeurs peuvent utiliser dans le but de réduire ou d'éliminer les lacunes éventuelles. Les tests visant les applications logicielles sur mesure pourraient nécessiter des mesures axées sur les analyses statiques, les analyses dynamiques, les analyses binaires ou encore des analyses recourant à une combinaison des types d'analyse précités. Les développeurs peuvent employer ces types d'analyses dans plusieurs outils (p. ex. analyseurs d'application Web, outils d'analyse statique, analyseurs binaires) ainsi que dans des examens de code source. Les plans d'évaluation de sécurité énoncent spécifiquement les activités que les développeurs seront appelés à mener, notamment des analyses, des tests, des évaluations et des examens visant des composants logiciels ou micrologiciels, le degré de rigueur à respecter ainsi que les types d'artéfacts produits durant ces activités. La profondeur (*depth*) des tests et des évaluations renvoie au degré d'exhaustivité et de précision associé aux processus d'évaluation (p. ex. tests en boîte noire, en boîte grise ou en boîte blanche). L'envergure des tests et des évaluations de sécurité renvoie à la portée (p. ex. nombre et type) des artéfacts compris dans le processus d'évaluation. Les contrats contiennent les critères d'acceptation relatifs aux plans d'évaluation de sécurité, les processus de correction des lacunes ainsi que les preuves que les plans/les processus ont été appliqués rigoureusement et en temps opportun. Les méthodes d'examen et de protection des plans d'évaluation, les preuves et la documentation sont proportionnelles à la catégorie de sécurité ou au niveau de classification du système d'information visé. Les contrats peuvent également fournir des exigences concernant la protection des documents. Contrôles connexes : CA-2, CM-4, SA-3, SA-4, SA-5, SI-2.

Améliorations du contrôle :

(1) TESTS ET ÉVALUATIONS DE SÉCURITÉ EFFECTUÉS PAR LES DÉVELOPPEURS | ANALYSE DE CODE STATIQUE

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe utilise des outils d'analyse de code statique pour identifier les lacunes courantes et documente les résultats de l'analyse.

Conseils supplémentaires sur l'amélioration : L'analyse de code statique fournit la technologie et la méthodologie nécessaire aux examens de sécurité. Ce type d'analyse peut être utilisé pour identifier les vulnérabilités de sécurité et pour commander l'observation des pratiques de codage de sécurité. L'analyse de code statique est particulièrement efficace quand elle est utilisée dans les premiers stades du processus de développement, lorsque les changements de code peuvent être automatiquement balayés dans le but de trouver les lacunes, le cas échéant. L'analyse statique peut fournir des conseils clairs en matière de correction et de défectuosité, de façon à assister les développeurs dans l'application de mesures correctives. Les preuves d'une mise en œuvre adéquate de l'analyse statique peuvent prendre diverses formes : agrégation de la densité des défauts pour les défauts critiques, preuve que les défauts ont été inspectés par les développeurs ou par les spécialistes de la sécurité, et preuves que les défauts ont été corrigés. Une trop forte densité de résultats inaperçus (couramment appelés des faux positifs) pourraient être le symptôme d'un problème se situant du côté des outils d'analyse ou de traitement. Dans de tels cas, les organisations établissent la validité des preuves en les comparant aux preuves provenant d'autres sources.

(2) TESTS ET ÉVALUATIONS DE SÉCURITÉ EFFECTUÉS PAR LES DÉVELOPPEURS | ANALYSE DES MENACES ET DES VULNÉRABILITÉS

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe procède à des analyses de menaces et de vulnérabilités ainsi qu'à des tests et des évaluations des systèmes, des composants ou des services définitifs.

Conseils supplémentaires sur l'amélioration : Les applications peuvent s'écarter considérablement des spécifications de fonction et de conception qui ont été créées pendant les phases de conception et de formulation des exigences du cycle de développement des systèmes. Par conséquent, les analyses de menaces et de vulnérabilités des systèmes d'information, des composants de systèmes ou des services connexes, qui sont effectuées préalablement à la mise en service, sont essentielles à une exploitation efficace de ces systèmes, composants et services. Les analyses de menaces et de vulnérabilités, à cette étape du cycle de développement des systèmes, permettent de veiller à ce que les changements sur le plan de la conception ou de la mise en œuvre ont été pris en compte et que toute nouvelle vulnérabilité résultant de ces changements a été examinée et a fait l'objet de mesures d'atténuation. Contrôle connexe : RA-5.

(3) TESTS ET ÉVALUATIONS DE SÉCURITÉ EFFECTUÉS PAR LES DÉVELOPPEURS | VÉRIFICATION INDÉPENDANTE DES PLANS D'ÉVALUATION / PREUVES

(a) L'organisation exige qu'un agent indépendant satisfaisant à [*Affectation : critères d'indépendance définis par l'organisation*] soit en mesure d'attester ou non de l'adéquation de la mise en œuvre du plan d'évaluation de sécurité et de vérifier les preuves produites pendant les tests/les évaluations de sécurité.

(b) L'organisation veille à ce que l'agent indépendant ait reçu suffisamment d'information pour mener à bien le processus de vérification ou dispose de l'autorité nécessaire pour obtenir ladite information.

Conseils supplémentaires sur l'amélioration : Les agents indépendants possèdent les compétences nécessaires (p. ex. connaissances, aptitudes, formation et expérience) pour être en mesure d'attester ou non de l'adéquation de la mise en œuvre des plans d'évaluation de sécurité du développeur. Contrôles connexes : AT-3, CA-7, RA-5, SA-12.

(4) TESTS ET ÉVALUATIONS DE SÉCURITÉ EFFECTUÉS PAR LES DÉVELOPPEURS | EXAMEN MANUEL DU CODE

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe procède à un examen manuel du code de [*Affectation : code spécifique désigné par l'organisation*] au moyen de [*Affectation : processus, procédures ou techniques définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les examens manuels de code sont généralement réservés aux composants fondamentaux (logiciels et microgiciels) des systèmes d'information. De tels examens de code sont singulièrement efficaces, lorsqu'il s'agit d'identifier les lacunes nécessitant une connaissance des exigences ou du contexte relatifs à l'application, lesquels sont généralement inaccessibles aux techniques et outils automatisés d'analyse comme les analyses statiques ou dynamiques. Au nombre des composants pouvant bénéficier des examens manuels, comptons notamment la comparaison des matrices de contrôle d'accès aux contrôles d'application, ainsi que l'examen approfondi des mises en œuvre et des contrôles cryptographiques.

(5) TESTS ET ÉVALUATIONS DE SÉCURITÉ EFFECTUÉS PAR LES DÉVELOPPEURS | TESTS DE PÉNÉTRATION / ANALYSES

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe procède à des tests de pénétration à [*Affectation : étendue/profondeur définies par l'organisation*] et selon [*Affectation : contraintes définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les tests de pénétration constituent des méthodes d'évaluation par lesquelles les évaluateurs tentent de contourner les fonctions de sécurité des produits de technologie de l'information et des systèmes d'information, et ce, en utilisant toutes la documentation disponible sur les produits de technologies de l'information et sur les systèmes d'information (p. ex. spécifications de conception de produits/de systèmes; code source; et guides de l'administrateur/de l'utilisateur) et en travaillant selon des contraintes spécifiquement définies. Les tests de pénétration peuvent comprendre notamment les tests en boîte blanche, en boîte grise ou en boîte noire avec des analyses menées par des professionnels de sécurité chevronnés, qui simulent des attaques. L'objectif des tests de pénétration est de mettre au jour les vulnérabilités potentielles des produits de technologies de l'information et des systèmes d'information pouvant résulter d'erreurs de mise en œuvre, de fautes de configuration ou encore de lacunes ou défectuosités du déploiement opérationnel. Les tests de pénétration peuvent être

effectués conjointement avec les examens de code manuels ou automatisés dans le but de produire des niveaux d'analyse plus élevés que ceux que l'on retrouve couramment.

(6) TESTS ET ÉVALUATIONS DE SÉCURITÉ EFFECTUÉS PAR LES DÉVELOPPEURS | EXAMEN DE LA SURFACE D'ATTAQUE

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe procède à des examens de surface d'attaque.

Conseils supplémentaires sur l'amélioration : Les surfaces d'attaque des systèmes d'information sont des secteurs exposés qui accentuent la vulnérabilité des systèmes aux cyberattaques. Elles comprennent tous les secteurs accessibles où des faiblesses/des défauts des systèmes d'information (y compris les composants matériels, logiciels et microgiciels) pourraient être exploités par des adversaires. Les examens de surface d'attaque permettent aux développeurs d'effectuer ce qui suit : (i) analyser les changements de conception et de mise en œuvre apportés aux systèmes d'information; (ii) et atténuer les vecteurs d'attaque générés consécutivement aux des changements. La correction des lacunes signalées peut comprendre, par exemple, la proscription des fonctions risquées.

(7) TESTS ET ÉVALUATIONS DE SÉCURITÉ EFFECTUÉS PAR LES DÉVELOPPEURS | VÉRIFICATION DE LA PORTÉE DES TESTS / ÉVALUATION

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe s'assure que l'étendue des tests/des évaluations de sécurité fournisse une couverture complète des contrôles de sécurité requis à [*Affectation : profondeur des tests/des évaluations définie par l'organisation*].

Conseils supplémentaires sur l'amélioration : Il est possible de vérifier si les tests/les évaluations de sécurité fournissent une couverture complète des contrôles de sécurité requis, et ce, au moyen d'une variété de techniques d'analyses formelles ou informelles. Chacune de ces techniques fournit un niveau d'assurance accru qui correspond au degré de formalité de l'analyse. Il est possible de rigoureusement démontrer que la couverture des contrôle de sécurité atteint des niveaux supérieurs d'assurance en recourant à la modélisation formelle et à des techniques d'analyse comme la corrélation entre la mise en œuvre de contrôles et des scénarios de tests comparables.

(8) TESTS ET ÉVALUATIONS DE SÉCURITÉ EFFECTUÉS PAR LES DÉVELOPPEURS | ANALYSE DE CODE DYNAMIQUE

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe utilise des outils d'analyse de code statique pour identifier les lacunes courantes et documente les résultats de l'analyse.

Conseils supplémentaires sur l'amélioration : L'analyse de code dynamique fournit une vérification d'exécution des programmes logiciels au moyen d'outils permettant de signaler l'occurrence de corruption de la mémoire, les problèmes liés aux privilèges des utilisateurs ou d'autres éventuels problèmes de sécurité. L'analyse dynamique met à profit des outils d'exécution pour vérifier si les fonctionnalités de sécurité s'exécutent comme prévu. Il existe un type d'analyse dynamique spécialisée, que l'on nomme également test à données aléatoires, qui provoque des défaillances de programme en introduisant délibérément des données mal formatées ou aléatoires dans les logiciels. Les tests à données aléatoires se fondent sur l'utilisation prévue des applications ainsi que sur les spécifications de fonctions et de conception des applications. Pour comprendre la portée des analyses de code dynamiques et, par conséquent, de l'assurance qu'elle fournit, les organisations peuvent également envisager de mener des analyses de couverture de code (vérification du degré auquel le code a été testé au moyen de mesures comme le pourcentage des sous-routines testées ou le pourcentage des instructions de programme appelés pendant l'exécution de la suite de tests), ou encore l'analyse de concordance (signalement des mots qui sont mal placés dans le code logiciel, notamment les termes dérogatoires ou les mots qui ne sont pas de l'anglais).

Références :

Aucune

SA-12 PROTECTION DE LA CHAÎNE D'APPROVISIONNEMENT

Contrôle :

(A) Les organisations assurent une protection contre les menaces à la chaîne d'approvisionnement qui visent les systèmes d'information, leurs composants ou les services connexes, au moyen de [*Affectation : mécanismes de sécurité définis par l'organisation*] dans le cadre d'une stratégie détaillée de défense intégrale de la sécurité de l'information.

Conseils supplémentaires : La politique ainsi que les procédures d'acquisition des systèmes et des services sont conformes aux lois du GC et aux politiques, directives et normes applicables du SCT. Les systèmes d'information (y compris leurs composants) doivent être protégés pendant la durée du cycle de développement des systèmes (CDS) (c.-à-d. durant la conception, le développement, la fabrication, le conditionnement, l'assemblage, la distribution, l'intégration au système, l'exploitation, la maintenance et la mise hors service). La protection des systèmes organisationnels d'information est assurée grâce à la sensibilisation aux menaces, à l'identification, la gestion et l'élimination des vulnérabilités propres à chaque phase du cycle de vie ainsi qu'au recours à des stratégies complémentaires et mutuellement renforçantes dans le but de réagit aux risques. Les organisations envisagent la mise en place d'un processus normalisé visant à répondre aux risques qui pèsent sur la chaîne d'approvisionnement – plus particulièrement en ce qui a trait aux systèmes d'information et aux composants des systèmes –, et à informer le personnel affecté aux acquisitions au sujet des menaces, des risques et des contrôles de sécurité à appliquer. Les organisations utilisent les processus d'acquisition/d'approvisionnement pour exiger de la part des entités de la chaîne d'approvisionnement qu'elles mettent en œuvre les mesures de sécurité qui permettront de (i) réduire la probabilité que surviennent des modifications non autorisées, et ce, à chacune des étapes de la chaîne d'approvisionnement; (ii) et de protéger les systèmes d'information et leurs composants préalablement à leur mise en service. Cette amélioration de contrôle s'applique également aux services des systèmes d'information. Les mesures de sécurité comprennent, par exemple, (i) les contrôles de sécurité pour les systèmes de développement, les installations de développement et les liens vers les systèmes de développement externes; (ii) les enquêtes concernant le personnel de développement; (iii) et l'utilisation d'un conditionnement inviolable pendant l'expédition ou l'entreposage. Les méthodes d'examen et de protection des plans de développement, les preuves et la documentation sont proportionnelles à la catégorie de sécurité ou au niveau de classification du système d'information visé. Les contrats peuvent également fournir des exigences concernant la protection des documents. Contrôles connexes : AT-3, CM-8, IR-4, PE-16, PL-8, SA-3, SA-4, SA-8, SA-10, SA-14, SA-15, SA-18, SA-19, SC-29, SC-30, SC-38, SI-7.

Améliorations du contrôle :

(1) PROTECTION DE LA CHAÎNE D'APPROVISIONNEMENT | STRATÉGIES D'ACQUISITION / OUTILS / MÉTHODES

L'organisation emploie [*Affectation : stratégies d'acquisition, outils de contrats et méthodes d'approvisionnement sur mesure définis par l'organisation*] pour l'achat des systèmes d'information, de leurs composants et des services connexes auprès des fournisseurs.

Conseils supplémentaires sur l'amélioration : Lorsqu'elles ont recours aux processus d'acquisition et d'approvisionnement dès les premiers stades du cycle de développement des systèmes, les organisations se dotent d'un important mécanisme de protection de la chaîne d'approvisionnement. Les organisations utilisent l'analyse de renseignement provenant de toute source dans le but d'optimiser la personnalisation des stratégies, des outils et des méthodes d'acquisition. Il existe une gamme d'outils et de techniques (p. ex. l'obscurcissement de l'usage terminal d'un système d'information ou de ses composants à l'aide d'achats voilés ou filtrés). Les organisations envisagent également de créer des incitatifs à l'intention des fournisseurs qui : (i) mettent en œuvre les mesures de sécurité requises; (ii) optent pour la transparence dans leurs processus organisationnels et leurs pratiques de sécurité; (iii) accroissent les mesures de contrôle des processus et pratiques de sécurité des fournisseurs sous-traitants, des composants des systèmes essentiels d'information et des services connexes; (iv) limitent les achats auprès de certains fournisseurs ou de certains pays; (v) et fournissent des libellés de contrats relativement à la prohibition de

composants altérés ou contrefaits. De plus, les organisations envisagent de réduire le temps s'écoulant entre la décision d'acheter et la date de livraison, de façon à limiter les occasions par lesquelles les parties adverses pourraient corrompre les composants ou les produits de systèmes d'information. Enfin, les organisations peuvent avoir recours aux options fiables de distribution, de livraison et d'entreposage dans le but d'atténuer les risques auxquels s'expose la chaîne d'approvisionnement (p. ex. exiger un conditionnement inviolable pour les composants de systèmes d'information pendant l'expédition ou l'entreposage). Contrôle connexe : SA-19.

(2) PROTECTION DE LA CHAÎNE D'APPROVISIONNEMENT | EXAMEN DES FOURNISSEURS

L'organisation procède à un examen des fournisseurs avant de conclure un contrat visant à acquérir des systèmes d'information, des composants de systèmes d'information ou des services connexes.

Conseils supplémentaires sur l'amélioration : L'examen des fournisseurs comprend, par exemple, (i) l'analyse des processus qu'un fournisseur utilise pour concevoir, développer, tester, implémenter, vérifier, livrer et soutenir les systèmes d'information, les composants de systèmes et les services connexes; (ii) et l'évaluation du niveau de formation et d'expérience du fournisseur en matière de développement de systèmes, de composants ou de services disposant des capacités de sécurité requises. Ces examens fournissent aux organisations un niveau accru de connaissance des activités que les fournisseurs mènent pendant le cycle de développement des systèmes, ce qui accroit l'efficacité de la gestion des risques liés à la chaîne d'approvisionnement. Les examens de fournisseurs permettent également d'établir si les fournisseurs primaires disposent de mesures de sécurité et s'ils sont aptes à contrôler les fournisseurs sous-traitants, par exemple, les fournisseurs de deuxième et de troisième ou tout autre type de sous-traitants.

(3) PROTECTION DE LA CHAÎNE D'APPROVISIONNEMENT | EXPÉDITION ET ENTREPOSAGE SÉCURISÉS

[Annulée : Intégrée au contrôle SA-12 (1)]

(4) PROTECTION DE LA CHAÎNE D'APPROVISIONNEMENT | DIVERSITÉ DES FOURNISSEURS

[Annulée : Intégrée au contrôle SA-12 (13)]

(5) PROTECTION DE LA CHAÎNE D'APPROVISIONNEMENT | LIMITATION DES DOMMAGES

L'organisation emploie [*Affectation : mesures de sécurité définies par l'organisation*] de façon à limiter les dommages pouvant être causés par d'éventuels adversaires qui pourraient identifier et cibler la chaîne d'approvisionnement organisationnelle.

Conseils supplémentaires sur l'amélioration : Les risques liés à la chaîne d'approvisionnement font partie de la menace persistante sophistiquée (APT pour *Advanced Persistent Threat*). Au nombre des mesures de protection et des contremesures de sécurité visant à réduire la probabilité que des adversaires parviennent à identifier et à cibler une chaîne d'approvisionnement, citons les suivantes : (i) éviter d'acheter des configurations personnalisées de façon à réduire les risques d'acquisition de systèmes d'information, de composants ou de produits ayant été corrompus par des interventions menées pendant le processus d'approvisionnement et visant certaines organisations; (ii) recourir à une diversité de fournisseurs dans le but de limiter les dommages éventuels pouvant être causés par l'un des fournisseur de la chaîne d'approvisionnement; (iii) employer une liste de fournisseurs autorisés qui jouissent d'une réputation durable dans l'industrie; (iv) et recourir à des mesures exceptionnelles en matière d'approvisionnement (p. ex. des exclusions par rapport aux engagements ou aux obligations).

(6) PROTECTION DE LA CHAÎNE D'APPROVISIONNEMENT | RÉDUCTION DU TEMPS D'APPROVISIONNEMENT

[Annulée : Intégrée au contrôle SA-12 (1)]

(7) PROTECTION DE LA CHAÎNE D'APPROVISIONNEMENT | ÉVALUATION PRÉALABLE À LA SÉLECTION / ACCEPTATION / MISE À JOUR

L'organisation procède à l'évaluation d'un système d'information, d'un composant du système ou d'un service connexe exécute préalablement à la sélection, à l'acceptation ou à la mise à jour.

Conseils supplémentaires sur l'amélioration : Les évaluations comprennent notamment les tests, les contrôles, les examens et les analyses. Une tierce partie indépendante ou le personnel organisationnel procède à l'évaluation des systèmes, des composants, des produits, des outils et des services. Les organisations procèdent à des évaluations visant à mettre au jour les vulnérabilités intentionnelles ou accidentelles, notamment le code malveillant, les processus malveillants, les logiciels défectueux ou la contrefaçon. Au nombre des évaluations, citons par exemple, les analyses statiques, les analyses dynamiques, les simulations, le test de la boîte blanche, de la boîte grise ou de la boîte noire, les tests à données aléatoires, les tests de pénétration, et la vérification de l'authenticité des composants ou des services (p. ex. recours aux étiquettes, aux vérifications de hachage cryptographiques ou aux signatures numériques). Les preuves cumulées pendant les évaluations de sécurité sont documentées de façon à ce que les organisations puissent procéder aux mesures consécutives. Contrôles connexes : CA-2, SA-11.

(8) PROTECTION DE LA CHAÎNE D'APPROVISIONNEMENT | UTILISATION DES RENSEIGNEMENTS PROVENANT DE TOUTES SOURCES

L'organisation utilise des analyses de renseignements provenant de toutes sources concernant les fournisseurs actuels ou éventuels de systèmes d'information, de composants de systèmes ou de services connexes.

Conseils supplémentaires sur l'amélioration : L'analyse de renseignements provenant de toutes sources est utilisée par les organisations dans le but d'éclairer les prises de décision en matière d'ingénierie, d'acquisition et de gestion des risques. Les renseignements provenant de toutes sources sont des produits de renseignements ou encore des organisations/des activités qui regroupent, à des fins de production de produits finis de renseignement, les sources d'information les plus courantes, à savoir le renseignement humain, le renseignement par imagerie, le renseignement de mesure et de signature, le renseignement électromagnétique ainsi que les données de source ouverte. Dès qu'elles sont disponibles, de telles informations sont utilisées pour analyser les risques de vulnérabilités intentionnelles ou accidentelles pouvant découler d'interventions humaines ou de processus pendant les étapes du développement, de la fabrication ou de l'expédition. Ces examens visent les fournisseurs à divers niveaux de la chaîne d'approvisionnement. Menés en nombre suffisants, ils ont pour objet d'assurer une gestion adéquate des risques. Contrôle connexe : SA-15.

(9) PROTECTION DE LA CHAÎNE D'APPROVISIONNEMENT | SÉCURITÉ DES OPÉRATIONS

L'organisation emploie [*Affectation : mesures de protection relatives à la sécurité des opérations (OPSEC pour Operations Security) définies par l'organisation*] conformément aux guides de classification, dans le but de protéger les informations de la chaîne d'approvisionnement qui ont trait aux systèmes d'information, aux composants de systèmes ou aux services connexes.

Conseils supplémentaires sur l'amélioration : Les informations de la chaîne d'approvisionnement comprennent notamment l'identité des utilisateurs; l'utilité des systèmes d'information; les composants des systèmes d'information et les services des systèmes d'information; l'identité des fournisseurs; les processus des fournisseurs, les exigences de sécurité; les spécifications de conception; les résultats de tests et d'évaluations; ainsi que les configurations de systèmes/de composants. Cette amélioration de contrôle étend la portée de l'OPSEC en incluant les fournisseurs actuels et éventuels. L'OPSEC est un processus permettant d'identifier l'information essentielle, puis d'analyser les actions amies accompagnant les opérations ou d'autres activités avec les visées suivantes : (i) identifier les actions pouvant être observées par d'éventuels adversaires; (ii) déterminer les indicateurs que les adversaires pourraient obtenir et mettre en perspective ou interpréter de façon à révéler des renseignements essentiels en assez de temps pour causer des dommages aux organisations; (iii) mettre en œuvre les mesures de protection et les contremesures visant à éliminer les vulnérabilités exploitables ou à les réduire à un niveau acceptable; (iv) et imaginer comment les amalgames d'informations pourraient compromettre la confidentialité des utilisateurs ou des intervenants de la chaînes d'approvisionnement. L'OPSEC peut exiger que les organisations soustraient de l'information (mission/opérations) aux fournisseurs, et peut inciter au recours à des intermédiaires dans le but de taire l'identité des utilisateurs ou les utilisations terminales des systèmes d'information, des composants de systèmes ou des services connexes. Contrôle connexe : PE-21.

(10) PROTECTION DE LA CHAÎNE D'APPROVISIONNEMENT | ATTESTATION DE L'AUTHENTICITÉ ET DE LA NON-ALTÉRITÉ

L'organisation emploie [*Affectation : mécanismes de sécurité définis par l'organisation*] pour attester qu'un système d'information ou un composant de système qui ont été livrés n'ont pas été altérés.

Conseils supplémentaires sur l'amélioration : Pour certains composants de systèmes d'information, particulièrement les dispositifs matériels, il y a des moyens techniques permettant d'établir si les composants sont authentiques ou s'ils ont été altérés. Les mécanismes de sécurité utilisés pour attester de l'authenticité des systèmes d'information et des composants de systèmes d'information sont, notamment, l'analyse optique, l'analyse par étiquetage nanotechnologique et l'analyse des canaux auxiliaires. Pour les composants matériels, une note détaillée d'information relative au matériel peut en révéler les éléments, leur logique interne, ainsi que leurs composants et leur lieu de production.

(11) PROTECTION DE LA CHAÎNE D'APPROVISIONNEMENT | TESTS DE PÉNÉTRATION / ANALYSE D'ÉLÉMENTS, DE PROCESSUS ET D'INTERVENANTS

L'organisation emploie [*Sélection (un ou plusieurs) : analyse organisationnelle, analyse d'une tierce partie indépendante, tests de pénétration par l'organisation, tests de pénétration par une tierce partie indépendante*] pour [*Affectation : éléments, processus et intervenants de la chaîne d'approvisionnement désignés par l'organisation*] associés aux systèmes d'information, aux composants de systèmes ou aux services connexes.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle ne porte pas seulement sur les éléments livrés, mais aussi sur les analyses et les tests relatifs à la chaîne d'approvisionnement. Les éléments de la chaîne d'approvisionnement sont des produits de technologie de l'information ou des composants de produits qui sont pourvus d'une logique programmable et qui s'avèrent considérablement importants pour les fonctions des systèmes d'information. Les processus liés à la chaîne d'approvisionnement sont, notamment, les suivant : (i) les processus de développement du matériel, des logiciels et des microgiciels; (ii) les procédures d'expédition et de manutention; (iii) les programmes de sécurité du personnel et de l'équipement; (iv) les outils/les mesures de gestion de configurations visant à contrôler la provenance; (v) les programmes, les processus ou les procédures liés à la production ou à la distribution des éléments de la chaîne d'approvisionnement. Les intervenants de la chaîne d'approvisionnement sont des personnes auxquelles on a attribué des responsabilités ou des rôles particuliers au sein de la chaîne d'approvisionnement. Les preuves générées par les analyses et les tests menés sur les éléments, les processus et les intervenants de la chaîne d'approvisionnement sont documentées et utilisées de façon à éclairer les prises de décision et les activités relatives à la gestion organisationnelle des risques. Contrôle connexe : RA-5.

(12) PROTECTION DE LA CHAÎNE D'APPROVISIONNEMENT | ENTENTES ENTRE LES ORGANISATIONS

De concert avec d'autres entités de la chaîne d'approvisionnement, l'organisation conclut des ententes et établit des procédures relatives aux systèmes d'information, aux composants de systèmes et aux services connexes.

Conseils supplémentaires sur l'amélioration : L'établissement d'ententes interorganisationnelles et de procédures communes permet de signaler la compromission des chaînes d'approvisionnement. Le signalement précoce des compromissions (de la chaîne d'approvisionnement) pouvant nuire ou ayant pu nuire aux systèmes d'information organisationnels, y compris aux composants des systèmes, est essentiel aux organisations qui souhaitent réagir aux incidents en temps opportun et adéquatement.

(13) PROTECTION DE LA CHAÎNE D'APPROVISIONNEMENT | COMPOSANTS DE SYSTÈME D'INFORMATION ESSENTIELS

L'organisation emploie [*Affectation : mécanismes de sécurité définis par l'organisation*] pour assurer un approvisionnement adéquat des [*Affectation : composant de systèmes essentiels d'information désignés par l'organisation*].

Conseils supplémentaires sur l'amélioration : Des adversaires pourraient tenter de contrecarrer les opérations organisationnelles en entravant l'approvisionnement de composants essentiels des systèmes d'information ou en interférant avec les opérations des fournisseurs. Au nombre des mesures de protection visant à assurer l'approvisionnement adéquat des composant essentiels des systèmes d'information, citons en exemple les suivants : (i) le recours à de multiples fournisseurs répartis dans l'ensemble de la chaîne d'approvisionnement pour ce qui a trait à certains composants essentiels; (ii) la conservation d'un certain

nombre de composants de rechange pour assurer la continuité des opérations en période de mission critique.

(14) PROTECTION DE LA CHAÎNE D'APPROVISIONNEMENT | IDENTITÉ ET TRAÇABILITÉ

L'organisation établit et retient un seul identifiant pour [*Affectation : éléments de la chaîne d'approvisionnement, processus et intervenants désignés par l'organisation*] relativement aux systèmes d'information, aux composants des systèmes et aux services connexes.

Conseils supplémentaires sur l'amélioration : Il est essentiel d'être au fait des éléments et des intervenants qui font partie de la chaîne d'approvisionnement organisationnelles, si l'on souhaite maintenir un vue d'ensemble des activités et de leur nature, tout en surveillant et en identifiant les événements ainsi que les activités comportant un niveau élevé de risque. Sans cette vue d'ensemble et sans la traçabilité des constituants d'une chaîne d'approvisionnement (p. ex. les éléments, les processus et les intervenants), il est passablement difficile pour les organisations de comprendre et, par conséquent, de gérer les risques et de réduire la probabilité d'occurrence des événements préjudiciables. Il importe donc d'attribuer un identifiant unique aux rôles d'acquéreur et d'intégrateur de même qu'aux organisations, au personnel, aux missions et processus liés aux éléments, aux procédures de test et d'évaluation, aux mécanismes de livraison, aux mécanismes de soutien, aux lignes d'acheminement et de communications, aux activités de mise hors service ou d'élimination, ainsi qu'aux composants et aux outils pour être en mesure de jeter les bases d'une structure d'identification à des fins d'évaluation de la chaîne d'approvisionnement. Par exemple, grâce aux vignettes (numéros de série) et à l'étiquetage à des fins d'identification par radiofréquences [RFID]), chacun des éléments d'une chaîne d'approvisionnement (progiciels, modules et dispositifs matériels) ainsi que les processus qui leur sont associés peuvent servir à constituer cette base. Les méthodes d'identification sont suffisantes pour indiquer la provenance, advenant un problème ou un événement préjudiciable visant la chaîne d'approvisionnement.

(15) PROTECTION DE LA CHAÎNE D'APPROVISIONNEMENT | PROCESSUS VISANT À RÉAGIR AUX FAIBLESSES ET AUX LACUNES

Pour ce qui a trait aux chaînes d'approvisionnement, l'organisation établit des processus permettant de réagir aux faiblesses et aux lacunes signalées pendant les évaluations menées par l'organisation ou par des entités indépendantes.

Conseils supplémentaires sur l'amélioration : Les preuves produites par les évaluations internes ou indépendantes des éléments d'une chaîne d'approvisionnement (p. ex. tests de pénétration, audits, vérifications et activités de validation) sont documentées et utilisées dans les processus subséquents mis en place par les organisations dans le but de répondre aux risques mis en évidence par le signalement des faiblesses ou des lacunes. Au nombre des éléments d'une chaîne d'approvisionnement, citons notamment les processus de développement des fournisseurs et les systèmes de distribution de ces mêmes fournisseurs.

Références :

CST, TSCG-01\G, *Clauses contractuelles liées à l'équipement et aux services de télécommunication* [Référence 72].

SA-13 FIABILITÉ

[Non attribué dans les profiles du GC. Pour le CST, toutefois, le terme « robustesse » (*robustness*) renvoi à une notion similaire à celle que la National Institute of Standards and Technology désigne par le terme « fiabilité » (*trustworthiness*). Le chapitre 7 de l'*ITSG-33, Annexe 2 – Activités de gestion des risques liés à la sécurité des systèmes d'information* [Référence 58] considère la robustesse comme un attribut intégré dans le processus d'application de la sécurité dans les systèmes d'information (PASSI).]

SA-14 ANALYSE DE CRITICITÉ

Contrôle :

(A) L'organisation identifie les composants et les fonctions des systèmes d'information en procédant à une analyse de criticité de [*Affectation : systèmes d'information, composants de systèmes d'information ou services connexes*] à [*Affectation : points de décision du cycle de développement des systèmes définis par l'organisation*].

Conseils supplémentaires : L'analyse de criticité est un principe clé en gestion des chaînes d'approvisionnement, puisqu'elle permet d'optimiser la priorisation des activités de protection d'une chaîne d'approvisionnement, notamment la réduction de la surface d'attaque, l'utilisation des renseignements provenant de toutes sources et la personnalisation des stratégies d'acquisition. Les spécialistes des systèmes d'information peuvent procéder à une décomposition fonctionnelle de l'intégralité d'un système d'information dans le but d'identifier les fonctions et les composants essentiels aux missions. La décomposition fonctionnelle comprend l'identification des missions centrales d'une organisation qui jouissent du soutien des systèmes, la décomposition du tout en fonctions particulières qui servent à l'exercice des missions, ainsi que la traçabilité vers les composants matériels, logiciels et microgiciels qui servent à mettre les fonctions en œuvre, et ce, même lorsque ces fonctions sont partagées par de multiples composants pouvant se trouver à l'extérieur comme à l'intérieur du système d'information. Les composants de systèmes d'information qui permettent un accès direct aux fonctions ou composants essentiels sont considérés comme essentiels en raison de la vulnérabilité qu'ils engendrent. La criticité est évaluée en fonction de l'impact des défaillances des fonctions ou des composants sur la capacité de ces derniers à exécuter comme prévu les missions organisationnelles qui jouissent du soutien des systèmes d'information. Une analyse de criticité est menée dès lorsqu'une architecture ou la conception est en cours de développement, de modification ou de mise à jour/à niveau. Contrôles connexes : CP-2, PL-2, PL-8, SA-8, SA-12, SA-13, SA-15, SA-20.

Références :

Aucune

SA-15 PROCESSUS DE DÉVELOPPEMENT, NORMES ET OUTILS

Contrôle :

(A) L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe suive un processus de développement documenté qui permette ce qui suit :

(a) répondre explicitement aux exigences de sécurité;

(b) identifier les normes et les outils devant servir au processus de développement;

(c) documenter les options et configurations particulières aux outils utilisés dans le processus de développement;

(d) documenter, gérer et garantir l'intégrité des changements apportés aux processus ou aux outils servant au développement.

(B) L'organisation examine les processus, les normes et les outils ainsi que les options/la configuration des outils liés au développement [*Affectation : fréquence définie par l'organisation*] dans le but d'établir si les processus, les normes, les outils et les options/la configuration des outils employés peuvent répondre à [*Affectation : exigences de sécurité définies par l'organisation*].

Conseils supplémentaires : Les outils de développement comprennent notamment les langages de programmation et les systèmes de conception assistée par ordinateur (CAD pour *Computer-Aided Design*).

L'examen des processus de développement peut inclure, par exemple, l'utilisation de modèles d'évolution dans le but de définir l'efficacité potentielle desdits processus. Le maintien de l'intégrité des changements apportés aux outils ou aux processus permet d'exercer une évaluation ainsi qu'une atténuation juste et adéquate des risques liés à la chaîne d'approvisionnement, mais elle nécessite aussi un contrôle robuste des configurations pendant la durée du cycle de développement des systèmes (nommément la conception, le développement, le transport, la livraison, l'intégration et la maintenance) de façon à faire un suivi des changements autorisés et à prévenir les changements non autorisés. Contrôles connexes : SA-3, SA-8.

Améliorations du contrôle :

(1) PROCESSUS DE DÉVELOPPEMENT, NORMES ET OUTILS | MESURE DE LA QUALITÉ

(a) L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe définisse les paramètres de mesure de la qualité dès le commencement du processus de développement.

(b) L'organisation exige que le développeur d'un système d'information, d'un composant du système d'information ou d'un service connexe fournisse des preuves que les critères de qualité sont respectés à [*Sélection (une ou plusieurs)* : [*Affectation : fréquence définie par l'organisation*]; [*Affectation : échéancier d'examen de programmes défini par l'organisation*]; *au moment de la mise en service*].

Conseils supplémentaires sur l'amélioration : Les organisations ont recours à des paramètres de mesure de la qualité pour établir les niveaux minimums acceptables de qualité des systèmes d'information. Ces paramètres peuvent comprendre des jalons de qualité, qui représentent un ensemble critères d'accomplissement ou de normes de suffisance qui définissent l'exécution adéquate des diverses phases du projet de développement des systèmes. Un jalon de qualité, par exemple, pourrait exiger l'élimination de tous les avertissements de compilateurs ou établir explicitement que les avertissements n'ont aucune incidence sur l'efficacité des capacités de sécurité requises. Pendant l'exécution des phases des projets de développement, les jalons de qualité s'avèrent des indicateurs de progression clairs et précis. D'autres paramètres de mesure s'appliquent à l'intégralité du projet de développement. Les mesures de qualité peuvent également inclure la définition des seuils de sévérité des vulnérabilités, par exemple, le fait d'exiger l'élimination de toute vulnérabilité connue des systèmes d'information mis en service et la définition des niveaux de sévérité « moyen » et « élevé » du *Common Vulnerability Scoring System* (CVSS).

(2) PROCESSUS DE DÉVELOPPEMENT, NORMES ET OUTILS | OUTILS DE SUIVI DE LA SÉCURITÉ

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe sélectionne et emploie un outil de suivi de la sécurité pendant le processus de développement.

Conseils supplémentaires sur l'amélioration : Les équipes de développement de systèmes d'information sélectionnent et déploient des outils de suivi de la sécurité, notamment des systèmes de suivi de la vulnérabilité/des éléments de travail visant à faciliter l'attribution, le triage, le filtrage et le suivi des éléments de travail accomplis ou des tâches associées aux processus de développement des systèmes.

(3) PROCESSUS DE DÉVELOPPEMENT, NORMES ET OUTILS | ANALYSE DE CRITICITÉ

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe exécute une analyse de criticité à [*Affectation : étendue/profondeur définies par l'organisation*] et à [*Affectation : points de décision du cycle de développement des systèmes définis par l'organisation*].

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle fournit de l'information issue des développeurs et pouvant servir aux analyses de criticité menées par les organisations conformément à SA-14. L'apport des développeurs est essentielle dans une telle analyse, puisque les organisations pourraient ne pas avoir accès à une documentation de conception détaillée concernant les composants des systèmes d'information qui sont développés en tant que produits de technologie de l'information destinés au marché commercial (p. ex. spécifications fonctionnelles, conception de haut niveau, conception de bas niveau, et code source/schémas d'éléments matériels). Contrôles connexes : SA-4, SA-14.

(4) PROCESSUS DE DÉVELOPPEMENT, NORMES ET OUTILS | MODÉLISATION DES MENACES / ANALYSE DES VULNÉRABILITÉS

L'organisation exige que les développeurs se chargent de la modélisation des menaces et de l'analyse des vulnérabilités relativement aux systèmes d'information à [*Affectation : étendue/profondeur définies par l'organisation*] et de façon à répondre aux critères suivants :

(a) utiliser [*Affectation : information au sujet des impacts définies par l'organisation, environnement opérationnel, menaces connues ou présumées, et niveaux acceptables de risque*];

(b) employer [*Affectation : méthodes et outils désignés par l'organisation*];

(c) produire des preuves de conformité à [*Affectation : critères d'acceptation définis par l'organisation*].

Conseils supplémentaires sur l'amélioration – Contrôle connexe : SA-4.

(5) PROCESSUS DE DÉVELOPPEMENT, NORMES ET OUTILS | RÉDUCTION DE LA SURFACE D'ATTAQUE

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe réduise la surface d'attaque à [*Affectation : seuils définis par l'organisation*].

Conseils supplémentaires sur l'amélioration : La réduction de la surface d'attaque s'aligne étroitement sur les analyses de menaces et de vulnérabilité menées par le développeur ainsi que sur l'architecture et la conception des systèmes d'information. La réduction de la surface d'attaque constitue un moyen de réduire les risques encourus par les organisations en limitant considérablement les occasions d'exploiter les faiblesses et les lacunes (p. ex. les vulnérabilités potentielles) inhérentes aux systèmes d'information, aux composants des systèmes d'information et aux services connexes. La réduction de la surface d'attaque implique l'application du principe du droit d'accès minimal en employant des défenses par couches, l'application du principe de la fonctionnalité minimale (p. ex. les contraintes au niveau des ports, des protocoles, des fonctions et des services), la proscription des fonctions risquées et l'élimination des interfaces de programme d'application (API pour *Application Programming Interfaces*) qui sont vulnérables aux attaques. Contrôle connexe : CM-7.

(6) PROCESSUS DE DÉVELOPPEMENT, NORMES ET OUTILS | AMÉLIORATION CONTINUE

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe mette en œuvre un processus détaillé visant expressément à améliorer continuellement le processus de développement.

Conseils supplémentaires sur l'amélioration : Les développeurs de systèmes d'information, de composants de systèmes d'information et de services connexes évaluent l'efficacité/l'efficience des processus de développement en place pour faire en sorte qu'ils répondent toujours mieux aux objectifs de qualité et qu'ils soient dotés des capacités de sécurité requises compte tenu des environnements de menaces.

(7) PROCESSUS DE DÉVELOPPEMENT, NORMES ET OUTILS | ANALYSES AUTOMATISÉE DES VULNÉRABILITÉS

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe exécute ce qui suit :

(a) réaliser une analyse des vulnérabilités au moyen de [*Affectation : outils désignés par l'organisation*];

(b) définir les possibilités d'exploitation des vulnérabilités signalées;

(c) définir les mesures d'atténuation des risques liés aux vulnérabilités décelées;

(d) fournir les données produites par les outils ainsi que les résultats des analyses auprès de [*Affectation : personnel ou rôles définis par l'organisation*].

Conseils supplémentaires sur l'amélioration – Contrôle connexe : RA-5.

(8) PROCESSUS DE DÉVELOPPEMENT, NORMES ET OUTILS | RÉUTILISATION DES INFORMATIONS SUR LES MENACES / VULNÉRABILITÉS

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe examine des modélisations de menaces et des analyses des vulnérabilités exécutées sur des systèmes, des composants ou des services semblables, de façon à orienter le processus de développement en cours.

Conseils supplémentaires sur l'amélioration : Les analyses de vulnérabilités menées sur des applications logicielles semblables peuvent donner de précieux renseignements permettant de résoudre d'éventuels problèmes de conception ou de mise en œuvre dans les systèmes d'information en cours de développement. Des systèmes d'information ou des composants de systèmes semblables pourraient exister au sein des organisations de développement. De l'information faisant autorité en matière de de vulnérabilité est disponible auprès d'une diversité de sources des secteurs privé et public, notamment la National Vulnerability Database.

(9) PROCESSUS DE DÉVELOPPEMENT, NORMES ET OUTILS | UTILISATION DE DONNÉES EN DIRECT

L'organisation approuve, documente et contrôle l'utilisation de données en direct dans les environnements de développement et de test utilisés pour les systèmes d'information, les composants de systèmes ou les services connexes.

Conseils supplémentaires sur l'amélioration : L'utilisation de données en direct dans les environnements de préproduction peut comporter des risques considérables pour les organisations. Les organisations peuvent réduire les risques au minimum en utilisant de fausses données pendant les activités de développement et de test menées sur les systèmes d'information, sur les composants de systèmes d'information ou sur les services connexes.

(10) PROCESSUS DE DÉVEOLOPPEMENT, NORMES ET OUTILS | PLAN D'INTERVENTION EN CAS D'INCIDENT

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe produise un plan d'intervention en cas d'incident.

Conseils supplémentaires sur l'amélioration : Le plan d'intervention en cas d'incident à l'intention des développeurs des systèmes d'information, des composants de systèmes et des services connexes est intégré aux plans organisationnels d'intervention en cas d'incident, dans le but de fournir un type d'information pertinente qui n'est souvent pas aisément accessible aux organisations. Une telle information peut s'avérer extrêmement utile, par exemple, lorsque les organisations réagissent aux vulnérabilités décelées dans les produits commerciaux de technologie de l'information. Contrôle connexe : IR-8.

(11) PROCESSUS DE DÉVELOPPEMENT, NORMES ET OUTILS | SYSTÈME D'ARCHIVAGE D'INFORMATION / COMPOSANT

L'organisation exige que le développeur d'un système d'information ou d'un composant du système archive le système ou le composant à mettre en service en compagnie des preuves correspondantes qui visent à appuyer l'examen de sécurité définitif.

Conseils supplémentaires sur l'amélioration : L'archivage de la documentation relative au processus de développement comporte l'avantage de fournir une base d'information facilement accessible qui pourrait s'avérer utile pendant la mise à jour/à niveau ou la modification des systèmes d'information/des composants de systèmes.

Références :

Aucune

SA-16 FORMATION OFFERTE PAR LE DÉVELOPPEUR

Contrôle :

(A) L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe fournisse [*Affectation : formation définie par l'organisme*] portant sur l'utilisation et l'exploitation adéquates des fonctions, des contrôles et des mécanismes de sécurité mis en œuvre.

Conseils supplémentaires : Ce contrôle concerne les développeurs externes et internes (de l'organisation en question). La formation du personnel est un élément essentiel qui permet d'optimiser l'efficacité des contrôles de sécurité mis en œuvre au sein des systèmes organisationnels d'information. Les options de formation comprennent, notamment, la formation en classe, la formation en ligne ou assistée par ordinateur, ainsi que la formation pratique. Les organisations peuvent également demander, auprès des développeurs, du matériel de formation en quantités suffisantes pour offrir des options de formation en interne ou d'auto-formation à leurs personnels respectifs. Les organisations établissent le type de formation qui répond à leurs besoins et peuvent demander divers types de formation selon les fonctions, les contrôles ou les mécanismes de sécurité visés. Contrôles connexes : AT-2, AT-3, SA-5.

Améliorations du contrôle :

Aucune

Références :

Aucune

SA-17 ARCHITECTURE ET CONCEPTION DE SÉCURITÉ DU DÉVELOPPEUR

Contrôle :

(A) L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe produise des spécifications de conception et une architecture de sécurité qui s'alignent sur l'architecture de sécurité organisationnelle, laquelle est partie intégrante de l'architecture d'entreprise de l'organisation.

(B) L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe produise des spécifications de conception et une architecture de sécurité qui décrivent intégralement et précisément les fonctionnalités de sécurité requises ainsi que l'attribution des contrôles de sécurité parmi les composants physiques et logiques.

(C) L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe produise des spécifications de conception et une architecture de sécurité qui exposent comment les fonctions de sécurité, les mécanismes et les services fonctionnent ensemble pour fournir les capacités de sécurité requises et favoriser une approche coordonnée en matière de protection.

Conseils supplémentaires : La présente amélioration s'adresse principalement aux développeurs externes, bien qu'elle puisse tout autant être pertinente au développement en interne. En revanche, le PL-8 concerne d'abord les développeurs internes de façon à ce que les organisations puissent développer une architecture de sécurité et veiller à l'intégration de celle-ci à l'architecture d'entreprise. Il importe de faire cette distinction lorsque les organisations externalisent le développement de systèmes d'information, de composants de systèmes d'information ou de services connexes, et qu'il est nécessaire qu'il y ait correspondance avec l'architecture d'entreprise ou avec l'architecture de sécurité de l'information d'une organisation. Contrôles connexes : PL-8, SA-3, SA-8.

Améliorations du contrôle :

(1) ARCHITECTURE ET CONCEPTION DE SÉCURITÉ DU DÉVELOPPEUR | MODÈLE FORMEL DE POLITIQUE

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe exécute ce qui suit :

(a) produire, en parfaite intégration avec le processus de développement, un modèle formel de politique décrivant [*Affectation : éléments de politique organisationnelle de sécurité définis par l'organisme*] à mettre en œuvre;

(b) démontrer que le modèle formel de politique est cohérent et suffisant pour appliquer les dispositions de la politique organisationnelle de sécurité dès lors que celle-ci est en vigueur.

Conseils supplémentaires sur l'amélioration : Les modèles formels expriment des comportements particuliers ou des politiques de sécurité en langage formel, ce qui permet de prouver l'adéquation de ces comportements/de ces politiques de façon formelle. Or, tous les composants de systèmes d'information ne peuvent pas forcément être modélisés et généralement, les spécifications formelles concernent des politiques ou comportements particuliers qui revêtent un certain intérêt (p. ex. politiques de contrôle non discrétionnaire des accès). Pour ce qui est du modèle formel de politique, les organisations choisissent un langage et une approche en se fondant sur la nature des politiques/des comportements devant être décrits et sur les outils disponibles. Les outils de modélisation formelle comprennent notamment Gypsy et Zed.

(2) ARCHITECTURE ET CONCEPTION DE SÉCURITÉ DU DÉVELOPPEUR | COMPOSANTS LIÉS À LA SÉCURITÉ

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe exécute ce qui suit :

(a) définir le matériel, les logiciels et les microgiciels devant servir à la sécurité;

(b) fournir un argumentaire démontrant que la définition du matériel, des logiciels et des microgiciels est complète.

Conseils supplémentaires sur l'amélioration : Dans un système d'information, un composant de système ou un service connexe, le matériel, les logiciels et les microgiciels servant à la sécurité forment la partie dont le fonctionnement adéquat sera garant des propriétés de sécurité qui sont exigées. Contrôle connexe : SA-5.

(3) ARCHITECTURE ET CONCEPTION DE SÉCURITÉ DU DÉVELOPPEUR | CORRESPONDANCE FORMELLE

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe exécute ce qui suit :

(a) produire, en parfaite intégration avec le processus de développement, des spécifications formelles de haut niveau qui décrivent les interfaces du matériel, des logiciels et des microgiciels servant à la sécurité sur le plan des exceptions, des messages d'erreur et des effets;

(b) montrer – par des preuves accessibles et, s'il y a lieu, par des démonstrations informelles – que les spécifications de haut niveau sont conformes au modèle formel de politique;

(c) montrer, par des démonstrations informelles, que les spécifications formelles de haut niveau prennent en compte toutes les interfaces du matériel, des logiciels et des microgiciels servant à la sécurité;

(d) montrer que les spécifications formelles de haut niveau décrivent précisément le matériel, les logiciels et les microgiciels utilisés à des fins de sécurité;

(e) décrire les mécanismes liés au matériel, aux logiciels et aux microgiciels servant à la sécurité qui ne sont pas explicitement pris en compte dans les spécifications formelles de haut niveau, mais qui sont inhérents à ce matériel, à ces logiciels et à ces microgiciels servant à la sécurité.

Conseils supplémentaires sur l'amélioration : La correspondance est un élément important de l'assurance gagnée en cours de modélisation. Elle démontre que la mise en œuvre constitue une transformation précise du modèle, et que tout code ou détail de mise en œuvre additionnel n'aura aucun impact sur les comportements ou sur les politiques en cours de modélisation. Les méthodes formelles peuvent être utilisées pour montrer que la description formelle d'un système d'information est conforme aux propriétés de sécurité de haut niveau, et que la description formelle de système est adéquatement mise en œuvre, et ce, par la description d'un niveau inférieur, notamment la description des composants matériels. La cohérence entre les spécifications formelles de haut niveau et les modèles formels de politiques est généralement impossible à prouver hors de tout doute. Par conséquent, une combinaison de méthodes formelles et informelles pourrait être requise pour démontrer la cohérence. La cohérence entre les spécifications de haut niveau et la mise en œuvre pourraient nécessiter l'utilisation de démonstrations informelles en raison des contraintes liées à l'applicabilité des méthodes formelles dans le but de prouver que les spécifications sont intégralement conformes à la mise en œuvre. Les mécanismes liés au matériel, aux logiciels et aux microgiciels, qui sont strictement inhérents au matériel, aux logiciels et aux microgiciels, comprennent notamment les registres de mappage et les entrées/sorties directes liées à la mémoire. Contrôle connexe : SA-5.

(4) ARCHITECTURE ET CONCEPTION DE SÉCURITÉ DU DÉVELOPPEUR | CORRESPONDANCE INFORMELLE

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe exécute ce qui suit :

(a) produire, en parfaite intégration avec le processus de développement, des spécifications informelles de haut niveau qui décrivent les interfaces du matériel, des logiciels et des microgiciels servant à la sécurité sur le plan des exceptions, des messages d'erreur et des effets;

(b) montrer par [*Sélection : démonstration informelle, arguments convaincants fournis, si possible, par des méthodes formelles*] que les spécifications descriptives de haut niveau sont conformes au modèle formel de politique;

(c) montrer, par des démonstrations informelles, que les spécifications descriptives de haut niveau prennent en compte toutes les interfaces du matériel, des logiciels et des microgiciels servant à la sécurité;

(d) montrer que les spécifications descriptives de haut niveau décrivent précisément les interfaces du matériel, des logiciels et des microgiciels servant à la sécurité;

(e) décrire les mécanismes liés au matériel, aux logiciels et aux microgiciels servant à la sécurité qui ne sont pas explicitement pris en compte dans les spécifications descriptives de haut niveau, mais qui sont strictement inhérents à ce matériel, à ces logiciels et à ces microgiciels servant à la sécurité.

Conseils supplémentaires sur l'amélioration : La correspondance est un élément important de l'assurance gagnée en cours de modélisation. Elle démontre que la mise en œuvre constitue une transformation précise du modèle, et que tout code ou détail de mise en œuvre additionnel n'aura aucun impact sur les comportements ou sur les politiques en cours de modélisation. La cohérence entre les spécifications descriptives de haut niveau (p. ex. conception de haut niveau/de bas niveau) et le modèle formel de politique est généralement impossible à prouver hors de tout doute. Par conséquent, une combinaison de méthodes formelles et informelles pourrait être requise pour démontrer la cohérence. Les mécanismes liés au matériel, aux logiciels et aux microgiciels, qui sont strictement inhérents au matériel, aux logiciels et aux microgiciels comprennent notamment les registres de mappage et les entrées/sorties directes liées à la mémoire. Contrôle connexe : SA-5.

(5) ARCHITECTURE ET CONCEPTION DE SÉCURITÉ DU DÉVELOPPEUR | CONCEPTION SIMPLE SUR LE PLAN CONCEPTUEL

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe exécute ce qui suit :

(a) concevoir et structurer le matériel, les logiciels et les microgiciels servant à la sécurité de façon à créer un mécanisme de protection complet et conceptuellement simple doté d'une sémantique précisément définie;

(b) structurer en interne le matériel, les logiciels et les microgiciels servant à la sécurité, en portant une attention particulière au mécanisme en question.

Conseils supplémentaires sur l'amélioration : Contrôle connexe : SC-3.

(6) ARCHITECTURE ET CONCEPTION DE SÉCURITÉ DU DÉVELOPPEUR | STRUCTURE DE TESTS

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe structure le matériel, les logiciels et les microgiciels servant à la sécurité de façon à faciliter l'exécution des tests.

Conseils supplémentaires sur l'amélioration – Contrôle connexe : SA-11.

(7) ARCHITECTURE ET CONCEPTION DE SÉCURITÉ DU DÉVELOPPEUR | STRUCTURE RELATIVE AU DROIT D'ACCÈS MINIMAL

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe structure le matériel, les logiciels et les microgiciels servant à la sécurité de façon à faciliter le contrôle des accès dotés de privilèges minimaux.

Conseils supplémentaires sur l'amélioration – Contrôles connexes : AC-5, AC-6**.**

Références :

Aucune

SA-18 RÉSISTANCE AU TRAFIQUAGE ET DÉTECTION

Contrôle :

(A) L'organisation met en œuvre un programme de protection contre le trafiquage à l'avantage des systèmes d'information, des composants de systèmes et des services connexes.

Conseils supplémentaires : Les technologies et techniques antitrafiquage fournissent un niveau de protection des systèmes d'information, des composants de systèmes et des produits de technologie de l'information essentiels contre un certain nombre de menaces, notamment la modification, la rétroingénierie et la substitution. Les modalités robustes d'identification combinées aux moyens permettant de contrer et de détecter le trafiquage sont essentielles, lorsqu'il s'agit d'assurer la protection des systèmes, des composants et des produits d'information pendant la distribution et l'utilisation. Contrôles connexes : PE-3, SA-12, SI-7.

Améliorations du contrôle :

(1) RÉSISTANCE AU TRAFIQUAGE ET DÉTECTION | MULTIPLES PHASES DU CDS

L'organisation emploie des technologies et techniques antitrafiquage pendant plusieurs des phases du cycle de développement des systèmes, notamment la conception, le développement, l'intégration, l'exploitation et la maintenance.

Conseils supplémentaires sur l'amélioration : Les organisations utilisent une combinaison de dispositifs matériels et logiciels pour contrer et détecter le trafiquage. Les organisations ont recours à l'obscurcissement à aux autovérifications, notamment pour rendre la rétroingénierie et les modifications difficiles, chronophages et onéreuses pour les adversaires. Au demeurant, la personnalisation des systèmes d'information et des composants peut rendre les substitutions plus faciles à détecter, ce qui permet de limiter les dommages. Contrôle connexe : SA-3.

(2) RÉSISTANCE AU TRAFIQUAGE ET DÉTECTION | INSPECTION DES SYSTÈMES D'INFORMATION, DES COMPOSANTS OU DES DISPOSITIFS

Les organisations inspectent [*Affectation : systèmes d'information, composants de systèmes ou dispositifs*] [Sélection (une ou plusieurs) : au hasard; au [*Affectation : fréquence définie par l'organisation*], lorsque [*Affectation : indications concernant le besoin de mener une inspection définies par l'organisme*]] dans le but de détecter le trafiquage.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle permet de s'attaquer au trafiquage physique et logique, et est généralement utilisé pour les dispositifs mobiles, les ordinateurs portables ou les composants de systèmes qui ont été sortis des secteurs contrôlés par l'organisation. Une inspection pourrait être requise, par exemple, lorsque des individus reviennent d'un voyage effectué dans des régions à haut risque. Contrôle connexe : SI-4.

Références :

Aucune

SA-19 AUTHENTICITÉ DES COMPOSANTS

Contrôle :

(A) L'organisation développe et met en œuvre une politique ainsi que des procédures qui visent à combattre la contrefaçon et qui prévoient la mise en place de mesures visant à détecter et à prévenir l'entrée de dispositifs contrefaits dans les systèmes d'information.

(B) L'organisation signale les composants de systèmes d'information qui ont été contrefaits à [*Sélection (une ou plusieurs) : source de composant contrefait*; [*Affectation : organismes rapporteurs externes désignés par l'organisation*]; [*Affectation : personnel ou rôle désigné par l'organisation*]].

Conseils supplémentaires : Les sources de composants contrefaits pourraient être, par exemple, les fabricants, les développeurs, les fournisseurs et les entrepreneurs. Les politiques et procédures visant à combattre la contrefaçon renforcent la résistance au trafiquage et fournissent un niveau de protection contre l'introduction de code malveillant. Parmi les organismes rapporteurs externes, pensons aux CERTS. Contrôles connexes : PE-3, SA-12, SI-7.

Améliorations du contrôle :

(1) AUTHENTICITÉ DES COMPOSANTS | BALAYAGE ANTICONTREFAÇON

L'organisation forme [*Affectation : personnel ou rôle désignés par l'organisation*] dans le domaine de la détection des composants contrefaits de systèmes d'information (y compris les composants matériels, logiciels et microgiciels).

(2) AUTHENTICITÉ DES COMPOSANTS | CONTRÔLE DES CONFIGURATIONS POUR L'ENTRETIEN ET LA RÉPARTION DES COMPOSANTS

L'organisation se réserve le contrôle des configurations pour [*Affectation : composants de systèmes d'information désignés par l'organisation*] appelés à subir un entretien ou une réparation ainsi que des composants réparés ou entretenus qui sont appelés à retourner à leur lieu de service.

(3) AUTHENTICITÉ DES COMPOSANTS | MISE HORS SERVICE DES COMPOSANTS

Les organisations mettent les composants de systèmes d'information hors service au moyen de [*Affectation : techniques et méthodes définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : La mise hors service adéquate des composants de systèmes d'information aide à empêcher que les composants en question ne soient introduits dans le marché semi-clandestin (marché gris).

(4) AUTHENTICITÉ DES COMPOSANTS | FORMATION À L'ANTICONTREFAÇON

L'organisation effectue un balayage visant à détecter les composants contrefaits de systèmes d'information [*Affectation : fréquence définie par l'organisation*].

Références :

CST, TSCG-01\G, *Clauses contractuelles liées à l'équipement et aux services de télécommunication* [Référence 72].

SA-20 DÉVELOPPEMENT SUR MESURE DES COMPOSANTS ESSENTIELS

Contrôle :

(A) L'organisation remet en œuvre ou développe sur mesure [*Affectation : composants essentiels de systèmes d'information désignés par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les organisations établissent que certains composants de systèmes d'information ne peuvent vraisemblablement pas être considérés comme fiables en raison de certaines menaces ou de vulnérabilités inhérentes, et que ces mêmes composants ne disposent pas de contrôles de sécurité aptes à atténuer raisonnablement les risques résiduels. La remise en œuvre ou le développement sur mesure de tels composants peut permettre à ces derniers de répondre à des niveaux d'assurances supérieurs. Cette amélioration s'accomplit en apportant des changements aux composants de systèmes (matériel, logiciel et microgiciel) pour faire en sorte que les attaques courantes des adversaires aient peu de chances de réussir. Dans les situations où il n'y a pas d'autres options de sourçage et les organisations choisissent de ne pas remettre en œuvre ou de ne pas personnaliser les composants essentiels de systèmes, des mesures de protection additionnelles peuvent être employées (p. ex. audit approfondies, restrictions concernant l'accès au code source et aux auxiliaires de systèmes, ainsi que la protection contre les suppressions de fichiers et d'applications de système). Contrôles connexes : CP-2, SA-8, SA-14.

Améliorations du contrôle :

Aucune

Références :

Aucune

SA-21 SÉLECTION DES DÉVELOPPEURS

Contrôle :

(A) L'organisation exige que le développeur de [*Affectation : systèmes d'information, composants de système ou services connexes*] dispose des autorisations d'accès requises en fonction des [*Affectation : responsabilités gouvernementales officielles définies par l'organisation*] qui ont été attribuées.

(B) L'organisation exige que le développeur de [*Affectation : systèmes d'information, composants de système ou services connexes*] satisfasse à [*Affectation : critères additionnels de sélection de personnel définis par l'organisation*].

Conseils supplémentaires : Puisque les systèmes d'information, les composants de systèmes ou les services connexes peuvent être employés dans le cadre d'activités de nature critique qui s'avèrent essentielles à la protection des intérêts du Canada en matière de sécurité nationale ou économique, il est primordial que les organisations s'assurent qu'un développeur est digne de confiance. Il se pourrait que le niveau de fiabilité du développeur doive correspondre à celui des autres personnes ayant accès aux systèmes d'information, aux composants ou aux services après le déploiement. Parmi les exemples de critères d'autorisation ou de sélection du personnel, citons l'habilitation de sécurité, les enquêtes de sécurité, la citoyenneté et la nationalité. La

vérification de fiabilité des développeurs peut également nécessiter l'examen et l'analyse des titre de propriété ainsi que des relations que l'entreprise entretient avec des entités pouvant interférer avec la qualité/la fiabilité des systèmes d'information, des composants ou des services en développement. Contrôles connexes : PS-3, PS-7.

Améliorations du contrôle :

(1) SÉLECTION DES DÉVELOPPEURS | VALIDATION DE LA SÉLECTION

L'organisation exige que le développeur d'un système d'information, d'un composant du système ou d'un service connexe prenne [*Affectation : mesures définies par l'organisation*] pour veiller à ce que les critères visant les autorisations d'accès et la sélection soient respectés.

Conseils supplémentaires sur l'amélioration : Le fait de respecter les critères visant les autorisations d'accès et la sélection du personnel se manifeste, par exemple, par la production de listes des personnes autorisées à mener des activités de développement sur les divers systèmes d'information, composants de systèmes et ou services connexes, de façon à permettre aux organisations d'établir si un développeur répond aux exigences relatives aux autorisations et à la sélection.

Références :

Aucune

SA-22 COMPOSANTS SYSTÈMES NON PRIS EN CHARGE

Contrôle :

(A) L'organisation remplace les composants des systèmes d'information, lorsque la prise en charge de ces mêmes composants n'est plus offerte par le développeur, le fournisseur ou le fabricant.

(B) L'organisation justifie et documente l'approbation relative à la continuation de l'usage de composants de systèmes qui ne sont plus pris en charge, mais qui continuent de répondre aux besoins des missions ou des opérations.

Conseils supplémentaires : La prise en charge (ou le soutien) des composants de systèmes d'information englobe, par exemple, les programmes de correction, la mise à jour des microgiciels, les pièces de rechange, ainsi que les contrats de maintenance. Les composants non pris en charge (p. ex. lorsque les fournisseurs ne produisent plus de correctifs pour les problèmes critiques) constituent une vulnérabilité que des adversaires peuvent exploiter pour tirer parti de faiblesses nouvellement découvertes dans les composants déjà installés. En certaines situations exceptionnelles, il pourrait convenir de ne pas remplacer des composants de systèmes qui ne sont plus pris en charge, par exemple, lorsque les systèmes fournissent des capacités essentielles à une mission dans un lieu où les plus récentes technologies ne sont pas disponibles ou encore lorsque les systèmes sont si éloignés que l'installation de composants de rechange n'apparaît pas viable. Contrôles connexes : PL-2, SA-3.

Améliorations du contrôle :

(1) COMPOSANTS DE SYSTÈMES NON PRIS EN CHARGE | SOLUTION DE RECHANGE VISANT À ASSURER LA CONTINUITÉ DU SOUTIEN

L'organisation fournit [*Sélection (un ou plusieurs) : soutien en interne*; [*Affectation : soutien de fournisseurs externes défini par l'organisation*]] pour les composants de systèmes d'information non pris en charge.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle répond au besoin de fournir un soutien continu pour certains composants de systèmes qui ne sont plus pris en charge par les développeurs d'origine, les fournisseurs ou les fabricants, lorsque ces composants demeurent des éléments essentiels des missions ou des opérations. Les organisations peuvent elles-mêmes assurer un service de soutien, par exemple, en développant en interne des correctifs pour les principaux composants logiciels. En revanche, elles peuvent tout aussi bien retenir les services d'un fournisseur externe qui, en vertu d'une relation contractuelle, fournira un soutien continu visant certains composants non pris en charge. Les

relations contractuelles en question peuvent concerner, par exemple, les fournisseurs à valeur ajoutée de logiciels de source ouverte.

Références :

Aucune

CONTRÔLES D'ACQUISITION DES SYSTÈMES ET DES SERVICES

DÉVELOPPEMENT DE SYSTÈMES, DE COMPOSANTS ET DE SERVICES

Considérant l'importance des facteurs de fiabilité des systèmes d'information et de sécurité de la chaîne d'approvisionnement, il s'avère essentiel que les organisations se dotent de capacités qui leur permettent d'exprimer clairement et précisément leurs besoins en matière de sécurité de l'information, et ce, dans le but susciter l'intérêt de l'industrie des technologie de l'information et, ultimement, d'obtenir des systèmes, des composants et des services qui seront essentiels à la réussite des missions et des opérations. Pour veiller à ce que les organisations jouissent de telles capacités, la présente publication fournit un ensemble de contrôles de sécurité dans la famille *Acquisition des systèmes et des services* (p. ex. la famille SA) portant sur les exigences relatives au développement des systèmes d'information, des produits de technologie de l'information et de services de systèmes d'information. Ainsi, plusieurs des contrôles de la famille SA s'adressent directement aux développeurs de ces systèmes, composants et services. Il importe que les organisations reconnaissent que la portée des contrôles de sécurité de la famille SA englobe le développement de tous les systèmes/composants/services ainsi que les développeurs concernés, et que ledit développement soit exécuté par le personnel interne des organisations ou par des développeurs externes désignés par voie de contrats ou de processus d'acquisition. Contrôles touchés : SA-8, SA-10, SA-11, SA-15, SA-16, SA-17, SA-20 et SA-21.

3.16 FAMILLE : PROTECTION DES SYSTÈMES ET DES COMMUNICATIONS

CLASSE : TECHNIQUE

SC-1 POLITIQUE ET PROCÉDURES DE PROTECTION DES SYSTÈMES ET DES COMMUNICATIONS

Contrôle :

(A) L'organisation élabore et consigne, ainsi que diffuse aux [*Affectation : personnel ou rôles définis par l'organisation*] :

(a) une politique de protection des systèmes et des communications, qui définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité;

(b) des procédures visant à faciliter la mise en œuvre de la politique de protection des systèmes et des communisations ainsi que des contrôles connexes de protection des systèmes et des communications.

(B) L'organisation examine et met à jour :

(a) la politique de protection des systèmes et des communications au [*Affectation : fréquence définie par l'organisation*];

(b) les procédures de protection des systèmes et des communications au [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : Ce contrôle porte sur l'application de la politique et des procédures afférentes, qui ont pour objet de mettre en œuvre les divers contrôles ainsi que les améliorations ayant trait à la famille SC. La politique et les procédures de protection des systèmes et des communications répondent aux lois du GC ainsi qu'aux politiques, directives et normes applicables du SCT. Les politiques et les procédures du programme de sécurité organisationnel peuvent rendre facultatives les politiques et procédures propres au système. La politique peut être intégrée à la politique générale sur la sécurité de l'information des organisations ou, inversement, elle peut être représentée par de multiples politiques compte tenu de la nature complexe de certaines organisations. Les procédures peuvent être établies pour le programme de sécurité général et pour des systèmes d'information particuliers, le cas échéant. La stratégie organisationnelle de gestion des risques est un facteur clé dans l'établissement de la politique et des procédures.

Améliorations du contrôle :

Aucune

Références :

SCT, *Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information* [Référence 7].

SC-2 PARTITIONNEMENT DES APPLICATIONS

Contrôle :

(A) Le système d'information sépare la fonctionnalité de l'utilisateur (y compris les services d'interface utilisateur) de la fonctionnalité de gestion du système d'information.

Conseils supplémentaires : La fonctionnalité de gestion du système d'information comprend, par exemple, les fonctions nécessaires à l'administration des bases de données, des composants réseau, des postes de travail ou des serveurs, et exige normalement un accès utilisateur privilégié. La séparation de la fonctionnalité de l'utilisateur et de la fonctionnalité de gestion du système d'information est soit physique, soit logique. Les organisations appliquent la séparation de la fonctionnalité de gestion des systèmes de celle de l'utilisateur, par l'utilisation d'ordinateurs différents, d'unités centrales de traitement et d'instances du système d'exploitation différentes, d'adresses réseau différentes, de techniques de virtualisation, de combinaisons de ces méthodes, ou d'autres méthodes jugées appropriées. Ce type de séparation comprend, par exemple, les interfaces administratives Web qui utilisent des méthodes d'authentification distinctes (p. ex. à l'aide d'une séparation logique, un administrateur Web ferait appel à une authentification à deux facteurs, et les utilisateurs de l'application Web se serviraient de leur ID utilisateur et de leur mot de passe pour s'authentifier). La séparation des fonctionnalités de l'utilisateur et du système peut prévoir l'isolement des interfaces d'administration pour certains domaines et l'ajout de contrôles d'accès. Contrôles connexes : SA-4, SA-8, SC-3.

Améliorations du contrôle :

(1) PARTITIONNEMENT DES APPLICATIONS | INTERFACES POUR LES UTILISATEURS NON PRIVILÉGIÉS

Le système d'information empêche la présentation de la fonctionnalité liée à la gestion du système d'information à une interface pour les utilisateurs non privilégiés.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle permet de veiller à ce qu'aucune option d'administration (p. ex. les privilèges d'administrateur) ne soit accessible aux utilisateurs généraux (y compris l'interdiction de recourir aux options grisées normalement utilisées pour empêcher l'accès à ce type d'information). De telles restrictions peuvent comprendre, par exemple, le fait de ne pas afficher les options d'administration jusqu'à ce que les utilisateurs aient ouvert une session avec des privilèges d'administrateur. Contrôle connexe : AC-3.

Références :

Aucune

SC-3 ISOLEMENT DES FONCTIONS DE SÉCURITÉ

Contrôle :

(A) Le système d'information isole les fonctions de sécurité des autres fonctions.

Conseils supplémentaires : Le système d'information isole les fonctions de sécurité des autres fonctions au moyen d'un périmètre d'isolement (mis en œuvre à l'aide de partitions et de domaines). Un tel isolement permet l'accès aux composants matériels, logiciels et micrologiciels qui accomplissent les fonctions de sécurité, tout en en assurant l'intégrité. Les systèmes d'information appliquent la séparation des codes (p. ex. séparation entre les fonctions de sécurité et les autres fonctions) de diverses façons, y compris, à titre d'exemple, par des noyaux de sécurité au moyen d'anneaux de processeurs ou par des modes de processeurs. Pour ce qui est du code hors noyau, l'isolement de la fonction de sécurité est souvent réalisée par des mesures de protection du système de fichiers qui permettent de protéger le code sur disque et de tenir compte de la protection des espaces d'adressage, ce qui permet de préserver l'exécution du code. Les systèmes d'information restreignent l'accès aux fonctions de sécurité par le recours à des mécanismes de contrôle des accès et par la mise en œuvre de capacités fondées sur le principe des privilèges minimaux. Même s'il est largement préférable que l'espace réservé (isolement) à la fonction de sécurité ne contienne que l'intégralité du code ayant trait à la sécurité, il arrive exceptionnellement qu'il soit nécessaire d'ajouter d'autres fonctions à celles qui font déjà partie de l'espace isolé. Contrôles connexes : AC-3, AC-6, SA-4, SA-5, SA-8, SA-13,- SC-2, SC-7, SC-39.

Améliorations du contrôle :

(1) ISOLEMENT DE LA FONCTION DE SÉCURITÉ | SÉPARATION DU MATÉRIEL

Le système d'information recourt à des mécanismes sous-jacents de séparation matérielle pour appliquer l'isolement des fonctions de sécurité.

Conseils supplémentaires sur l'amélioration : Les mécanismes sous-jacents de séparation matérielle comprennent, par exemple, les architectures matérielles en anneau, qui sont couramment mises en œuvre pour les microprocesseurs, ainsi que la segmentation physique des adresses, qui est employée pour assurer le soutien des objets de stockage logiquement différents possédant chacun ses attributs (p. ex. lisible, modifiable).

(2) ISOLEMENT DE LA FONCTION DE SÉCURITÉ | ACCÈS / FONCTIONS DE CONTRÔLE DES FLUX

Le système isole les fonctions de sécurité appliquant le contrôle de l'accès et du flux d'information des autres fonctions de sécurité et des fonctions non liées à la sécurité.

Conseils supplémentaires sur l'amélioration : L'isolement de la fonction de sécurité est le résultat de la mise en œuvre; les fonctions continuent de se prêter aux balayages et à la surveillance. Les fonctions de sécurité qui sont potentiellement isolées des fonctions d'application du contrôle des accès et des flux comprennent, par exemple, les audits, la détection des intrusions et les fonctions antivirales.

(3) ISOLEMENT DE LA FONCTION DE SÉCURITÉ | REDUCTION DES FONCTIONNALITÉS N'AYANT PAS TRAIT À LA SÉCURITÉ

L'organisation réduit à son minimum le nombre des fonctions non liées à la sécurité appelées à intégrer le périmètre isolé qui comprend les fonctions de sécurité.

Conseils supplémentaires sur l'amélioration : Dans les cas où il s'avère impossible de procéder à la stricte ségrégation des fonctions de sécurité et des autres fonctions, il importera d'adopter des mesures visant à réduire, au sein du périmètre d'isolement de la fonction de sécurité, le nombre des fonctions n'ayant pas trait à la sécurité. En raison de leur proximité, les fonctions non liées à la sécurité qui sont comprises dans le périmètre d'isolement sont considérées comme pertinentes à la sécurité, puisque les erreurs ou les éléments malveillants qu'elles peuvent contenir peuvent avoir des répercussions directes sur les fonctions de sécurité des systèmes organisationnels d'information. Sur le plan de la conception, il est donc important que les parties de systèmes d'information qui assurent la protection de l'information soient aussi modestes que possible, tant sur le plan du volume que de la complexité. La réduction du nombre de fonctions non liées à la sécurité au sein des composants servant à la sécurité dans les systèmes d'information permet aux ingénieurs et aux responsables de la mise en œuvre de se concentrer exclusivement sur les fonctions qui sont essentielles à l'exécution des capacités de sécurités requises (typiquement les mesures de contrôle des accès). En réduisant le nombre des fonctions non liées à la sécurité dans le périmètre d'isolement, on observe une réduction du volume de code devant être jugé fiable sur le plan de l'application des politiques de sécurité, ce qui accroit l'intelligibilité.

(4) ISOLEMENT DE LA FONCTION DE SÉCURITÉ | JUMELAGE ET COHÉSION DES MODULES

L'organisation applique les fonctions de sécurité sous forme de modules essentiellement indépendants qui maximisent la cohésion interne des modules et réduisent les jumelages entre modules.

Conseils supplémentaires sur l'amélioration : La réduction des interactions entre les modules aide à limiter les fonctions de sécurité et à en gérer la complexité. Les concepts de jumelage et de cohésion sont importants sur le plan de la modularité de la conception logicielle. Le jumelage renvoie aux dépendances qu'un module peut avoir avec d'autres modules. Or, la cohésion fait référence à la relation entre les différentes fonctions d'un module donné. Les pratiques exemplaires du domaine du génie logiciel misent sur la décomposition modulaire, la structuration en couches et la réduction, qui visent à diminuer et à gérer la complexité de façon à produire des modules logiciels hautement cohésifs et peu jumelés.

(5) ISOLEMENT DE LA FONCTION DE SÉCURITÉ |

L'organisation applique les fonctions de sécurité dans une structure en couches qui permet de réduire les interactions entre les couches de la conception et d'éviter que les couches inférieures soient tributaires du bon fonctionnement des couches supérieures ou de leurs fonctions.

Conseils supplémentaires sur l'amélioration : L'adoption de structures en couches nécessitant peu d'interaction entre les fonctions de sécurité et les couches libres [non-looping] (p. ex. les fonctions des couches inférieures ne dépendent pas des fonctions des couches supérieures) accentue l'isolement des fonctions de sécurité et facilite la gestion de la complexité.

Références :

CST, *ITSG-23, Isolement d'un serveur d'entreprise BlackBerry dans un environnement Microsoft Exchange* [Référence 42].
CST, *ITSG-38, Établissement des zones de sécurité dans un réseau – Considérations de conception relatives au positionnement des services dans les zones* [Référence 43].

SC-4 INFORMATION CONTENUE DANS LES RESSOURCES PARTAGÉES

Contrôle :

(A) Le système d'information empêche tout transfert d'information non autorisé et involontaire découlant du partage des ressources du système.

Conseils supplémentaires : Ce contrôle vise à empêcher l'information (y compris ses représentations chiffrées) produite par les opérations effectuées par des utilisateurs/des rôles antérieurs (ou des processus exécutés en leur nom) d'être transmise à des utilisateurs ou des rôles (ou processus) actuels qui accèdent à des ressources partagées (p. ex. registres, mémoire principale, disques durs) après que ces ressources ont été retournées aux systèmes d'information. Le contrôle de l'information contenue dans les ressources partagées est aussi couramment appelé réutilisation d'un objet et protection de l'information résiduelle. Ce contrôle ne s'applique pas (i) à la rémanence d'information, laquelle désigne les représentations résiduelles de données qui ont été supposément effacées ou supprimées; (ii) ni aux canaux cachés (y compris les canaux de stockage ou de synchronisation) où les ressources partagées sont manipulées de façon à enfreindre les restrictions relatives aux flux d'information, (iii) ni aux composants des systèmes d'information, chacun associé à un seul utilisateur ou un seul rôle. Contrôles connexes : AC-3, AC-4, MP-6.

Améliorations du contrôle :

(1) INFORMATION CONTENUE DANS LES RESSOURCES PARTAGÉES | NIVEAUX DE SÉCURITÉ

[Annulé : Intégré au contrôle SC-4]

(2) INFORMATION CONTENUE DANS LES RESSOURCES PARTAGÉES | TRAITEMENT DES PÉRIODES

Le système d'information prévient le transfert non autorisé d'information par l'intermédiaire de ressources partagées conformément à [*Affectation : procédures définies par l'organisation*] lorsque le traitement exécuté par le système alterne explicitement entre divers niveaux de classification de l'information ou différentes catégories de sécurité.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle s'applique lorsqu'il y a des changements explicites dans les niveaux de traitement de l'information pendant les opérations du système, par exemple, durant le traitement multiniveau et le traitement des périodes pour de l'information de divers niveaux de classification ou de différentes catégories de sécurité. Les procédures définies par l'organisme pourraient inclure, par exemple, des processus de nettoyage approuvés et destinés à l'information stockée électroniquement.

Références :

Aucune

SC-5 PROTECTION CONTRE LES DÉNIS DE SERVICE

Contrôle :

(A) Le système d'information assure une protection contre les types suivants d'attaques par déni de service ou en limite les effets : [*Affectation : types d'attaques par déni de service ou renvoi à la source de ces informations*] par l'emploi de [*Affectation : mesures de protection de sécurité définies par l'organisation*].

Conseils supplémentaires : Il existe une variété de technologies qui limitent ou, dans certains cas, éliminent les effets des attaques par déni de service. Par exemple, les mécanismes de protection des frontières peuvent filtrer certain types de paquets pour empêcher les composants d'un système d'information faisant partie de l'un des réseaux organisationnels internes d'être directement visés par des attaques par déni de service. Combinée à la redondance des services, l'utilisation d'une capacité et d'une largeur de bande accrues peut également réduire la sensibilité à certaines attaques par déni de service. Contrôles connexes : SC-6, SC-7.

Améliorations du contrôle :

(1) PROTECTION CONTRE LES DÉNIS DE SERVICE | RESTRICTIONS RELATIVES AUX UTILISATEURS INTERNES

Le système d'information limite la capacité d'auteurs de menaces à lancer [*Affectation : attaques par déni de service désignées par l'organisation*] contre d'autres systèmes d'information.

Conseils supplémentaires sur l'amélioration : L'aptitude à limiter la capacité des individus à lancer des attaques par déni de service exige que les mécanismes utilisés pour de telles attaques soient non disponibles. Les personnes à surveiller sont, par exemple, des membres hostiles de l'organisation ou des adversaires externes qui sont parvenus à percer le système d'information et à l'utiliser comme plateforme de lancement d'attaques sur de tiers partis. Les organisations peuvent restreindre la capacité des individus à se connecter et à transmettre de l'information aléatoire par le médium de transport (p. ex. réseau, spectre sans fil). Les organisations peuvent également restreindre la capacité des individus à utiliser excessivement les ressources du système d'information. La protection contre la capacité de certains individus à lancer des attaques par déni de service peut être mise en œuvre sur certains systèmes d'information ou sur des dispositifs limitrophes, de façon à prévenir les atteintes aux systèmes pouvant constituer une cible.

(2) PROTECTION CONTRE LES DÉNIS DE SERVICE | EXCÉDENT DE CAPACITÉ / BANDE PASSANTE / REDONDANCE

Le système d'information gère l'excédent de capacité et de bande passante ou toute autre redondance, afin de limiter l'effet des attaques par déni de service qui provoquent des inondations d'information.

Conseils supplémentaires sur l'amélioration : La gestion de l'excédent de capacité garantit que la capacité est suffisante pour contrer les inondations d'information. La gestion de l'excédent de capacité peut inclure, par exemple, l'établissement de priorités relatives à certaines utilisations, les normes de rendement, le partitionnement.

(3) PROTECTION CONTRE LES DÉNIS DE SERVICE | DÉTECTION / SURVEILLANCE

(a) L'organisation emploie [*Affectation : outils de surveillance désignés par l'organisation*] pour déceler les indicateurs d'attaques par déni de service lancées contre les systèmes d'information.

(b) L'organisation surveille [*Affectation : ressources de système d'information désignées par l'organisation*] dans le but d'établir si les ressources sont suffisantes pour prévenir efficacement les attaques par déni de service.

Conseils supplémentaires sur l'amélioration : Les organisations examinent l'utilisation et l'importance des ressources de systèmes d'information, lorsqu'ils procèdent à la gestion des risques liés à des attaques par déni de service pouvant résulter d'attaques malveillantes. Les attaques par déni de service peuvent provenir de sources internes ou externes. Dans les systèmes d'information, les ressources sensibles aux attaques par déni de service sont, par exemple, les fonctions de stockage sur disque matériel, la mémoire, et les cycles des unités centrales de traitement. Au nombre des mécanismes de protection courants qui permettent de prévenir les attaques par déni de service visant les fonctions et la capacité de stockage,

citons, par exemple, l'imposition d'une limite pour les disques, une configuration des systèmes d'information qui permette d'alerter automatiquement les administrateurs lorsque la limite d'une capacité de stockage est atteinte, l'utilisation de technologies de compression de fichiers dans le but de maximiser l'espace de stockage, et l'imposition de partitions distinctes pour les données système et les données d'utilisateurs. Contrôles connexes : CA-7, SI-4.

Références :

CST, *ITSG-22, Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada* [Référence 41].

SC-6 DISPONIBILITÉ DES RESSOURCES

Contrôle :

(A) Le système d'information garantit la disponibilité des ressources en attribuant [*Affectation : ressources désignées par l'organisation*] en fonction de [Sélection (une ou plusieurs); priorité; quota; [*Affectation : mécanismes de protection définis par l'organisation*]].

Conseils supplémentaires : La protection des priorités permet d'éviter que des processus retardent ou empêchent l'exécution de processus de priorité supérieure par le système d'information. Les quotas empêchent que des utilisateurs ou des processus disposent de plus de ressources que prévu. Ce contrôle ne s'applique pas aux composants du système d'information qui ne sont associés qu'à un seul utilisateur ou un seul rôle.

Améliorations du contrôle :

Aucune

Références :

Aucune

SC-7 PROTECTION DES FRONTIÈRES

Contrôle :

(A) Le système d'information surveille et contrôle les communications à sa frontière externe et à ses principales frontières internes.

(B) Le système d'information utilise des sous-réseaux pour les composants qui sont accessibles au public et qui sont [*Sélection : physiquement; logiquement*] séparés des réseaux internes organisationnels.

(C) Le système d'information se connecte aux réseaux ou aux systèmes d'information externes uniquement par des interfaces gérées qui sont dotées de mécanismes de protection des frontières répartis conformément à l'architecture de sécurité de l'organisation.

Conseils supplémentaires : Au nombre des interfaces gérées, citons, par exemple, les passerelles, les routeurs, les murs coupe-feu, les gardes, les systèmes réseaux de virtualisation et d'analyse de code malveillant ou les tunnels chiffrés qui ont été mis en place dans une architecture de sécurité (p. ex. routeurs protégeant les coupe-feux ou passerelles d'application hébergées dans des sous-réseaux protégés). Les sous-réseaux qui sont physiquement ou logiquement séparés des réseaux internes font partie de ce que l'on appelle communément des zones démilitarisées ou des DMZ (pour *Demilitarized Zones*). La restriction et l'interdiction relatives aux interfaces des systèmes d'information organisationnels peuvent inclure, par exemple, le fait de diriger le trafic Web externe vers les serveurs Web organisationnels en utilisant des interfaces gérées ou encore le fait d'interdire tout trafic externe qui semble mystifier une adresse interne. Les organisations tiennent compte de la nature

partagée des services commerciaux de télécommunications lors de la mise en œuvre des contrôles de sécurité associés à leur utilisation. Ces services s'appuient habituellement sur des composants réseau et des systèmes de gestion intégrés partagés par tous les clients commerciaux connectés et peuvent également inclure des lignes d'accès et autres éléments de service fournis par des tiers. De tels services de transmission peuvent représenter des sources de risque supplémentaire, malgré les dispositions du contrat en matière de sécurité. Contrôles connexes : AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13.

Améliorations du contrôle :

(1) PROTECTION DE LA FRONTIÈRE | RÉSEAUX SÉPARÉS PHYSIQUEMENT

[Annulé : Intégré au contrôle SC-7]

(2) PROTECTION DE LA FRONTIÈRE | ACCÈS PUBLIC

[Annulé : Intégré au contrôle SC-7]

(3) PROTECTION DE LA FRONTIÈRE | POINTS D'ACCÈS

L'organisation limite le nombre de connexions réseau externes au système d'information.

Conseils supplémentaires sur l'amélioration : La limitation du nombre de connexions réseau externes permet d'exercer une surveillance accrue du trafic de communication entrant et sortant. L'initiative Consolidation des points d'accès à Internet du SCT est un exemple de restriction du nombre de connexions réseau externes.

(4) PROTECTION DE LA FRONTIÈRE | SERVICES DE TÉLÉCOMMUNICATIONS EXTERNES

(a) L'organisation applique une interface gérée à chaque service de télécommunications externe.

(b) L'organisation établit une politique relative aux flux de trafic pour chaque interface gérée.

(c) L'organisation protège la confidentialité et l'intégrité de l'information transmise par l'intermédiaire les interfaces.

(d) L'organisation documente chaque exception à la politique de flux de trafic en précisant le besoin de la mission ou de l'activité opérationnelle donnant lieu à l'exception et la durée de ce besoin.

(e) L'organisation examine les exceptions à la politique relative aux flux de trafic [*Affectation : fréquence définie par l'organisation*] et retranche les exceptions qui ne sont plus justifiées par une mission ou par un besoin opérationnel.

Conseils supplémentaires sur l'amélioration : Contrôle connexe : SC-8.

(5) PROTECTION DE LA FRONTIÈRE | REFUS PAR DÉFAUT / PERMISSION PAR EXCEPTION

Le système d'information, au niveau des interfaces gérées, interdit tout trafic de communication réseau par défaut et ne l'autorise qu'exceptionnellement (c.-à-d. interdit tout trafic, permet le trafic par exception).

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle s'applique au trafic entrant et sortant des communications réseau. Une politique relative au trafic des communications réseau qui interdit tout trafic et ne permet le passage qu'à titre exceptionnel assure que seules les connexions essentielles et approuvées sont permises.

(6) PROTECTION DE LA FRONTIÈRE | RÉPONSE AUX ÉCHECS RECONNUS

[Annulé : Intégré au contrôle SC-7 (18)]

(7) PROTECTION DE LA FRONTIÈRE | PRÉVENTION DE LA TUNNELLISATION PARTAGÉE POUR LES DISPOSITIFS ÉLOIGNÉS

Le système d'information, en conjonction avec un dispositif éloigné, empêche que celui-ci établisse simultanément des connexions à des ressources locales du système et à d'autres ressources de réseaux externes.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle est appliquée dans les dispositifs à distance (p. ex. ordinateurs portables) en paramétrant les configurations de façon à y désactiver la fonction de tunnellisation partagée et en empêchant que les paramètres de configuration soient modifiable par les utilisateurs. Cette amélioration de contrôle est appliquée dans le système d'information par la détection de la tunnellisation partagée (ou des paramètres de configuration qui permettent la tunnellisation partagée) dans les dispositifs à distance, ainsi que par l'interdiction des connexions lorsque le dispositif à distance utilise la tunnellisation partagée. La tunnellisation partagée peut s'avérer désirable par les utilisateurs à distance lorsqu'ils souhaitent communiquer avec les ressources du système local d'information, notamment les serveurs d'impression et de fichiers. Toutefois, la tunnellisation partagée donnerait également libre cours aux connexions non autorisées, rendant ainsi le système plus vulnérable aux attaques et aux exfiltrations d'information organisationnelle. Lorsqu'il est doté des contrôles de sécurité appropriés, le réseau privé virtuel peut offrir, à une organisation, l'assurance que les connexions à distances seront adéquatement traitées comme des connexions locales (non distantes) du point de vue de la confidentialité et de l'intégrité. Ainsi, les réseaux privés virtuels constituent un moyen d'offrir des liens de communication de « type » local depuis des dispositifs à distance. Par contre, l'utilisation d'un réseau privé virtuel correctement conçu et adéquatement configuré n'écarte pas la nécessité d'interdire la tunnellisation partagée.

(8) PROTECTION DE LA FRONTIÈRE | ACHEMINEMENT DU TRAFIC VERS LES SERVEURS MANDATAIRES AUTHENTIFIÉS

Le système d'information achemine [*Affectation : trafic de communications interne défini par l'organisation*] vers [*Affectation : réseaux externes définis par l'organisation*] à travers des serveurs mandataires authentifiés à proximité des interfaces gérées.

Conseils supplémentaires sur l'amélioration : Les réseaux externes sont des réseaux qui échappent au contrôle de l'organisation. Un serveur mandataire est un serveur (p. ex. système d'information ou application) qui sert d'intermédiaire auprès des clients qui veulent accéder aux ressources d'un système d'information (p. ex. fichiers, connexions, pages Web ou services) depuis d'autres serveurs organisationnels. Par une connexion initiale au serveur mandataire, les clients soumettent des requêtes qui sont évaluées de façon à gérer la complexité et à fournir une protection additionnelle par la restriction des connexions directes. Les dispositifs de filtrage de contenus Web constituent les serveurs mandataires les plus couramment utilisés pour fournir un accès Internet. Les serveurs mandataires prennent en charge la création de sessions de protocole TCP (pour *Transmission Control Protocol*) individuelles de même que le blocage des localisateurs uniformes de ressources (URL pour *Uniform Resource Locators*), d'adresses de protocole IP (*Internet Protocol*) et de noms de domaine particuliers. Les serveurs mandataires Web peuvent également être configurés à partir de listes de sites Web autorisés et non autorisés définies par l'organisation. Contrôles connexes : AC-3, AU-2.

(9) PROTECTION DE LA FRONTIÈRE | RESTRICTION DU TRAFIC DE COMMUNICATIONS MALVEILLANT SORTANT

(a) Le système d'information détecte et bloque le trafic de communications sortant pouvant constituer une menace aux systèmes externes d'information.

(b) Le système d'information vérifie l'identité des utilisateurs internes associés aux communications bloquées.

Conseils supplémentaires sur l'amélioration : La détection du trafic de communications sortant provenant d'activités internes et susceptible de poser une menace pour les systèmes d'information externes est parfois désignée sous le nom de détection d'extrusion. Partie intégrante des interfaces gérées, la détection d'extrusions au niveau des frontières d'un système d'information comprend une analyse du trafic de communications entrant et sortant qui vise à trouver des indications de menaces internes ciblant la sécurité des systèmes externes. Les menaces peuvent être, par exemple, du trafic annonciateur d'attaques par déni de service et du trafic contenant du code malveillant. Contrôles connexes : AU-2, AU-6, SC-38, SC-44, SI-3, SI-4.

(10) PROTECTION DE LA FRONTIÈRE | PRÉVENTION DES EXFILTRATIONS NON AUTORISÉES

L'organisation empêche l'exfiltration d'information non autorisée à travers les interfaces gérées.

Conseils supplémentaires sur l'amélioration : Les mécanismes de protection mis en œuvre pour empêcher l'exfiltration d'information non autorisée du système d'information comprennent, par exemple, (i) le respect strict des formats de protocole; (ii) la surveillance du balisage en provenance des systèmes d'information; (iii) la surveillance de la stéganographie; (iv) la déconnexion des interfaces réseau externes, sauf lorsqu'elles sont explicitement requises; (v) le désassemblage et le réassemblage d'en-têtes de paquet; et (vi) l'analyse des profils de trafic visant à détecter tout écart par rapport au volume/aux types de trafic attendus au sein des organisations ou les procédures de rappel vers les centres de commandement et de contrôle. Les dispositifs qui appliquent un respect rigoureux des formats de protocole comprennent les coupe-feux d'inspection approfondie des paquets et les passerelles XML. Ces dispositifs vérifient le respect de la spécification et du format de protocole au niveau de la couche application et permettent d'identifier les vulnérabilités indétectables au moyen de dispositifs fonctionnant au niveau des couches réseau ou transport. Cette amélioration de contrôle est étroitement associée aux solutions interdomaines et aux gardes de systèmes qui appliquent les exigences relatives aux flux d'information. Contrôle connexe : SI-3.

(11) PROTECTION DE LA FRONTIÈRE | RESTRICTION DU TRAFIC DE COMMUNICATIONS ENTRANT

Le système d'information ne permet que les communications entrantes provenant de [*Affectation : sources autorisées désignées par l'organisation*] acheminée vers [*Affectation : destinations autorisées désignées par l'organisation*].

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle fournit des indices que les paires d'adresses (source et destination) représentent des communications autorisées/permises. Ce tels indices peuvent être fondés sur divers facteurs, notamment la présence de paires d'adresses (source/destination) dans les listes de communications autorisées/permises, l'absence de paires d'adresses dans les listes de paires non autorisées/interdites, ou le respect de règles plus générales de paires (sources/destination) autorisées/permises. Contrôle connexe : AC-3.

(12) PROTECTION DE LA FRONTIÈRE | PROTECTION AU NIVEAU DE L'HÔTE

Les organisations mettent en œuvre [*Affectation : mécanismes de protection de la frontière au niveau de l'hôte définis par l'organisation*] à [*Affectation : composants des systèmes d'information désignés par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les mécanismes de protection des frontières intégrés à l'hôte peuvent être, par exemple, des ordinateurs coupe-feu. Les composants de système d'information qui appliquent des mécanismes de protection des frontières intégrés à l'hôte peuvent être, par exemple, des serveurs, des postes de travail et des dispositifs mobiles.

(13) PROTECTION DE LA FRONTIÈRE | ISOLEMENT DES OUTILS DE SÉCURITÉ / MÉCANISMES / COMPOSANTS DE SOUTIEN

L'organisation isole les [*Affectation : outils, mécanismes et composants de soutien à la sécurité de l'information définis par l'organisation*] des autres composants internes du système d'information par l'implantation de sous-réseaux physiques distincts dotés d'interfaces gérées et tournées vers les autres composants du système.

Conseils supplémentaires sur l'amélioration : La distinction physique des sous-réseaux dotés d'interfaces gérées est utile, par exemple, lorsqu'il s'agit d'isoler les défenses d'un réseau informatique des réseaux de traitement opérationnel essentiel, dans le but d'empêcher les parties adverses de découvrir les techniques organisationnelles d'analyse et d'informatique judiciaire. Contrôles connexes : SA-8, SC-2, SC-3.

(14) PROTECTION DE LA FRONTIÈRE | PROTECTION CONTRE LES CONNEXIONS PHYSIQUES NON AUTORISÉES

L'organisation assure une protection contre les connexions physiques non autorisé à [*Affectation : interfaces gérées désignées par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les systèmes d'information fonctionnant selon diverses catégories de sécurité ou divers niveaux de classification pourraient partager des contrôles physiques et environnementaux communs, puisqu'ils peuvent occuper les mêmes locaux dans les installations de l'organisation. En pratique, ces systèmes d'information distincts peuvent également partager les mêmes

salles d'équipement, armoires de câblage et voies de distribution des câbles. La protection contre les connexions physiques non autorisées peut être assurée, par exemple, par l'utilisation de chemins de câbles, de boîtiers de raccordement et de tableaux de connexions physiquement distincts et clairement identifiés à chaque extrémité des interfaces gérées et dotés de contrôles d'accès physique qui limitent les accès. Contrôles connexes : PE-4, PE-19.

(15) PROTECTION DE LA FRONTIÈRE | ADRESSES RÉSEAU PRIVILÉGIÉES PAR UNE ROUTE

Le système d'information achemine tous les accès réseau privilégiés à travers une interface gérée spécialisée aux fins de contrôle des accès et de vérification.

Conseils supplémentaires sur l'amélioration – Contrôles connexes : AC-2, AC-3, AU-2, SI-4.

(16) PROTECTION DE LA FRONTIÈRE | PRÉVENTON DE LA DÉCOUVERTE DES COMPOSANTES / DISPOSITIFS

Le système d'information empêche la découverte des composants de système particuliers d'une interface gérée.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle assure une protection contre la découverte les adresses réseau des composants du système d'information qui font partie des interfaces gérées à l'aide de techniques et d'outils communs servant à identifier les dispositifs de réseaux. Des adresses réseau ne sont pas disponibles aux fins de découverte (p. ex. une adresse réseau qui n'est ni publiée ni entrée dans les systèmes de noms de domaines) et doivent être connues au préalable pour qu'on puisse y accéder. Une autre technique visant à camoufler ces adresses consiste à les changer périodiquement.

(17) PROTECTION DE LA FRONTIÈRE | APPLICATION AUTOMATISÉE DES FORMATS DE PROTOCOLES

Le système d'information applique la stricte adhésion aux formats de protocoles.

Conseils supplémentaires sur l'amélioration : Les composants de systèmes d'information qui servent à appliquer les formats de protocole comprennent, par exemple, les coupe-feux d'inspection approfondie des paquets et les passerelles XML. De tels composants de systèmes vérifient l'adhésion aux spécifications et aux formats de protocoles (p. ex. IEEE) au niveau de la couche application et permettent d'identifier les vulnérabilités indétectables par des dispositifs fonctionnant au niveau des couches réseau ou transport. Contrôle connexe : SC-4.

(18) PROTECTION DE LA FRONTIÈRE | MODE SÛR APRÈS DÉFAILLANCE

Le système d'information passe en mode de fonctionnement à sécurité intégrée (*fail secure*) dans l'éventualité d'une défaillance opérationnelle d'un dispositif de protection des frontières.

Conseils supplémentaires sur l'amélioration : Le fonctionnement à sécurité intégrée est une condition obtenue par l'emploi de mécanismes de systèmes d'information qui, dans l'éventualité de défaillances opérationnelle de dispositifs de protection des frontières au niveau des interfaces gérées (p. ex. routeurs, ordinateurs coupe-feu, gardes et passerelles d'applications situées dans des sous-réseaux protégés appelés couramment zones démilitarisées), font en sorte que les systèmes ne passent pas à des états non sécurisés dans lesquels les propriétés de sécurité prévues n'ont plus aucun effet. Les défaillances de dispositifs de protection des frontières ne doivent pas permettre à l'information qui est extérieure aux dispositifs d'entrer dans ce dernier ni permettre la diffusion non autorisée d'information. Contrôles connexes : CP-2, SC-24.

(19) PROTECTION DE LA FRONTIÈRE | BLOCAGE DES COMMUNICATIONS PROVENANT D'HÔTES NON CONFIGURÉS PAR L'ORGANISME

Le système d'information bloque le trafic de communications entrant et sortant entre [*Affectation : clients en communication désignés par l'organisation*] qui sont configurés indépendamment par les utilisateurs et les fournisseurs de services externes.

Conseils supplémentaires sur l'amélioration : Les clients communiquant qui sont configurés distinctement par des utilisateurs terminaux et des fournisseurs de services externes comprennent, par

exemple, les clients de messagerie instantanée. Le blocage de trafic ne s'applique pas aux clients communiquant qui sont configurés par des organisations dans le but d'exécuter des fonctions autorisées.

(20) PROTECTION DE LA FRONTIÈRE | ISOLEMENT DYNAMIQUE / SÉGRÉGATION

Le système d'information fournit la capacité d'isoler/de séparer dynamiquement [*Affectation : composants du système d'information définis par l'organisation*] des autres composants du système.

Conseils supplémentaires sur l'amélioration : La capacité d'isoler ou de séparer dynamiquement certains composants internes faisant partie des systèmes organisationnels d'information s'avère utile lorsqu'il est nécessaire de partitionner ou de séparer certains composants d'origine douteuse des composants jugés fiables. L'isolement des composants réduit la surface d'attaque des systèmes organisationnels d'information. L'isolement de certains composants de systèmes d'information représente également un moyen de limiter les dommages causés par les cyberattaques qui ont réussi.

(21) PROTECTION DE LA FRONTIÈRE | ISOLEMENT DES COMPOSANTS DE SYSTÈMES D'INFORMATION

L'organisation emploie des mécanismes de protection de la frontière dans le but de séparer [*Affectation : composants du système d'information définis par l'organisation*] assurant le soutien aux [*Affectation : fonctions opérationnelles/missions désignées par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les organisations peuvent isoler des composants de systèmes d'information qui exécutent diverses fonctions liées à une de mission ou à des opérations. Ce type d'isolement limite les flux d'information non autorisés parmi les composants de systèmes et fournit l'occasion de mettre en œuvre des niveaux de sécurité accrus pour certains composants. La séparation des composants de systèmes par des mécanismes de protection frontalière permet d'accroître la protection de chacun des composants et d'intensifier le contrôle des flux d'information entre ces mêmes composants. Ce type de protection accrue limite les dommages que les cyberattaques et les erreurs pourraient causer. Le degré de séparation varie selon les mécanismes choisis. Au nombre des mécanismes de protection, citons en exemple les routeurs, les passerelles et les dispositifs coupe-feu qui séparent les composants de systèmes dans des réseaux ou sous-réseaux physiques distincts; les dispositifs interdomaines séparant les sous-réseaux; les techniques de virtualisation; et le chiffrement des flux d'information circulant parmi les composants de systèmes au moyen de clés de chiffrement distinctes. Contrôles connexes : CS-9, SC-3.

(22) PROTECTION DE LA FRONTIÈRE | SOUS-RÉSEAUX DISTINCTS POUR LA CONNEXION À DES DOMAINES DE SÉCURITÉ DIFFÉRENTS

Le système d'information applique des adresses réseau distinctes (p. ex. sous-réseaux différents) pour établir une connexion à des systèmes se trouvant dans des domaines de sécurité différents.

Conseils supplémentaires sur l'amélioration : La segmentation des systèmes d'information en sous-réseaux aide à fournir le niveau de protection requis pour les connexions réseau à des domaines de sécurité différents qui contiennent de l'information dotée de catégories de sécurité différentes ou de niveaux de sécurité différents.

(23) PROTECTION DE LA FRONTIÈRE | DÉSACTIVATION DE LA RÉTROACTION DE L'ENVOYEUR APRÈS L'ÉCHEC DE VALIDATION D'UN PROTOCOLE

Le système d'information désactive la fonction de rétroaction à l'envoyeur lorsqu'il y a échec de la validation d'un format de protocole.

Conseils supplémentaires sur l'amélioration : La désactivation de la rétroaction à l'envoyeur en cas d'échec de la validation du format d'un protocole empêche les adversaires d'obtenir de l'information qui, en d'autres circonstances, serait non disponible.

Références :

CST, *ITSG-22, Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada* [Référence 41].
CST, *ITSG-23, Isolement d'un serveur d'entreprise BlackBerry dans un environnement Microsoft Exchange* [Référence 42].

CST, ITSG-38, Établissement des zones de sécurité dans un réseau – Considérations de conception relatives au positionnement des services dans les zones [Référence 43].

SC-8 CONFIDENTIALITÉ ET INTÉGRITÉ DES TRANSMISSIONS

Contrôle :

(A) Le système d'information protège [*Sélection (une ou plusieurs) la confidentialité; l'intégrité*] de l'information transmise.

Conseils supplémentaires : Ce contrôle s'applique aux réseaux internes et externes ainsi qu'à tout type de composant de système d'information depuis lequel de l'information peut être transmise (p. ex. serveurs, dispositifs mobiles, ordinateurs portables, imprimantes, photocopieurs, numériseurs, télécopieurs). Les voies de communication à l'extérieur de la protection physique d'une frontière contrôlée s'exposent aux interceptions et aux modifications. La protection de la confidentialité/de l'intégrité de l'information organisationnelle peut se concrétiser par des moyens physiques (p. ex. par l'emploi de systèmes de distribution protégés) ou par des moyens logiques (p. ex. emploi de techniques de chiffrement). Les organisations qui misent sur des fournisseurs commerciaux offrant des fonctions de transmission qui sont des services accessoires plutôt que des services nominaux (p. ex. services pouvant être hautement adaptés aux besoins de chaque client), peut éprouver des difficultés à obtenir les assurances nécessaires relativement à la mise en œuvre des contrôles de sécurité requis à des fins de transmissions confidentielles et intégrales. Dans de telles situations, les organisations établissent les types de services confidentiels/intégrés qui sont disponibles dans les ensembles de services de télécommunications commerciaux standards. S'il est impossible ou difficilement réalisable d'obtenir les contrôles de sécurité nécessaires et l'assurance qu'ils sont appliqués de manière efficace par la voie contractuelle appropriée, les organisations doivent soit appliquer des contrôles de sécurité compensatoires appropriés, soit accepter explicitement le risque supplémentaire. Contrôles connexes : AC-17, PE-4.

Améliorations du contrôle :

(1) CONFIDENTIALITÉ ET INTÉGRITÉ DES TRANSMISSIONS | PROTECTION CRYPTOGRAPHIQUE OU PHYSIQUE

Le système d'information applique des mécanismes cryptographiques pour [*Sélection (un ou plusieurs) : prévenir la divulgation non autorisée d'information; détecter les modifications apportées à l'information*] en cours de transmission, à moins que l'information en question soit protégée par [*Affectation : autres mesures de protection physiques définies par l'organisation*]. La cryptographie doit être conforme aux exigences du contrôle SC-13.

Conseils supplémentaires sur l'amélioration : Le chiffrement de l'information à des fins de transmission protège celle-ci contre les divulgations et les modifications non autorisées. Les mécanismes de chiffrement que l'on applique à des fins de protection de l'intégrité de l'information comprennent notamment les fonctions de hachage cryptographique qui ont une application semblable relativement aux signatures numériques, les sommes de contrôle et les codes d'authentification des messages. Les autres mesures physiques de protection comprennent, par exemple, les systèmes de diffusion protégée. Contrôle connexe : SC-13.

(2) CONFIDENTIALITÉ ET INTÉGRITÉ DES TRANSMISSIONS | TRAITEMENT PRÉ-TRANSMISSION / POST-TRANSMISSION

Le système d'information maintient [*Sélection (une ou plusieurs) : confidentialité; intégrité*] de l'information pendant la préparation à la transmission et pendant la réception.

Conseils supplémentaires sur l'amélioration : L'information est divulguée/modifiée accidentellement ou malicieusement en cours de transmission ou encore pendant la réception, notamment pendant l'agrégation, aux points de transformation de protocole et pendant le groupage/le dégroupage. Ces divulgations ou

modifications non autorisées compromettent la confidentialité ou l'intégrité de l'information. Contrôle connexe : AU-10.

(3) CONFIDENTIALITÉ ET INTÉGRITÉ DES TRANSMISSIONS | PROTECTION CRYPTOGRAPHIQUE RELATIVE AUX MESSAGES EXTERNES

Le système d'information applique des mécanismes visant à protéger les éléments complémentaires des messages, sauf si l'information est protégée par [*Affectation : autres mesures de protection physique définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle vise la protection contre la divulgation non autorisée d'information. Les éléments complémentaires des messages comprennent notamment l'en-tête des messages ou l'information relative au routage. Cette amélioration de contrôle prévient l'exploitation des éléments complémentaires et s'applique aux réseaux internes et externes ou encore aux liens pouvant être visibles à ceux qui ne sont pas des utilisateurs autorisés. L'information relative aux en-têtes et au routage est parfois transmise non chiffrée en raison du fait que l'information n'est pas adéquatement identifiée comme étant pertinente par les organisations ou parce que le chiffrement de l'information pourrait réduire la performance du réseau ou accroître le coût d'acheminement. Les autres mesures physiques de protection comprennent, par exemple, les systèmes de diffusion protégée. Contrôles connexes : SC-12, SC-13.

(4) CONFIDENTIALITÉ ET INTÉGRITÉ DES TRANSMISSIONS | DISSIMULATION / DISTRIBUTION ALÉATOIRE DES COMMUNICATIONS

Le système d'information applique des mécanismes visant à dissimuler ou à définir aléatoirement les schémas de communication, sauf si l'information est protégée par [*Affectation : autres mesures de protection physique définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle vise la protection contre la divulgation non autorisée d'information. Les schémas de communication comprennent notamment la fréquence, les périodes, les quantités et la prévisibilité. La modification des schémas de communication peut révéler que l'information transmise possède une valeur de renseignement, particulièrement lorsque celle-ci est combinée à d'autres informations disponibles ayant trait aux fonctions de mission/d'opérations soutenues par les systèmes organisationnels d'information. Cette amélioration de contrôle prévient le dévoilement indirect de renseignements fondé sur les schémas de communication et s'applique aux réseaux internes et externes ou encore aux liens pouvant être visibles à ceux qui ne sont pas des utilisateurs autorisés. Grâce au chiffrement des liens et à la transmission en continu, les schémas déterminés/aléatoires empêchent que des renseignements soient tirés d'une déduction faite à partir des schémas de communication. Les autres mesures physiques de protection comprennent, par exemple, les systèmes de diffusion protégée. Contrôles connexes : SC-12, SC-13.

Références :

Aucune

SC-9 CONFIDENTIALITÉ DES TRANSMISSIONS

[Annulé : Intégré au contrôle SC-8(4)]

SC-10 DÉCONNEXION RÉSEAU

Contrôle :

(A) Le système d'information met un terme à toute connexion réseau associée à une session de communications à la fin de la session ou après [*Affectation : durée définie par l'organisation*] d'inactivité.

Conseils supplémentaires : Ce contrôle s'applique aux réseaux internes et externes. L'interruption des connexions réseau associées à une session de communications comprend, par exemple, la libération des paires d'adresses TCP et ports IP au niveau du système d'exploitation, ou la libération des attributions réseau au niveau de l'application, lorsque de multiples sessions d'application utilisent une seule connexion réseau au niveau du système d'exploitation. La durée des périodes d'inactivité peut être établie par les organisations et peut comprendre, par exemple, des durées associées au type d'accès réseau ou à des accès réseau spécifiques.

Améliorations du contrôle :

Aucune

Références :

Aucune

SC-11 CHEMIN DE CONFIANCE

Contrôle :

(A) Le système d'information établit une voie de communication de confiance entre l'utilisateur et les fonctions de sécurité de système suivantes : [*Affectation : fonctions de sécurité définies par l'organisation et incluant, au minimum, l'authentification et la réauthentification du système d'information*].

Conseils supplémentaires sur l'amélioration : Les chemins de confiance sont des mécanismes par lesquels les utilisateurs (par le biais de dispositifs d'entrée) peuvent communiquer directement avec les fonctions de sécurité des systèmes d'information avec l'assurance expresse que les politiques de sécurité de l'information sont respectées. Les mécanismes peuvent être activés seulement par les utilisateurs ou par les fonctions de sécurité des systèmes organisationnels d'information. Les réponses de l'utilisateur acheminées par les chemins de confiance sont protégées contre les divulgations et les modifications non autorisées provoquées par des applications non fiables/au profit d'applications non fiables. Les organisations emploient les chemins de confiance pour les connexions d'assurance élevée entre les fonctions de sécurité des systèmes d'information et les utilisateurs (p. ex. pendant les connexions au système). L'application des voies de communication de confiance est généralement fournie dans le cadre d'une mise en œuvre qui répond au concept de contrôleur de référence. Contrôles connexes : AC-16, AC-25.

Améliorations du contrôle :

(1) CHEMIN DE CONFIANCE | ISOLEMENT LOGIQUE

Le système d'information fournit un chemin de communication de confiance qui est logiquement isolé et distinct des autres chemins.

Références :

Aucune

SC-12 ÉTABLISSEMENT ET GESTION DES CLÉS CRYPTOGRAPHIQUES

Contrôle :

(A) L'organisation établit et gère les clés cryptographiques pour les fonctions de cryptographie requises par le système d'information conformément à [*Affectation : exigences définies par l'organisme en matière de génération, de distribution, de stockage, de disponibilité et de destruction des clés*].

Conseils supplémentaires : L'établissement et la gestion des clés cryptographiques peuvent être effectués au moyen de procédures manuelles ou de mécanismes automatisés soutenus par des procédures manuelles. Les organisations définissent les exigences en matière de gestion des clés conformément aux lois du GC et aux politiques, directives et normes du SCT qui précisent les options, les niveaux et les paramètres à préconiser. Les organisations gèrent les magasins sécurisés (*trust stores*) en veillant à ce que seuls les ancrages de confiance préalablement approuvés se trouvent dans de tels magasins. Cela inclut les certificats disposant d'une visibilité à l'extérieur des systèmes organisationnels d'information et les certificats ayant trait aux systèmes opérationnels internes. La cryptographie doit être conforme aux exigences du contrôle SC-13. Contrôles connexes : SC-13, SC-17.

Améliorations du contrôle :

(1) ÉTABLISSEMENT ET GESTION DES CLÉS CRYPTOGRAPHIQUES | DISPONIBILITÉ

L'organisation maintient la disponibilité de l'information dans l'éventualité où les utilisateurs perdent leurs clés cryptographiques.

Conseils supplémentaires sur l'amélioration : Le séquestre des clés de chiffrement constitue une pratique courante visant à assurer une certaine disponibilité en cas de perte de clés (p. ex. en raison de l'oubli d'une phrase de passe).

(2) ÉTABLISSEMENT ET GESTION DES CLÉS CRYPTOGRAPHIQUES | CLÉS SYMÉTRIQUES

L'organisation produit, contrôle et distribue des clés cryptographiques symétriques à l'aide de technologies et de processus de gestion des clés [*Sélection : conformes aux dispositions du CST; approuvés par le CST*].

(3) ÉTABLISSEMENT ET GESTION DES CLÉS CRYPTOGRAPHIQUES | CLÉS ASYMÉTRIQUES

L'organisation produit, contrôle et distribue des clés cryptographiques asymétriques à l'aide [*Sélection : technologies et processus de gestion des clés approuvés par le CST; certificats d'ICP approuvés d'assurance de niveau moyen ou matériel de chiffrement préplacé; certificats approuvés d'assurance de niveau moyen ou élevé et des jetons de sécurité matériels qui protègent la clé privée de l'utilisateur*].

(4) ÉTABLISSEMENT ET GESTION DES CLÉS CRYPTOGRAPHIQUES | CERTIFICATS ICP

[Annulé : Intégré au contrôle SC-12]

(5) ÉTABLISSEMENT ET GESTION DES CLÉS CRYPTOGRAPHIQUES | CERTIFICATS ICP / JETONS MATÉRIELS

[Annulé : Intégré au contrôle SC-12]

Références :

CST, *ITSA-11, Algorithmes cryptographiques approuvés par le CST pour la protection des renseignements protégés* [Référence 8].
CST, *ITSB-40A, Politique du gouvernement du Canada pour la protection de l'information classifiée à l'aide d'algorithmes Suite B* [Référence 28].
CST, *ITSD-03A, Directive sur le contrôle du matériel COMSEC au sein du gouvernement du Canada* [Référence 36].
CST, *ITSG-13, Manuel sur la commande de clés cryptographiques* [Référence 39].

SC-13 PROTECTION CRYPTOGRAPHIQUE

Contrôle :

(A) Le système d'information applique [*Affectation : usages de la cryptographie et type de cryptographie requis pour chaque usage, tel qu'il est défini par l'organisation*] conformément aux lois applicables du GC ainsi qu'aux politiques, directives et normes applicables du SCT.

Conseils supplémentaires : La cryptographie peut être employée pour soutenir une variété de solutions de sécurité, notamment la protection d'information classifiée et d'information non classifiée contrôlée, la fourniture de signatures numériques, et l'obligation de séparer les informations, lorsque des personnes autorisées disposent des habilitations requises pour l'information en question sans avoir les approbations formelles d'accès nécessaires. La cryptographie peut également servir à soutenir la génération aléatoire de nombres et la génération de hachage. Parmi les normes généralement appliquées en matière de cryptographie, citons la cryptographie homologuée FIPS ainsi que la cryptographie approuvée par le CST. Le présent contrôle ne contraint aucune organisation à utiliser la cryptographie. Cependant, lorsque la cryptographie est exigée en vertu d'autres contrôles ou politiques de sécurité, les organisations documentent chaque type d'usage cryptographique ainsi que les types de cryptographie requis (p. ex. protection d'information classifiée : cryptographie approuvée par le CST; fourniture de signatures numériques : cryptographie homologuée FIPS). Contrôles connexes : AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.

Améliorations du contrôle :

(1) PROTECTION CRYPTOGRAPHIQUE | CRYPTOGRAPHIE HOMOLOGUÉE FIPS

[Annulé : Intégré au contrôle SC-13]

(2) PROTECTION CRYPTOGRAPHIQUE | CRYPTOGRAPHIE APPROUVÉE PAR LA NSA

[Annulé : Intégré au contrôle SC-13]

(3) PROTECTION CRYPTOGRAPHIQUE | PERSONNES NE DISPOSANT PAS DES APPROBATIONS FORMELLES D'ACCÈS

[Annulé : Intégré au contrôle SC-13]

(4) PROTECTION CRYPTOGRAPHIQUE | SIGNATURES NUMÉRIQUES

[Annulé : Intégré au contrôle SC-13]

(100) L'organisation utilise une cryptographie validée par le PVMC pour protéger les données PROTÉGÉ A en transit.

[Annulé : Intégré au contrôle SC-13]

(101) L'organisation utilise une cryptographie validée par le PVMC pour protéger les données PROTÉGÉ B en transit.

[Annulé : Intégré au contrôle SC-13]

(102) L'organisation utilise une cryptographie approuvée par le CST pour protéger les données PROTÉGÉ C en transit.

[Annulé : Intégré au contrôle SC-13]

(103) L'organisation utilise une cryptographie [*Sélection : validée par le PVMC; approuvée par le CST*] pour protéger les [*Sélection : données désignées par l'organisation*] PROTÉGÉ inactives.

[Annulé : Intégré au contrôle SC-13]

(104) L'organisation utilise l'équipement COMSEC conformément aux *Directives pour l'application de la sécurité des communications au sein du gouvernement du Canada (ITSD-01)* du CST [Référence 14].

[Annulé : Intégré au contrôle SC-13]

Références :

CST, *ITSA-11, Algorithmes cryptographiques approuvés par le CST pour la protection des renseignements protégés* [Référence 8].

CST, ITSB-40A, Politique du gouvernement du Canada pour la protection de l'information classifiée à l'aide d'algorithmes Suite B [Référence 28].
CST, ITSD-01A, Directives pour l'application de la sécurité des communications au sein du gouvernement du Canada [Référence 14].

SC-14 PROTECTION DE L'ACCÈS PUBLIC

[Annulé : Capacité fournie par AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, et SI-10]

SC-15 DISPOSITIFS D'INFORMATIQUE COOPÉRATIVE

Contrôle :

(A) Le système d'information interdit l'activation à distance des dispositifs d'informatique coopérative, sauf dans les situations suivantes : [*Affectation : exceptions définies par l'organisation pour lesquelles l'activation à distance doit être permise*].

(B) Le système d'information indique de manière explicite l'utilisation permise de ces dispositifs par les personnes qui se trouvent physiquement à proximité desdits dispositifs.

Conseils supplémentaires : Les dispositifs d'informatique coopérative comprennent, par exemple, les tableaux blancs virtuels, les caméras et les microphones en réseau. L'indication explicite de l'utilisation comprend, par exemple, un signal transmis à l'utilisateur, lorsque le dispositif d'informatique coopérative est activé. Contrôle connexe : AC-21.

Améliorations de contrôle :

(1) DISPOSITIFS D'INFORMATIQUE COOPÉRATIVE | DÉCONNEXION PHYSIQUE

Le système d'information facilite aux utilisateurs la déconnexion physique des dispositifs d'informatique coopérative.

Conseils supplémentaires sur l'amélioration : L'échec de la déconnexion d'un dispositif physique d'informatique coopérative peut ultérieurement occasionner des compromissions d'information organisationnelle. L'application de méthodes simples de déconnexions par rapport à de tels dispositifs après une séance de coopération permet d'assurer que les participants exécutent concrètement la déconnexion sans avoir à suivre des procédures complexes et longues.

(2) DISPOSITIFS D'INFORMATIQUE COOPÉRATIVE | BLOCAGE DU TRAFIC DE COMMUNICATIONS ENTRANT / SORTANT

[Annulé : Intégré au contrôle SC-7]

(3) DISPOSITIFS D'INFORMATIQUE COOPÉRATIVE | DÉSACTIVATION / RETRAIT DANS LES ZONES DE TRAVAIL SÉCURISÉES

L'organisation désactive ou retire les dispositifs d'informatique coopérative de [*Affectation : systèmes d'information ou composants de systèmes d'information désignés par l'organisation*] dans [*Affectation : zones de travail sécurisées définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : La non-désactivation ou le non-retrait de dispositifs d'informatique coopérative des systèmes d'information ou des composants de systèmes d'information peuvent donner lieu à des compromissions d'information organisationnelle, notamment l'écoute illicite de conversations.

(4) DISPOSITIFS D'INFORMATIQUE COOPÉRATIVE | INDICATION EXPLICITE DES PARTICIPANTS

Le système d'information identifie explicitement les participants à [*Affectation : réunions en ligne et téléconférences désignées par l'organisation*].

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle permet d'empêcher les personnes non autorisées de participer à des séances d'informatique coopérative à l'insu des autres participants.

Références :

Aucune

SC-16 TRANSMISSION DES ATTRIBUTS DE SÉCURITÉ

Contrôle :

(A) Le système d'information associe [*Affectation : attributs de sécurité définis par l'organisation*] avec de l'information échangée entre les systèmes d'information et les composants de systèmes d'information.

Conseils supplémentaires : Les attributs de sécurité peuvent être explicitement ou implicitement associés à l'information contenue dans le système d'information ou les composants de systèmes de l'organisation. Contrôles connexes : AC-3, AC-4, AC-16.

Améliorations du contrôle :

(1) TRANSMISSION DES ATTRIBUTS DE SÉCURITÉ | VALIDATION DE L'INTÉGRITÉ

Le système d'information atteste l'intégrité des attributs de sécurité transmis.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle permet de veiller à ce que la vérification de l'intégrité de l'information transmise porte également sur les attributs de sécurité. Contrôles connexes : AU-10, SC-8.

Références :

Aucune

SC-17 CERTIFICATS D'INFRASTRUCTURE À CLÉ PUBLIQUE

Contrôle :

(A) L'organisation émet des certificats à clé publique en vertu de [*Affectation : politique de certification définie par l'organisation*] ou les obtient auprès d'un fournisseur de services autorisé.

Conseils supplémentaires : Pour tous les certificats, les organisations gèrent les magasins sécurisés des systèmes d'information dans le but de veiller à ce que seuls les ancrages approuvés se trouvent dans les magasins sécurisés. Ce contrôle porte sur les certificats disposant d'une visibilité à l'extérieur des systèmes organisationnels d'information et sur les certificats ayant trait aux systèmes opérationnels internes, par exemple, les services de temps propres aux diverses applications. Contrôle connexe : SC-12.

Améliorations de contrôle :

Aucune

Références :

SCT, *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI)* [Référence 74].

SC-18 CODE MOBILE

Contrôle :

(A) L'organisation définit le code mobile et les technologies de code mobile jugés comme acceptables ou inacceptables.

(B) L'organisation définit les restrictions d'utilisation et donne des conseils sur la mise en œuvre du code mobile et des technologies de code mobile acceptables.

(C) L'organisation autorise, surveille et contrôle l'utilisation du code mobile dans le système d'information.

Conseils supplémentaires : Les décisions concernant le recours à du code mobile dans les systèmes d'information organisationnels reposent sur la possibilité qu'une utilisation malveillante du code cause des dommages aux systèmes. Les technologies de code mobile comprennent, par exemple, Java, JavaScript, ActiveX, Postscript, PDF, films Shockwave, animations Flash et VBScript. Les restrictions d'utilisation et les conseils sur la mise en œuvre du code mobile s'appliquent autant à la sélection et à l'utilisation du code mobile installé dans les serveurs qu'à celles du code mobile téléchargé et exécuté dans chacun des postes de travail et des dispositifs (p. ex. téléphones intelligents). La politique et les procédures relatives au code mobile visent à prévenir le développement, l'acquisition ou l'insertion de code mobile inacceptable dans les systèmes organisationnels d'information. Contrôles connexes : AU-2, AU-12, CM-2, CM-6, SI-3.

Améliorations de contrôle :

(1) CODE MOBILE | IDENTIFICATION DU CODE INADÉQUAT / APPLICATION DE MESURES CORRECTIVES

Le système d'information identifie [*Affectation : code mobile inadéquat désigné par l'organisation*] et prend [*Affectation : mesures correctives définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les mesures correctives à prendre lorsque du code mobile inadéquat est détecté comprennent, par exemple, le blocage, la mise en quarantaine ou la notification des administrateurs. Le blocage sert notamment à empêcher la transmission de fichiers de traitement de texte contenant des macros, dès lors que celles-ci ont été jugées comme étant du code mobile inadéquat.

(2) CODE MOBILE | ACQUISITION / DÉVELOPPEMENT / UTILISATION

L'organisation veille à ce que l'acquisition, le développement et l'utilisation de code mobile qui sera déployé dans le système d'information répondent aux [*Affectation : exigences définies par l'organisation concernant le code mobile*].

(3) CODE MOBILE | PRÉVENTION DU TÉLÉCHARGEMENT / EXÉCUTION

Le système d'information empêche le téléchargement et l'exécution de [*Affectation : code mobile inadéquat désigné par l'organisation*].

(4) CODE MOBILE | PRÉVENTION DE L'EXÉCUTION AUTOMATISÉE

Le système d'information empêche l'exécution automatisée de code mobile dans [*Affectation : applications logicielles définies par l'organisation*] et applique [*Affectation : mesures définies par l'organisation*] préalablement à l'exécution du code.

Conseils supplémentaires sur l'amélioration : Les mesures appliquées avant l'exécution du code mobile comprennent, par exemple, l'affichage d'une invite aux utilisateurs avant l'ouverture d'une pièce jointe de courriel. La prévention de l'exécution automatisée comprend notamment la désactivation des fonctions d'exécution automatisée sur les composants de systèmes d'information qui emploient des dispositifs de stockage portatifs comme les disques compacts (CD), les vidéodisques numériques (DVD) et les dispositifs USB.

(5) CODE MOBILE | EXÉCUTION PERMISE SEULEMENT DANS LES LIEUX CLOS

Les organisations n'autorisent l'exécution de code mobile permis que dans les environnements clos de machines virtuelles.

Références :

Aucune

SC-19 VOIX SUR PROTOCOLE INTERNET

Contrôle :

(A) L'organisation définit les restrictions d'utilisation et donne des conseils sur la mise en œuvre des technologies de voix sur protocole Internet (VoIP pour *Voice over Internet Protocol*) en tenant compte de la possibilité qu'une utilisation malveillante de ces technologies cause des dommages au système d'information.

(B) L'organisation autorise, surveille et contrôle l'utilisation de la voix sur IP dans le système d'information.

Conseils supplémentaires : Contrôles connexes : CM-6, SC-7, SC-15.

Améliorations du contrôle :

(100) Il est interdit d'utiliser un service VoIP non classifié dans des installations classifiées, sauf si ce service est converti en service téléphonique ordinaire (STO) avant de quitter la frontière de l'installation.

Conseils supplémentaires sur l'amélioration : La VoIP dans les installations classifiées doit être conforme aux lignes directrices du CNSSI-5000 [Référence 55]. Certains autorisateurs pourraient exiger la conformité aux directives du CNSSI-5000.

(101) Il est interdit d'utiliser, dans une installation classifiée, un service VoIP non classifié dans un réseau local ayant accès à un réseau de données public.

Conseils supplémentaires sur l'amélioration : La VoIP dans les installations classifiées doit être conforme aux lignes directrices du CNSSI-5000 [Référence 55]. Certains autorisateurs pourraient exiger la conformité aux directives du CNSSI-5000.

Références :

CNSSI 5000, *Guidelines For Voice Over Internet Protocol (VoIP) Computer Telephony* [Référence 55].

SC-20 SERVICE SÉCURISÉ DE RÉSOLUTION DE NOM OU D'ADRESSE (SOURCE AUTORISÉE)

Contrôle :

(A) Le système d'information fournit des éléments additionnels d'information sur l'authentification de l'origine et sur la vérification de l'intégrité des données en plus des données de résolution de nom faisant autorité, éléments qu'il retourne en réponse aux requêtes externes de résolution de nom ou d'adresse.

(B) Lorsqu'il est utilisé dans un espace de nom hiérarchique distribué, le système d'information offre des moyens d'indiquer l'état de sécurité des zones enfants et (si l'enfant prend en charge des services sécurisés de résolution) de vérifier l'existence d'une chaîne de confiance entre les domaines parents et enfants.

Conseils supplémentaires : Ce contrôle permet aux clients externes, ce qui comprend, par exemple, les clients à distance provenant d'Internet, d'obtenir des assurances d'authentification de l'origine ou de vérification de l'intégrité pour l'information de résolution de nom d'hôte ou encore de service en adresse réseau obtenue par l'intermédiaire du service. Les systèmes d'information qui fournissent des services de résolution de nom et d'adresse incluent, par exemple, les serveurs de système de nom par domaine (DNS pour *Domain Name System*).

Parmi les artefacts additionnels, notons, par exemple, les signatures numériques et les clés cryptographiques en sécurité des DNS (DNSSEC pour *DNS Security*). Les dossiers de ressources DNS sont des exemples de données faisant autorité. Parmi les moyens d'indiquer l'état de sécurité des zones enfants, citons, par exemple, l'utilisation d'enregistrements de ressource de signataire par délégation du service DNS. Les systèmes d'information qui utilisent des technologies autres que le DNS pour mettre en correspondance les noms d'hôte ou de service et les adresses réseau offrent d'autres moyens d'assurer l'authenticité et l'intégrité des réponses. Contrôles connexes : AU-10, SC-8, SC-12, SC-13, SC-21, SC-22.

Améliorations de contrôle :

(1) SERVICE SÉCURISÉ DE RÉSOLUTION DE NOM / D'ADRESSE (SOURCE AUTORISÉE) | ZONES ENFANTS

[Annulé : Intégré au contrôle SC-20]

(2) SERVICE SÉCURISÉ DE RÉSOLUTION DE NOM / D'ADRESSE (SOURCE AUTORISÉE) | ORIGINE / INTÉGRITÉ DES DONNÉES

Le système d'information fournit des artefacts de protection de l'origine et de l'intégrité des données pour les requêtes en résolution de nom/d'adresse.

Références :

Aucune

SC-21 SERVICE SÉCURISÉ DE RÉSOLUTION DE NOM OU D'ADRESSE (RÉSOLVEUR RÉCURSIF OU CACHE)

Contrôle :

(A) Le système d'information soumet une requête, puis authentifie l'origine et vérifie l'intégrité des données des réponses de résolution de nom et d'adresse qu'il reçoit de sources faisant autorité.

Conseils supplémentaires : Chaque client des services de résolution de nom/d'adresse effectue cette vérification de façon autonome ou par des canaux authentifiés menant à des fournisseurs de validation dignes de confiance. Les systèmes d'information qui fournissent des services de résolution de nom et d'adresse pour les clients locaux incluent, par exemple, les serveurs DNS résolveurs récursifs ou cache. Les résolveurs de clients de DNS exécutent une validation des signatures DNSSEC, ou encore, les clients utilisent des canaux authentifiés vers des résolveurs récursifs qui se chargent de telles validations. Les systèmes d'information qui utilisent des technologies autres que le DNS pour mettre en correspondance les noms d'hôte ou de service et les adresses réseau offrent d'autres moyens d'assurer l'authenticité et l'intégrité des réponses. Contrôles connexes : SC-20, SC-22.

Améliorations de contrôle :

(1) SERVICE SÉCURISÉ DE RÉSOLUTION DE NOM / D'ADRESSE (SOURCE AUTORISÉE) | ORIGINE / INTÉGRITÉ DES DONNÉES

[Annulé : Intégré au contrôle SC-21]

Références :

Aucune

SC-22 ARCHITECTURE ET FOURNITURE DE SERVICES DE RÉSOLUTION DE NOM OU D'ADRESSE

Contrôle :

(A) Les systèmes d'information qui offrent collectivement des services de résolution de nom et d'adresse pour une organisation sont tolérants aux pannes et appliquent une séparation des rôles internes et externes.

Conseils supplémentaires sur l'amélioration : Les systèmes d'information qui fournissent des services de résolution de nom et d'adresse incluent, par exemple, les serveurs de DNS. Pour éliminer les points de défaillance uniques et améliorer la redondance, les organisations emploient au moins deux serveurs de système de noms de domaine faisant autorité dont l'un est configuré comme le serveur principal et l'autre, configuré comme serveur secondaire. De plus, les organisations disposent généralement les serveurs dans deux sous-réseaux faisant respectivement partie de réseaux situés dans des régions géographiques distinctes (p. ex. situés dans des installations physiques différentes). Pour ce qui est de la séparation des rôles, les serveurs DNS associés à des rôles internes exécutent uniquement le processus de résolution de nom et d'adresse pour les requêtes provenant de l'intérieur des organisations (c.-à-d. provenant de clients internes). Les serveurs DNS associés à des rôles externes traitent uniquement les requêtes de résolution des clients à l'extérieur des organisations (c.-à-d. en provenance de réseaux externes, y compris d'Internet). Les organisations désignent les clients qui peuvent accéder aux serveurs DNS faisant autorité dans des rôles particuliers (p. ex. par plage d'adressage ou par des listes explicites). Contrôles connexes : SC-2, SC-20, SC-21, SC-24.

Améliorations de contrôle :

Aucune

Références :

Aucune

SC-23 AUTHENTICITÉ DES SESSIONS

Contrôle :

(A) Le système d'information protège l'authenticité des sessions de transmission.

Conseils supplémentaires : Ce contrôle porte sur la protection des communications au niveau de la session plutôt que des paquets (p. ex. sessions dans des architectures axées sur le service, qui fournissent des services Web) et permet d'instaurer un niveau de confiance adéquat aux deux extrémités des sessions de communication quant à l'identité des autres parties et à la validité de l'information transmise. La protection de l'authenticité peut comprendre, notamment, la protection contre les attaques par interception/les détournements de session ou contre l'insertion d'information erronée dans les sessions. Contrôles connexes : SC-8, SC-10, SC-11.

Améliorations de contrôle :

(1) AUTHENTICITÉ DES SESSIONS | INVALIDER LES IDENTIFICATEURS DE SESSION À LA FERMETURE DES SESSIONS

Le système d'information invalide les identificateurs de session, lorsque l'utilisateur ferme sa session ou lorsque la session s'est terminée autrement.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle réduit la capacité des adversaires à saisir et à poursuivre l'emploi d'identificateurs de session antérieurement valides.

(2) AUTHENTICITÉ DES SESSIONS | FERMETURES DE SESSION EXÉCUTÉES PAR LES UTILISATEURS / AFFICHAGE DE MESSAGES

[Annulée : Intégrée au contrôle AC-12 (1)]

(3) AUTHENTICITÉ DES SESSIONS | IDENTIFICATEURS DE SESSION UNIQUES AVEC RANDOMISATION

Le système d'information génère un identificateur de session unique pour chaque session avec [*Affectation : exigences relatives à la randomisation définies par l'organisation*] et reconnaît uniquement les identificateurs qu'il a générés.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle réduit la capacité des adversaires à réutiliser les identificateurs de session antérieurement valides. L'utilisation du concept aléatoire pour la génération d'identificateurs de session uniques permet de protéger le système contre les attaques de force brute visant à déterminer les futurs identificateurs de session. Contrôle connexe : SC-13.

(4) AUTHENTICITÉ DES SESSIONS | IDENTIFICATEURS DE SESSION UNIQUES AVEC RANDOMISATION

[Annulé : Intégré au contrôle SC-23 (3)]

(5) AUTHENTICITÉ DES SESSIONS | AUTORITÉS DE CERTIFICATION HOMOLOGUÉES

Le système d'information permet uniquement l'utilisation de [*Affectation : autorités de certification désignées par l'organisation*] à des fins de vérification de l'établissement de sessions protégées.

Conseils supplémentaires sur l'amélioration : Le fait de s'en remettre aux autorités de certifications (AC) pour l'établissement de sessions sécurisées entraîne, par exemple, l'utilisation de certificats SSL (*Secure Socket Layer*) ou TLS (*Transport Layer Security*). Après vérification auprès des autorités respectives, ces certificats facilitent l'établissement de sessions protégées entre les clients Web et les serveurs Web. Contrôle connexe : SC-13.

Références :

Aucune

SC-24 DÉFAILLANCE DANS UN ÉTAT CONNU

Contrôle :

(A) Le système d'information tombe à l'état [*Affectation : état connu défini par l'organisation*] pour [*Affectation : types de défaillance définis par l'organisation*] et conserve [*Affectation : information sur l'état du système définie par l'organisation*] durant la défaillance.

Conseils supplémentaires : La défaillance du système dans un état connu met en relief les questions de sécurité conformément à la mission ou aux besoins opérationnels des organisations. La défaillance en milieu sécurisé aide à prévenir les pertes sur le plan de la confidentialité, de l'intégrité ou de la disponibilité dans les cas de défaillance des systèmes organisationnels d'information ou de composants de systèmes. Il permet également d'empêcher les systèmes de tomber en panne dans un état susceptible de causer des préjudices aux personnes ou la destruction des biens. La protection de l'information d'état du système d'information facilite le redémarrage du système et le retour au mode opérationnel des organisations tout en perturbant le moins possible les processus liés à la mission ou aux opérations. Contrôles connexes : CP-2, CP-10, CP-12, SC-7, SC-22.

Améliorations de contrôle :

Aucune

Références :

Aucune

SC-25 NŒUDS LÉGERS

Contrôle :

(A) L'organisation emploie [*Affectation : composants de systèmes d'information désignés par l'organisation*] avec un minimum de fonctionnalités et de stockage d'information.

Conseils supplémentaires : Le déploiement de composants de système d'information ayant une fonctionnalité réduites/minimale (p. ex. nœuds sans disque et technologies de client léger) réduit la nécessité de sécuriser chaque point d'extrémité utilisateur et peut atténuer les risques d'exposition de l'information, des systèmes d'information et des services à des cyberattaques. Contrôle connexe : SC-30.

Améliorations de contrôle :

Aucune

Références :

Aucune

SC-26 PIÈGES À PIRATES

Contrôle :

(A) Le système d'information comporte des composants conçus spécifiquement pour servir de cibles aux attaques malveillantes dans le but de les détecter, de les repousser et de les analyser.

Conseils supplémentaires : Un piège à pirates est conçu comme un leurre visant à attirer les adversaires et à détourner leurs attaques des systèmes opérationnels qui assurent le soutien aux fonctions liées aux missions et aux opérations. Tout dépendant de l'usage particulier du piège à pirates, une discussion préalable avec le Bureau de l'avocat général pourrait être requise. Contrôles connexes : SC-30, SC-44, SI-3, SI-4.

Améliorations de contrôle :

(1) PIÈGES À PIRATES | DÉTECTION DE CODE MALVEILLANT

[Annulé : Intégré au contrôle SC-35]

Références :

Aucune

SC-27 APPLICATIONS INDÉPENDANTES DES PLATEFORMES

Contrôle :

(A) Le système d'information comprend : [*Affectation : applications définies par l'organisation qui sont indépendantes des plateformes*].

Conseils supplémentaires : Les plateformes sont des combinaisons de matériel et de logiciels servant à exécuter des applications logicielles. Les plateformes comprennent : (i) les systèmes d'exploitation; (ii) les architectures informatiques sous-jacentes; (iii) ou les deux. Les applications indépendantes des plateformes peuvent s'exécuter sur diverses plateformes. De telles applications favorisent la portabilité et la reconstitution sur des plateformes différentes, augmentant ainsi la disponibilité des fonctions essentielles au sein des organisations, lorsque des attaques sont lancées contre des systèmes d'information tournant sur des systèmes d'exploitation particuliers. Contrôle connexe : SC-29.

Améliorations de contrôle :

Aucune

Références :

Aucune

SC-28 PROTECTION DE L'INFORMATION INACTIVE

Contrôle :

(A) Le système d'information protège [*Sélection (une ou plusieurs) la confidentialité; l'intégrité*] de [*Affectation : l'information inactive désignée par l'organisation*].

Conseils supplémentaires : Ce contrôle porte sur la confidentialité et l'intégrité de l'information inactive, et concerne l'information relative aux utilisateurs ainsi que l'information relative aux systèmes. L'information inactive renvoie à l'état de l'information lorsqu'elle se trouve dans des dispositifs de stockage à titre de composants particuliers des systèmes d'information. L'information relative aux systèmes nécessitant une protection comprend, notamment, les configurations ou ensembles de règles pour les coupe-feu, les passerelles, les dispositifs mandataires, les systèmes de détection/de prévention des intrusions, les routeurs de filtrage, et le contenu d'authentification. Les organisations pourraient employer divers mécanismes pour assurer la protection de la confidentialité et de l'intégrité, y compris les mécanismes cryptographiques et le balayage des échanges de fichiers. La protection de l'intégrité peut être assurée, par exemple, par la mise en œuvre de technologies WORM (*Write-Once-Read-Many*). Les organisations peuvent également employer d'autres contrôles de sécurité, par exemple, les mémoires autonomes sécurisées au lieu du stockage en ligne – lorsque la protection adéquate de l'information inactive ne peut être assurée autrement – et la surveillance continue visant à identifier le code malveillant inactif. Contrôles connexes : AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7.

Améliorations de contrôle :

(1) PROTECTION DE L'INFORMATION INACTIVE | PROTECTION CRYPTOGRAPHIQUE

Les organisations mettent en œuvre des mécanismes cryptographiques visant à prévenir la divulgation et la modification non autorisées de [*Affectation : information désignée par l'organisation]*.

Conseils supplémentaires sur l'amélioration : La sélection des mécanismes cryptographiques se fonde sur le besoin de protéger la confidentialité et l'intégrité de l'information organisationnelle. La robustesse d'un mécanisme correspond à la catégorie de sécurité et à la classification de l'information. Cette amélioration de contrôle s'applique généralement aux concentrations importantes de médias numériques dans les secteurs organisationnels désignés pour le stockage des médias; elle s'applique également aux qualités plus modestes de médias souvent associées aux composants de systèmes d'information dans les environnements opérationnels (p. ex. dispositifs de stockage portatifs, dispositifs mobiles). Les organisations sont assez souples pour chiffrer toute l'information sur des dispositifs de stockage (p. ex. chiffrement intégral d'un disque) ou encore pour chiffrer des structures particulières de données (p. ex. fichiers, dossiers, champs). Les organisations qui emploient les mécanismes cryptographiques dans le but de protéger l'information inactive envisagent également les solutions de gestion de clés cryptographiques. Contrôles connexes : AC-19, SC-12.

(2) PROTECTION DE L'INFORMATION INACTIVE | STOCKAGE AUTONOME (HORS LIGNE)

L'organisation retire [*Affectation : information désignée par l'organisme*] des dispositifs de stockage en ligne et la transfère vers des modes de stockage hors ligne dans des lieux sécurisés.

Conseils supplémentaires sur l'amélioration : Le retrait de l'information organisationnelle des systèmes de stockage d'information en ligne élimine la possibilité que des individus parviennent à accéder sans autorisation à de l'information par l'intermédiaire d'un réseau. Par conséquent, les organisations peuvent

choisir de déplacer leur information vers des dispositifs de stockage autonomes (hors-ligne) au lieu de la protéger pendant qu'elle est enregistrée dans du stockage en ligne.

Références :

CST, *ITSA-11, Algorithmes cryptographiques approuvés par le CST pour la protection des renseignements protégés* [Référence 8].
CST, *ITSB-40A, Politique du gouvernement du Canada pour la protection de l'information classifiée à l'aide d'algorithmes Suite B* [Référence 28].

SC-29 HÉTÉROGÉNÉITÉ

Contrôle :

(A) L'organisation emploie un ensemble diversifié de technologies de l'information pour [*Affectation : composants de systèmes d'information désignés par l'organisation*] pendant la mise en œuvre du système d'information.

Conseils supplémentaires : Le fait d'accroître la diversité des technologies de l'information au sein d'un système organisationnel d'information réduit l'impact d'éventuelles tentatives d'exploitation au moyen de certaines technologies, et assure une défense contre les défaillances de modes communs, y compris les défaillances découlant d'attaques contre la chaîne d'approvisionnement. La diversité sur le plan des technologies de l'information réduit considérablement la probabilité que les moyens employés par les adversaires pour compromettre un composant de système d'information soit aussi efficace contre d'autres composants de systèmes, ce qui risquerait d'étendre les dommages causés par les cyberattaques. Un accroissement de la diversité peut ajouter en complexité et en charge de gestion, ce qui pourrait ultimement mener à des erreurs ou à des configurations non autorisées. Contrôles connexes : SA-12, SA-14, SC-27.

Améliorations du contrôle :

(1) HÉTÉROGÉNÉITÉ | TECHNIQUES DE VIRTUALISATION

L'organisation utilise des techniques de virtualisation pour faciliter le déploiement de divers systèmes d'exploitation et applications qui sont changés [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les changements fréquents apportés aux systèmes d'exploitation et aux applications posent des défis sur le plan de la gestion des configurations, mais ils ont l'avantage de compliquer la tâche des adversaires qui lancent des cyberattaques. Les changements d'applications ou de systèmes d'exploitation virtuels, par opposition aux changements de véritables applications/systèmes d'exploitation, engendre des changements virtuels qui endiguent l'efficacité des attaques tout en réduisant les efforts de gestion des configurations. De plus, les techniques de virtualisation peuvent aider les organisations à isoler les logiciels non fiables ou de provenance douteuse dans des environnements d'exécution clos.

Références :

Aucune

SC-30 DISSIMULATION ET DÉTOURNEMENT

Contrôle :

(A) L'organisation emploie [*Affectation : techniques de dissimulation et de détournement définies par l'organisation*] pour [*Affectation : systèmes d'information désignés par l'organisation*] à [*Affectation : périodes définies par l'organisation*].

Conseils supplémentaires : Les techniques de dissimulation et de détournement permettent de considérablement réduire la capacité de ciblage des adversaires (p. ex. les créneaux et la surface d'attaque) qui préparent et lancent des cyberattaques. Par exemple, les techniques de virtualisation permettent aux organisations de dissimuler les systèmes d'information et, éventuellement, de réduire la probabilité de réussite des attaques tout en évitant les coûts importants associés à la mise en place de plateformes multiples. L'usage accru des techniques de dissimulation/de détournement, notamment le facteur aléatoire, le facteur d'incertitude ou la virtualisation, peut suffisamment confondre et désorienter les adversaires et, ultérieurement, accroître le risque de découverte ou d'exposition de leur savoir-faire. Les techniques de dissimulation et de détournement peuvent également accroître le temps dont les organisations disposent pour mener à terme les missions et les activités opérationnelles. Considérant le temps et les efforts qu'il faut investir dans les mesures de dissimulation et de détournement, il y a lieu de croire que les organisations utiliseront de telles techniques avec réserve. Contrôles connexes : SC-26, SC-29, SI-14.

Améliorations de contrôle :

(1) DISSIMULATION ET DÉTOURNEMENT | TECHNIQUES DE VIRTUALISATION

[Annulé : Intégré au contrôle SC-29 (1)]

(2) DISSIMULATION ET DÉTOURNEMENT | FACTEUR ALÉATOIRE

L'organisation emploie [*Affectation : techniques désignées par l'organisation*] pour introduire le facteur aléatoire dans la gestion des activités et des actifs organisationnels.

Conseils supplémentaires sur l'amélioration : Le facteur aléatoire introduit un niveau accru d'incertitude dans l'esprit des adversaires relativement aux mesures que les organisations comptent appliquer à des fins de cyberdéfense. En effet, de telles mesures peuvent freiner la capacité des adversaires à cibler correctement les ressources informationnelles des organisations qui assurent le soutien de fonctions essentielles liées aux missions et aux opérations. L'incertitude peut également faire hésiter les adversaires avant de lancer ou de poursuivre des cyberattaques. Les techniques de détournement qui recourent au facteur aléatoire comprennent, par exemple, l'application de pratiques habituelles à divers moments de la journée, l'emploi de diverses technologies de l'information (p. ex. navigateurs, moteurs de recherche), le recours à divers fournisseurs, et la rotation des rôles et des responsabilités au sein du personnel organisationnel.

(3) DISSIMULATION ET DÉTOURNEMENT | TRAITEMENT DES CHANGEMENTS / LIEUX DE STOCKAGE

L'organisation change le lieu de [*Affectation : traitement et/ou stockage désignés par l'organisation*] [*Sélection :* [*Affectation : fréquence définie par l'organisation*]; à intervalles irrégulières]].

Conseils supplémentaires sur l'amélioration : Les adversaires ciblent les fonctions organisationnelles liées aux missions/aux opérations ainsi que les ressources d'information qui sont affectées aux missions et aux fonctions en question, tout en essayant de minimiser l'exposition de leurs activités et de leur savoir-faire. Les systèmes organisationnels d'information qui sont par nature statiques, homogènes et prévisibles prêtent davantage le flanc aux cyberattaques peu coûteuses (financement, efforts) et, malgré tout, efficaces. La modification des lieux de traitement et de stockage organisationnels (parfois appelée défense par déplacement des cibles) prend en compte les menaces persistantes sophistiquées (APT pour *Advanced Persistent Threat*) qui impliquent diverses techniques, notamment la virtualisation, le traitement distribué et la réplication. Cette approche permet aux organisations de relocaliser les ressources d'information (p. ex. traitement ou stockage) servant au soutien des fonctions essentielles aux missions et aux opérations. Les changements de sites de traitement et de stockage sème l'incertitude chez les adversaires quant aux cibles à préconiser pour d'éventuelles cyberattaques. Cette incertitude accroît la somme de travail que les adversaires doivent investir, ce qui rend la compromission et la violation des systèmes organisationnels d'information beaucoup plus difficile et chronophage; ce qui accroît également les chances que ces mêmes adversaires dévoilent accidentellement certains aspects du savoir-faire qu'ils utilisent pour tenter de repérer les ressources organisationnelles essentielles.

(4) DISSIMULATION ET DÉTOURNEMENT | INFORMATION TROMPEUSE

L'organisation emploie de l'information en apparence réelle, mais en définitive trompeuse, dans [*Affectation : composants de systèmes d'information*] au sujet de sa posture et de ses mesures de sécurité.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle sert à tromper d'éventuels adversaires au sujet de la nature et de l'étendue des mécanismes de sécurité déployés par les organisations. De cette façon, les adversaires risquent d'employer des techniques d'attaque inadéquates et, par conséquent, inefficaces. Une autre façon dont les organisations disposent pour tromper les adversaires consiste à placer de l'information erronée au sujet de certains contrôles de sécurité dans les systèmes d'information externes dont on sait qu'ils peuvent être ciblés par les adversaires. En outre, il est tout aussi possible de recourir aux faux réseaux [*deception nets*] (p. ex. les réseaux-pièges, les environnements virtualisés) qui imitent certains aspects des vrais systèmes organisationnels d'information, mais qui utilisent, par exemple, des configurations logicielles périmées.

(5) DISSIMULATION ET DÉTOURNEMENT | DISSIMULATION DES COMPOSANTS DE SYSTÈMES

L'organisation emploie [*Affectation : techniques définies par l'organisation*] pour cacher ou dissimuler [*Affectation : composant de systèmes d'information désignés par l'organisation*].

Conseils supplémentaires sur l'amélioration : Par les mesures visant à cacher, à déguiser, bref à dissimuler les composants des systèmes essentiels d'information, les organisations se donnent les moyens de réduire la probabilité que les adversaires ciblent les actifs organisationnels ou parviennent à les compromettre. Parmi les moyens de dissimulation des composants de systèmes d'information, les organisations pourront recourir notamment à la configuration de routeurs, à l'utilisation de réseaux-pièges ou encore aux techniques de virtualisation.

Références :

Aucune

SC-31 ANALYSE DES VOIES CLANDESTINES

Contrôle :

(A) L'organisation procède à une analyse des voies clandestines dans le but d'identifier les éléments du système d'information qui pourraient éventuellement constituer des voies clandestines de [*Sélection (un ou plusieurs) : stockage; réglage*].

(B) L'organisation évalue la bande passante maximale de ces voies.

Conseils supplémentaires : Les développeurs sont les mieux placés pour déterminer les parties des systèmes qui sont susceptibles d'être converties en voies clandestines. L'analyse des voies clandestines est une activité importante, lorsqu'il y a possibilité que des flux d'information non autorisés traversent des domaines de sécurité comme, par exemple, dans le cas des systèmes d'information qui contiennent de l'information à exportation contrôlée et qui sont connectés à des réseaux externes (c.-à-d. réseaux non contrôlés par les organisations). L'analyse des voies clandestines est également importante pour les systèmes d'information à sécurité multiniveau (MLS pour *Multilevel Secure*), les systèmes à niveau multisécurité (MSL pour *Multiple Security Level*) et les systèmes interdomaines. Contrôles connexes : AC-3, AC-4, PL-2.

Améliorations de contrôle :

(1) ANALYSE DES VOIES CLANDESTINES | TEST D'EXPLOITABILITÉ DES VOIES CLANDESTINES

L'organisation teste un sous-ensemble de voies clandestines identifiées, afin de savoir quelles voient s'avèrent exploitables.

(2) ANALYSE DES VOIES CLANDESTINES | RESTREINDRE LA BANDE PASSANTE MAXIMALE

L'organisation réduit la bande passante maximale pour certaines voies de [*Sélection (un ou plusieurs) : stockage; réglage*] clandestines à [*Affectation : valeurs définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les développeurs de systèmes d'information sont mieux à même de réduire la bande passante maximale pour certaines voies de stockage ou de réglage clandestines.

(3) ANALYSE DES VOIES CLANDESTINES | MESURE DE LA BANDE PASSANTE DANS LES ENVIRONNEMENTS OPÉRATIONNELS

L'organisation mesure la bande passante de [*Affectation : sous-ensemble de voies clandestines particulières défini par l'organisation*] dans l'environnement opérationnel du système d'information.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle porte sur la bande passante des voies clandestines dans les environnements opérationnels en comparaison des environnements de développement. La mesure de la bande passante des voies clandestines dans les environnements opérationnels aide les organisations à établir les quantités d'information qui peuvent fuir clandestinement avant que la fuite ait, en soit, un impact sur les fonctions des missions et des opérations organisationnelles. La bande passante des voies clandestines peut varier considérablement lorsqu'elle est mesurée selon des réglages qui sont indépendants des environnements opérationnels particuliers (p. ex. les laboratoires ou les environnements de développement).

Références :

Aucune

SC-32 PARTITIONNEMENT DES SYSTÈMES D'INFORMATION

Contrôle :

(A) L'organisation partitionne le système d'information [*Affectation : composants de systèmes d'information désignés par l'organisation*] se trouvant dans des domaines ou environnements physiques distincts en fonction de [*Affectation : circonstances propices à la séparation physique des composants définies par l'organisation*].

Conseils supplémentaires : Le partitionnement du système d'information fait partie de la stratégie de protection en profondeur. Les organisations établissent le degré de séparation physique des composants de systèmes, qu'il s'agisse de composants physiquement distincts dans des bâtis distincts d'une même pièce, de composants dans des pièces séparées réservées aux composants ultra-essentiels, ou encore d'une séparation plus importante, à savoir géographique, pour les composants critiques. La catégorisation de sécurité peut également guider la sélection des composants qui se prêtent le mieux au partitionnement de domaine. Les interfaces gérées limitent ou interdisent l'accès réseau et les flux d'information entre les composants partitionnés du système d'information. Contrôles connexes : AC-4, SA-8, SC-2, SC-3, SC-7.

Améliorations de contrôle :

Aucune

Références :

Aucune

SC-33 INTÉGRITÉ DE LA PRÉPARATION DES TRANSMISSIONS

[Annulé : Intégré au contrôle SC-8]

SC-34 PROGRAMMES EXÉCUTABLES NON MODIFIABLES

Contrôle :

(A) Le système d'information, au niveau de [*Affectation : composants de système d'information définies par l'organisation*], charge et exécute l'environnement d'exploitation à partir de supports non inscriptibles mis en œuvre par matériel.

(B) Le système d'information, au niveau de [*Affectation : composants de système d'information définis par l'organisation*], charge et exécute [*Affectation : applications définies par l'organisation*] à partir de supports non inscriptibles mis en œuvre par matériel.

Conseils supplémentaires : Le terme « environnement d'exploitation » désigne le code particulier qui héberge les applications, par exemple, les systèmes d'exploitation, les outils de gestion, ou les moniteurs, y compris les moniteurs de machines virtuelles (p. ex. les hyperviseurs). Il peut également renvoyer à certaines applications s'exécutant directement sur des plateformes matérielles. Les supports non inscriptibles mis en œuvre par matériel comprennent, par exemple, le disque compact enregistrable (CD-R pour *Compact Disc Recordable*) ou le vidéodisque numérique inscriptible (DVD-R pour *Digital Video Disk-Recordable*) ainsi que la mémoire morte programmable une seule fois. L'utilisation du stockage non modifiable garantit l'intégrité de l'aspect logiciel à partir du point de création de l'image en lecture seule. L'utilisation de mémoire morte reprogrammable peut être acceptée comme support non inscriptible pourvu que (i) l'intégrité puisse être adéquatement protégée depuis le point de l'inscription initiale jusqu'à l'insertion de la mémoire dans le système d'information; (ii) et qu'il y ait des mécanismes fiables de protection du matériel contre la reprogrammation de la mémoire tant que celle-ci est installée dans les systèmes organisationnels d'information. Contrôles connexes : AC-3, SI-7.

Améliorations de contrôle :

(1) PROGRAMMES EXÉCUTABLES NON MODIFIABLES | ABSENCE DE STOCKAGE INSCRIPTIBLE

L'organisation utilise [*Affectation : composants de système d'information définis par l'organisation*] avec des dispositifs de stockage qui demeurent non inscriptibles à chaque redémarrage du composant ou lors des mises sous tension et hors tension.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle (i) élimine la possibilité d'insertion de code malveillant par une mémoire inscriptible persistante dans le composant de système d'information désigné; (ii) et s'applique aux mémoires de stockage fixes et amovibles, celles-ci étant utilisées directement ou selon les restrictions imposées par les contrôles d'accès des dispositifs mobiles. Contrôles connexes : AC-19, MP-7.

(2) PROGRAMMES EXÉCUTABLES NON MODIFIABLES | PROTECTION DE L'INTÉGRITÉ / SUPPORTS NON INSCRIPTIBLES

L'organisation protège l'intégrité de l'information avant le stockage sur des supports non inscriptibles et contrôle les supports après que ladite information a été enregistrée sur le support en question.

Conseils supplémentaires sur l'amélioration : Les mécanismes de protection préviennent la substitution de supports dans les systèmes d'information ou empêchent la reprogrammation de supports non inscriptibles programmables avant leur installation dans les systèmes. Les mécanismes de protection comprennent, par exemple, une combinaison de prévention, de détection et de réaction. Contrôles connexes : AC-5, CM-3, CM-5, CM-9, MP-2, MP-4, MP-5, SA-12, SC-28, SI-3.

(3) PROGRAMMES EXÉCUTABLES NON MODIFIABLES | PROTECTION MATÉRIELLE

(a) L'organisation la protection d'écriture matérielle pour [*Affectation : composants microgiciels de systèmes d'information désignés par l'organisation*].

(b) L'organisation applique des procédures particulières pour que [*Affectation : personnes autorisées désignées par l'organisation*] désactive manuellement la protection d'écriture matérielle aux fins de

modification de microgiciels, puis réactive la protection d'écriture avant de revenir au mode opérationnel.

Références :

Aucune

SC-35 CLIENTS-LEURRES

Contrôle :

(A) Le système d'information comprend des composants qui tentent proactivement d'identifier tout site Web malveillant et tout code malveillant en provenance du Web.

Conseils supplémentaires : Les clients-leurres (*honeyclients*) diffèrent des pièges à pirates (*honeypots*) par le fait que les composants sondent constamment l'Internet à la recherche de code malveillant (p. ex. vers) contenus dans les sites Web externes. Tout comme pour les pièges à pirates, les clients-leurres nécessitent des mesures d'isolement (p. ex. la virtualisation) pour veiller à ce que tout code malveillant découvert pendant la recherche et exécuté ultérieurement n'infecte pas les systèmes organisationnels d'information. Contrôles connexes : SC-26, SC-44, SI-3, SI-4.

Améliorations de contrôle :

Aucune

Références :

Aucune

SC-36 TRAITEMENT ET STOCKAGE RÉPARTIS

Contrôle :

(A) L'organisation répartit [*Affectation : traitement et stockage définis par l'organisation*] dans plusieurs lieux physiques.

Conseils supplémentaires : La répartition du traitement et du stockage dans plusieurs lieux physiques offre un certain degré de redondance ou de chevauchement pour les organisations et, par conséquent, accroit la somme de travail des adversaires qui cherchent à produire un effet négatif sur les opérations, les actifs ou les personnes de l'organisation. Ce contrôle ne se fonde pas sur un lieu central de traitement ou de stockage, mais permet plutôt le traitement et le stockage parallèles. Contrôles connexes : CP-6, CP-7.

Améliorations de contrôle :

(1) TRAITEMENT ET STOCKAGE RÉPARTIS | TECHNIQUES DE SCRUTATION

L'organisation emploie des techniques d'interrogation visant à identifier d'éventuelles anomalies, erreurs ou compromissions [*Affectation : Composants de traitement et de stockage distribués désignés par l'organisation*].

Conseils supplémentaires sur l'amélioration : Le traitement et le stockage distribués peuvent servir à réduire la possibilité que des adversaires arrivent à compromettre la confidentialité, l'intégrité ou la disponibilité de l'information et des systèmes d'information. Cependant, les composants de traitement et de stockage distribués ne peuvent empêcher que des adversaires compromettent un ou plusieurs des composants répartis. L'interrogation permet de comparer les résultats de traitement aux contenus de stockage des divers composants distribués, puis de s'assurer qu'ils s'accordent. L'interrogation permet

d'identifier les anomalies, les erreurs et les compromissions dans les composants de traitement et de stockage distribués. Contrôle connexe : SI-4.

Références :

Aucune

SC-37 VOIES DE D'ACHEMINEMENT HORS BANDE

Contrôle :

(A) L'organisation emploie [*Affectation : voies d'acheminement hors bande désignées par l'organisation*] pour la distribution physique ou la transmission électronique de [*Affectation : information, composants de systèmes d'information ou dispositifs désignés par l'organisation*] à [*Affectation : personnes ou systèmes d'information désignés par l'organisation*].

Conseils supplémentaires : Les voies de transmission hors bonde comprennent notamment les accès locaux (non réseau) aux systèmes d'information, les chemins réseaux qui sont physiquement séparés des chemins réseaux utilisés pour le trafic opérationnel ou les chemins non électroniques comme Canada Post. Cette approche se distingue de l'utilisation des voies semblables (p. ex. les voies intrabandes) qui servent au transport du trafic opérationnel courant. Les voies hors bandes ne comportent pas la même vulnérabilité/exposition que les voies intrabandes, ce qui permet de conclure que la compromission de la confidentialité, de l'intégrité et de la disponibilité des voies intrabandes n'aura pas d'effet aversif sur les voies hors bande. Les organisations peuvent employer les voies hors bande pour la distribution ou la transmission de nombreux éléments organisationnels, par exemple, les identifiants/les authentifiants; les changements de configuration relatifs au matériel, aux microgiciels ou aux logiciels; l'information concernant la gestion des clés de chiffrement; les mises à jour de sécurité; la sauvegarde des systèmes/des données; l'information sur la maintenance; et les mises à jour concernant la protection contre le code malveillant. Contrôles connexes : AC-2, CM-3, CM-5, CM-7, IA-4, IA-5, MA-4, SC-12, SI-3, SI-4, SI-7.

Améliorations de contrôle :

(1) VOIES D'ACHEMINEMENT HORS BANDE | GARANTIR LA DISTRIBUTION / TRANSMISSION

L'organisation emploie [*Affectation : mécanismes de protection désignés par l'organisation*] de façon à ce que seulement [*Affectation : personnes ou systèmes d'information désignés par l'organisation*] reçoivent [*Affectation : information, composants de systèmes d'information ou dispositifs*].

Conseils supplémentaires sur l'amélioration : Parmi les techniques ou les méthodes qui permettent aux organisations de veiller à ce que seuls certains systèmes d'information ou certaines personnes reçoivent des informations, des composants de systèmes d'information ou des dispositifs particuliers, citons, par exemple, l'envoi d'authentifiants par service de messagerie tout en exigeant que le destinataire produise une pièce d'identité avec photo délivrée par le gouvernement en guise de condition à la réception.

Références :

Aucune

SC-38 SÉCURITÉ DES OPÉRATIONS

Contrôle :

(A) L'organisation emploie [*Affectation : mécanismes de protection des opérations désignés par l'organisation*] pour protéger l'information organisationnelle essentielle pendant la durée des cycles de développement de systèmes.

Conseils supplémentaires : La sécurité des opérations (OPSEC) est un processus systématique par lequel il est possible d'empêcher d'éventuels adversaires d'accéder aux informations concernant les capacités et les intentions des organisations, et ce, par l'identification, le contrôle et la protection d'information généralement non classifiée portant spécifiquement sur la planification et l'exécution des activités organisationnelles de nature sensible. Le processus OPSEC en question comporte cinq étapes : (i) identification de l'information essentielle (p. ex. le processus de catégorisation de sécurité); (ii) analyse des menaces; (iii) analyse des vulnérabilités; (iv) évaluation des risques; (v) et application des mesures de prévention appropriées. Les mécanismes de protection OPSEC s'appliquent à l'organisation tout autant qu'aux systèmes organisationnels d'information ou aux environnements dans lesquels les systèmes sont utilisés. Les mécanismes de protection OPSEC aident à protéger la confidentialité d'informations essentielles, notamment les restrictions relatives aux échanges d'information avec d'actuels ou éventuels fournisseurs de composants de systèmes d'information, et de produits et services de technologie de l'information ou encore avec d'autres intervenants non organisationnels. Parmi les exemples d'information essentielle aux missions/aux opérations, citons, par exemple, les identifiants d'utilisateurs, l'utilisation de certains éléments, les fournisseurs, les processus relatifs à la chaîne d'approvisionnement, les exigences concernant les fonctions et la sécurité, les spécifications de conception des systèmes, les protocoles de tests, ainsi que les détails concernant la mise en œuvre de contrôles de sécurité. Contrôles connexes : RA-2, RA-5, SA-12.

Améliorations de contrôle :

Aucune

Références :

Aucune

SC-39 ISOLEMENT DES PROCESSUS

Contrôle :

(A) Le système d'information maintient un domaine d'exécution distinct pour chaque processus exécuté.

Conseils supplémentaires : Les systèmes d'information peuvent conserver des domaines d'exécution distincts pour chacun des processus d'exécution en attribuant un espace d'adressage à chacun de ces processus. Chaque processus de système d'information dispose de son espace d'adressage de sorte que la communication entre les processus s'effectue de manière contrôlée par le biais des fonctions de sécurité, ce qui empêche également qu'un processus en vienne à modifier le code d'exécution d'un autre processus. La conservation de domaines distincts pour l'exécution des processus est rendue possible grâce, notamment, à l'application d'espaces d'adressage distincts. Cette capacité est disponible dans la plupart des systèmes d'exploitation commerciaux qui emploient les technologies de traitement multiple. Contrôles connexes : AC-3, AC-4, AC-6, SA-4, SA-5, SA-8, SC-2, SC-3.

Améliorations de contrôle :

(1) ISOLEMENT DES PROCESSUS | SÉPARATION DU MATÉRIEL

Le système d'information recoure à des mécanismes sous-jacents de séparation matérielle pour faciliter la séparation des processus.

Conseils supplémentaires sur l'amélioration : La séparation matérielle des processus de systèmes d'information est généralement moins sujette à la compromission que la séparation logicielle, ce qui donne l'assurance que la séparation sera efficace. Parmi les mécanismes sous-jacents de séparation matérielle, citons, par exemple, la gestion matérielle de la mémoire.

(2) ISOLEMENT DES PROCESSUS | ISOLEMENT DES FILS D'EXÉCUTION

Le système d'information conserve un domaine d'exécution pour chacun des fils d'exécution dans [*Affectation : traitement multifils défini par l'organisation*].

Références :

Aucune

SC-40 PROTECTION DES LIAISONS SANS FIL

Contrôle :

(A) Le système d'information protège [*Affectation : liaisons sans fil désignées par l'organisation*] internes et externes contre [*Affectation : types d'attaques de paramètres de signaux ou références aux sources de telles attaques, tel qu'il a été défini par l'organisation*].

Conseils supplémentaires : Ce contrôle s'applique aux liaisons de communication internes et externes qui pourraient être visibles pour les personnes qui ne sont pas des utilisateurs autorisés des systèmes d'information. Les adversaires peuvent exploiter les paramètres de signaux des liaisons sans fil, lorsque ceux-ci ne sont pas adéquatement protégés. Il existe de nombreuses façons d'exploiter les paramètres de signaux de liaisons sans fil, dans le but de soutirer du renseignement, d'interrompre des services ou d'usurper l'identité d'utilisateurs des systèmes organisationnels d'information. Le présent contrôle atténue l'impact des attaques qui visent principalement les systèmes sans fil. Il pourrait être impossible d'appliquer le présent contrôle, lorsque les organisations comptent sur des fournisseurs de services commerciaux pour des services de transmission considérés comme des auxiliaires plutôt que comme des services affectés en propre. Contrôles connexes : AC-18, SC-5.

Améliorations de contrôle :

(1) PROTECTION DES LIAISONS SANS FIL | INTERFÉRENCE ÉLECTROMAGNÉTIQUE

Le système d'information met en œuvre des mécanismes cryptographiques visant à appliquer [*Affectation : niveau de protection définit par l'organisation*] dans le but de contrer les effets de l'interférence électromagnétique internationale.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle assure une protection contre le brouillage intentionnel qui pourrait entraver ou gêner les communications, de sorte que les formes d'onde à spectre étalé pour le sans fil qui servent à la protection antibrouillage ne sont pas prévisibles pour les personnes non autorisées. L'amélioration de contrôle pourrait incidemment contribuer à l'atténuation du brouillage accidentel causé par les transmetteurs légitimes qui partagent le même spectre. Les exigences des missions, les menaces anticipées, les concepts d'opération, de même que les lois, directives, règlements, politiques, normes et lignes directrices applicables servent à établir les niveaux de disponibilité des liaisons sans fil ainsi que les besoins en matière de rendement et de cryptographie. Contrôles connexes : SC-12, SC-13.

(2) PROTECTION DES LIAISONS SANS FIL | ATTÉNUATION DU POTENTIEL DE DÉTECTION

Le système d'information applique des mécanismes cryptographiques visant à réduire le potentiel de détection des liaisons sans fil [*Affectation : niveau de réduction défini par l'organisation*].

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle est nécessaire aux communications secrètes et à la protection des émetteurs sans fil contre la géolocalisation résultant de la transmission. La présente amélioration de contrôle veille à ce que les formes d'ondes à spectre étalé, qui sont utilisées pour garantir une faible probabilité de détection, ne soient pas prévisibles pour des personnes non autorisées. Les exigences des missions, les menaces anticipées, les concepts d'opération, de même que les lois, directives, règlements, politiques, normes et lignes directrices applicables servent à établir les niveaux d'indétectabilité des liaisons sans fil. Contrôles connexes : SC-12, SC-13.

(3) PROTECTION DES LIAISONS SANS FIL | DÉCEPTION PAR IMITATION OU PAR MANIPULATION

Le système d'information applique des mécanismes cryptographiques visant à identifier et à rejeter les transmissions sans fil qui constituent des tentatives délibérées de communication trompeuses par imitation ou par manipulation, qui sont fondées sur des paramètres de signaux.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle permet de garantir que les paramètres de signaux de transmissions sans fil ne sont pas prévisibles pour les personnes non autorisées. La non-prévisibilité réduit les risques d'occurrence des communications trompeuses par imitation ou par manipulation fondées sur les seuls paramètres de signaux. Contrôles connexes : SC-12, SC-13.

(4) PROTECTION DES LIAISONS SANS FIL | IDENTIFICATION DES PARAMÈTRES DE SIGNAUX

Le système d'information applique des mécanismes visant à prévenir l'identification des [*Affectation : émetteurs sans fil désignés par l'organisation*] par l'utilisation des paramètres de signaux de d'un émetteur.

Conseils supplémentaires sur l'amélioration : Les techniques de signature d'émetteurs radioélectriques permettent d'identifier les paramètres propres à un signal d'émetteur dans le but d'établir la signature desdits émetteurs à des fins de surveillance et d'identification des missions ou des utilisateurs. La présente amélioration de contrôle permet d'assurer une protection contre l'identification de l'unicité des émetteurs sans fil à des fins d'exploitation du renseignement, et ce, en assurant que les modifications « anti-signature » apportées aux paramètres de signaux ne sont pas prévisibles pour les personnes non autorisées. La présente amélioration de contrôle permet d'assurer la réussite de la mission dès lors que l'anonymat est requis. Contrôles connexes : SC-12, SC-13.

Références :

Aucune

SC-41 ACCÈS AUX PORTS ET AUX DISPOSITIFS D'E/S

Contrôle :

(A) L'organisation procède à une désactivation physique ou au retrait de [*Affectation : ports de connexion ou dispositifs d'entrée/de sortie désignés par l'organisation*] sur [*Affectation : systèmes d'information ou composants de systèmes d'information désignés par l'organisation*].

Conseils supplémentaires : Les ports de connexion comprennent, par exemple, les ports USB (*Universal Serial Bus*) et Firewire (IEEE-1394). Parmi les dispositifs d'entrée/de sortie, citons, par exemple, les lecteurs de disques compacts (CD) et de vidéodisques numériques (DVD). La désactivation physique ou le retrait de tels ports de connexion ou dispositifs E/S aide à prévenir l'exfiltration de renseignements contenus dans les systèmes d'information ainsi qu'à empêcher l'introduction de code malveillant dans les systèmes de ces ports et de ces dispositifs.

Améliorations de contrôle :

Aucune

Références :

Aucune

SC-42 CAPACITÉ DE CAPTATION ET DONNÉES

Contrôle :

(A) Le système d'information interdit l'activation à distance des capacités de captation environnementale, sauf dans les situations suivantes : [*Affectation : exceptions définies par l'organisation pour lesquelles l'activation à distance de capteurs est permise*].

(B) Le système d'information indique explicitement l'utilisation de capteurs pour [*Affectation : classes d'utilisateurs définies par l'organisation*].

Conseils supplémentaires : Le présent contrôle s'applique aux types de systèmes d'information ou de composants de systèmes d'information constituant des dispositifs mobiles, par exemple, les téléphones intelligents, les tablettes électroniques et les liseuses. Ces systèmes comprennent souvent des capteurs capables de collecter et d'enregistrer des données relatives à l'environnement où les systèmes sont utilisés. Les capteurs sont souvent intégrés aux dispositifs mobiles, par exemple, les appareils photo, les microphones, les récepteurs de système mondial de localisation (GPS pour *Global Positioning System*) et les accéléromètres. Même si les capteurs constituent d'importantes fonctionnalités des dispositifs mobiles, ceux-ci, lorsqu'ils sont activés furtivement, peuvent servir aux adversaires comme moyen de tirer de précieuses informations sur les personnes et sur les organisations. Par exemple, l'activation à distance de la fonction de GPS d'un dispositif mobile pourrait permettre à un adversaire de surveiller les mouvements d'une personne.

Améliorations de contrôle :

(1) CAPACITÉ DE CAPTATION ET DONNÉES | SIGNALEMENT AUPRÈS DES PERSONNES OU DES RÔLES AUTORISÉS

L'organisation veille à ce que le système d'information soit configuré de telle sorte que les données ou les informations collectées par [*Affectation : capteurs désignés par l'organisation*] ne soit signalées qu'aux personnes ou aux rôles autorisés à cette fin.

Conseils supplémentaires sur l'amélioration : Dans les situations où les capteurs sont activés par des personnes autorisées (p. ex. utilisateurs terminaux), il demeure malgré tout possible que l'information/les données collectées par les capteurs soient acheminées à des entités non autorisées.

(2) CAPACITÉ DE CAPTATION ET DONNÉES | UTILISATION AUTORISÉE

L'organisation emploie les mesures suivantes : [*Affectation : mesures définies par l'organisme*], pour que les données ou les informations collectées par [*Affectation : capteurs désignés par l'organisation*] ne soient utilisées que pour les fins autorisées.

Conseils supplémentaires sur l'amélioration : Les informations collectées par les capteurs pour une fin particulière pourraient éventuellement être utilisée à des fins non autorisées. Par exemple, les capteurs GPS qui servent normalement à assurer le soutien à l'orientation du trafic pourraient être exploités par des adversaires qui cherchent à surveiller les déplacements de personnes. Parmi les mesures visant à atténuer de telles activités, citons en exemple les formations additionnelles permettant d'assurer que les entités autorisées n'abusent pas de leurs pouvoirs (dans les cas où les données/les informations collectées par les capteurs sont maintenues par des entités externes) ou encore les restrictions contractuelles concernant l'utilisation de l'information/des données.

(3) CAPACITÉ DE CAPTATION ET DONNÉES | DISPOSITIFS INTERDITS D'UTILISATION

L'organisation interdit l'utilisation de dispositifs dotés de [*Affectation : capacités de captation environnementale*] dans [*Affectation : installations, secteurs ou systèmes désignés par l'organisation*].

Conseils supplémentaires sur l'amélioration : Par exemple, les organisations pourraient interdire aux personnes d'apporter des téléphones portables ou des appareils photo numériques dans l'enceinte de certaines installations ou dans certains secteurs contrôlés qui font partie d'installations servant au stockage d'information classifiée ou qui sont le lieux de conversations sur des sujets sensibles.

Références :

Aucune

SC-43 RESTRICTIONS CONCERNANT L'UTILISATION

Contrôle :

(A) L'organisation définit les restrictions d'utilisation et donne des conseils concernant [*Affectation : composants de systèmes d'information désignés par l'organisation*] en tenant compte de la possibilité qu'une utilisation malveillante de ces technologies cause des dommages au système d'information.

(B) L'organisation autorise, surveille et contrôle l'utilisation de ces composants dans le système d'information.

Conseils supplémentaires : Parmi les composants de systèmes d'information, citons notamment les composants matériels, logiciels ou microgiciels (p. ex. le protocole de la voix sur IP, le code mobile, les photocopieurs numériques, les imprimantes, les numériseurs, les dispositifs optiques, les technologies sans fil et les dispositifs mobiles). Contrôles connexes : CM-6 et SC-7.

Améliorations de contrôle :

Aucune

Références :

Aucune

SC-44 CHAMBRES DE DÉTONATION

Contrôle :

(A) L'organisation emploie une chambre de détonation (*detonation chamber*) dans [*Affectation : système d'information, composant de système ou lieu*].

Conseils supplémentaires : Les chambres de détonation, aussi appelées « environnements d'exécution dynamiques », permettent aux organisations d'ouvrir des fichiers joints à des courriels, d'exécuter des applications douteuses ou suspectes, ou encore d'exécuter des requêtes URL (*Universal Resource Locator*) dans un environnement sûr et isolé ou dans des bacs à sable virtuels. Ces environnements d'exécution protégés et isolés offrent les moyens d'établir si les fichiers joints ou les applications en question contiennent du code malveillant. Bien qu'il soit lié au concept des réseaux-leurres (*deception nets*), le contrôle n'est pas destiné à maintenir un environnement à long terme dans lequel des adversaires peuvent s'exécuter tout en étant surveillés. Il s'agit plutôt d'identifier rapidement le code malveillant et de réduire la probabilité que le code en question se propage aux environnements opérationnels (voire d'empêcher radicalement de telles propagations). Contrôles connexes : SC-7, SC-25, SC-26, SC-30.

Améliorations de contrôle :

Aucune

Références :

CST, ITSB-89 Version 3, *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information du gouvernement du Canada* [Référence 66].

SC-100 AUTHENTIFICATION DE LA SOURCE

Contrôle :

(A) Le système d'information permet au destinataire d'un message de vérifier l'identificateur présumé de la source dans un message.

Conseils supplémentaires : L'authentification de la source empêche toute partie non autorisée d'envoyer un message en usurpant l'identité de quelqu'un d'autre. Ce contrôle s'applique aux communications non liées à une session et peut être appliqué aux protocoles de n'importe quelle couche, des paquets IP au courrier électronique. Contrôles connexes : IA-1, IA-2, IA-3, IA-4, IA-5, SC-8, SC-13.

Améliorations de contrôle :

(1) L'authentification de l'identifiant présumé du message repose sur la cryptographie.

(2) L'organisation utilise la cryptographie validée par le PVMC pour la génération et la vérification des signatures numériques. Voir le contrôle SC-13.

(3) L'organisation utilise la cryptographie et les protocoles approuvés par le CST pour effectuer l'authentification. Voir le contrôle SC-13.

Références :

Aucune

SC-101 SYSTÈMES DE TÉLÉCOMMUNICATIONS NON CLASSIFIÉS DANS LES INSTALLATIONS SÉCURISÉES

Contrôle :

(A) Les systèmes de télécommunications non classifiés dans les installations sécurisées ne doivent ni laisser passer ni transmettre de discussions audio sensibles lorsqu'ils sont au repos et non utilisés. En plus, ils doivent être configurés de manière à en empêcher le contrôle ou l'activation externe. Les concepts de protection audio de type « combiné raccroché » mentionnés dans les publications *Committee on National Security Systems Instructions* (CNSSI 5002 et CNSSI 5006) du Committee on National Security Systems doivent être intégrés aux systèmes de télécommunications des installations sécurisées.

(B) Les systèmes et services téléphoniques non classifiés doivent être configurés de manière à empêcher les exploits techniques ou la pénétration. De plus, ils doivent intégrer des contrôles d'accès physique et logiciels pour empêcher la divulgation ou la manipulation de la programmation système et des données stockées.

(C) L'organisation doit veiller à appliquer aux systèmes de télécommunications non classifiés les exigences particulières suivantes.

(a) Assurer la protection audio de type « combiné raccroché » par l'utilisation d'équipement CNSSI 5006, de dispositifs de déconnexion approuvés CNSSI 5006, ou d'une configuration système CNSSI 5002 équivalente.

(b) Assurer l'isolement par l'utilisation d'un système téléphonique informatisé doté d'un contrôle de configuration logicielle et matérielle, et d'un contrôle des rapports de vérification (enregistrement détaillé des données d'appel, rapports sur les données d'appel, etc.). La programmation système n'offre pas la capacité de placer ou de maintenir le combiné en position non raccrochée. La configuration du système doit faire en sorte d'identifier et d'atténuer toutes les vulnérabilités associées à l'état du combiné (raccroché ou non).

(c) Veiller à ce que l'équipement utilisé pour administrer les systèmes téléphoniques soit installé dans une zone dont l'accès est réservé au personnel autorisé. Lorsque les terminaux d'administration locaux (d'un système téléphonique informatisé) ne sont pas ou ne peuvent pas être hébergés dans la zone contrôlée, ni protégés contre les manipulations non autorisées, alors l'utilisation d'un équipement téléphonique approuvé CNSSI 5006 doit être exigée, quelle que soit la configuration du système téléphonique informatisé.

(d) Veiller à ne pas recourir à la maintenance à distance, en dehors de l'installation sécurisée.

(e) Veiller à ne pas utiliser de téléphones à haut-parleur ni de systèmes d'audioconférences avec les systèmes de télécommunications non classifiés dans les installations sécurisées. Les exceptions à cette exigence peuvent être approuvées par le CST dans le cas où il y a une isolation audio suffisante entre ces systèmes et les autres pièces de discussion classifiée dans l'installation sécurisée et lorsqu'il existe des procédures pour empêcher la transmission par inadvertance d'information classifiée.

(f) Veiller à ce que les fonctions utilisées pour la messagerie vocale ou les systèmes unifiés de messagerie soient configurées de manière à empêcher l'accès non autorisé aux ports de diagnostic distants ou à la tonalité d'invitation à numéroter interne.

(g) Veiller à ce que les répondeurs téléphoniques (TAD) et les télécopieurs ne comportent pas de fonctions qui présentent des vulnérabilités au plan de la sécurité, p. ex. surveillance des locaux à distance, programmation à distance, ou autres fonctions similaires qui peuvent permettre un accès à distance aux sons de la pièce. Le CST doit donner son approbation avant l'installation ou l'utilisation de tels dispositifs.

(D) Tous les systèmes de télécommunications non classifiés et leurs infrastructures doivent être isolés physiquement et électriquement de tout système d'information ou de télécommunications classifié, conformément aux exigences du Committee on National Security Systems ou de toute autre norme de séparation appliquée au système d'information classifié en place.

(E) Il faut respecter les exigences de sécurité et les lignes directrices en matière d'installation données dans la publication CNSSI 5000 du Committee on National Security Systems pour les systèmes de téléphonie sur IP (VoIP) installés dans toute zone de sécurité physique où est traitée de l'information classifiée.

Conseils supplémentaires : Une installation sécurisée est toute zone de sécurité physique où l'on traite de l'information classifiée. Une installation sécurisée peut désigner une installation renfermant des informations sensibles cloisonnées (SCIF) au niveau TRÈS SECRET, ou toute autre installation sécurisée à un niveau inférieur (p. ex. SECRET, CONFIDENTIEL).

Améliorations de contrôle :

Aucune

Références :

CNSSI 5000, *Guidelines For Voice Over Internet Protocol (VoIP) Computer Telephony* [Référence 55].
CNSSI 5002, *National Information Assurance (IA) Instruction for Computerized Telephone Systems*. [Référence 59].
CNSSI 5006, *National Instruction for Approved Telephone Equipment*. [Référence 56].

3.17 FAMILLE : INTÉGRITÉ DE L'INFORMATION ET DES SYSTÈMES

CLASSE : OPÉRATIONNELLE

SI-1 POLITIQUE ET PROCÉDURES LIÉES À L'INTÉGRITÉ DE L'INFORMATION ET DES SYSTÈMES

Contrôle :

(A) L'organisation élabore, consigne et diffuse aux [*Affectation : personnel ou rôles définis par l'organisation*] :

(a) une politique d'intégrité des systèmes et de l'information qui définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité;

(b) des procédures visant à faciliter la mise en œuvre de la politique d'intégrité des systèmes et de l'information et des contrôles connexes d'intégrité des systèmes et de l'information.

(B) L'organisation examine et met à jour :

(a) la politique d'intégrité des systèmes et de l'information actuelle [*Affectation : fréquence définie par l'organisation*];

(b) les procédures d'intégrité des systèmes et de l'information [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : Ce contrôle porte sur l'établissement de la politique et les procédures nécessaires à la mise en œuvre efficace des contrôles de sécurité et des améliorations dans la famille SI. La politique et les procédures liées à l'intégrité de l'information et des systèmes sont conformes aux lois du GC et aux politiques, directives et normes applicables du SCT. Les politiques et les procédures du programme de sécurité organisationnel peuvent rendre facultatives les politiques et procédures propres au système. La politique peut être intégrée à la politique générale sur la sécurité de l'information des organisations ou, inversement, elle peut être représentée par de multiples politiques compte tenu de la nature complexe de certaines organisations. Les procédures peuvent être établies pour le programme de sécurité général et pour des systèmes d'information particuliers, au besoin. La stratégie organisationnelle de gestion des risques est un facteur clé dans l'établissement de la politique et des procédures.

Améliorations de contrôle :

Aucune

Références :

SCT, *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information* [Référence 7].

SI-2 CORRECTION DES DÉFAUTS

Contrôle :

(A) L'organisation identifie, signale et corrige les défauts du système d'information.

(B) L'organisation, avant leur installation, teste les mises à jour logicielles visant la correction des défauts pour en vérifier l'efficacité et les répercussions potentielles sur ses systèmes d'information.

(C) L'organisation installe les mises à jour de sécurité appropriées des logiciels et des micrologiciels dans un délai de [*Affectation : délai défini par l'organisation*] après la diffusion des mises à jour.

(D) L'organisation intègre la correction des défauts à son processus de gestion des configurations.

Conseils supplémentaires : L'organisation identifie les systèmes d'information touchés par les défauts logiciels récemment annoncés, y compris les possibles vulnérabilités résultant de ces défauts et l'organisation rapporte cette information au personnel responsable de la sécurité de l'information. Les mises à jour logicielles pertinentes en matière de sécurité comprennent, par exemple, des correctifs, des ensembles de modifications provisoires, des réparations à chaud et des signatures antivirus. Elle corrige également le plus rapidement possible les défauts relevés durant les évaluations de sécurité, la surveillance permanente, les activités liées aux interventions en cas d'incident ou le traitement des erreurs du système d'information. Les organisations sont encouragées à tirer parti de ressources déjà disponibles comme les bases de données *Common Weakness Enumeration* (CWE) ou *Common Vulnerabilities and exposures* (CVE) pour corriger des défauts découverts dans leurs systèmes d'information. En intégrant la correction d'anomalies aux processus permanents de gestion de configuration, on peut assurer le suivi et la vérification des mesures correctrices requises ou anticipées. Par exemple, vérifier si l'organisation suit les conseils de US-CERT et les alertes de vulnérabilité en matière d'assurance de l'information (*Information Assurance Vulnerability Alerts*) fait partie des mesures de correction des anomalies dont on peut faire le suivi et la vérification. Le délai défini par l'organisation pour les mises à jour logicielles et micrologicielles peut varier en fonction de divers facteurs, notamment, la catégorie de sécurité du système d'information ou le côté critique de la mise à jour (c.-à-d. la sévérité de la vulnérabilité liée à l'anomalie découverte). Certains types de correctifs d'anomalies peuvent nécessiter plus de mises à l'essai que d'autres. L'organisation doit déterminer le degré et le type de mises à l'essai nécessaires pour le type précis de correction d'anomalies considérées et aussi le type de changements dont la configuration doit être gérée. Dans certains cas, l'organisation peut déterminer que la mise à l'essai de mises à jour logicielles ou micrologicielles n'est pas nécessaire ou pratique, par exemple, lorsqu'il s'agit de mettre en œuvre de simples mises à jour d'une signature antivirus. L'organisation peut en outre considérer dans ses décisions de mise à l'épreuve si des mises à jour logicielles ou micrologicielles proviennent de sources autorisées ayant des signatures numériques appropriées. Contrôles connexes : CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11.

Améliorations de contrôle :

(1) CORRECTION DES DÉFAUTS | GESTION CENTRALE

L'organisation centralise la gestion du processus de correction des anomalies.

Conseils supplémentaires sur l'amélioration : La gestion centrale assure la gestion et la mise en œuvre des processus liés aux correctifs d'anomalies dans l'ensemble de l'organisation. La gestion centrale comprend la planification, la mise en œuvre, l'évaluation, l'autorisation et la surveillance des contrôles de sécurité définis par l'organisation, gérés centralement et visant la correction des anomalies.

(2) CORRECTION DES DÉFAUTS | AUTOMATISATION DES CORRECTIFS D'ANOMALIES

L'organisation utilise des mécanismes automatisés [*Affectation : fréquence définie par l'organisation*] pour déterminer l'état des composants du système d'information en ce qui concerne la correction des défauts.

Conseils supplémentaires sur l'amélioration : Contrôles connexes : CM-6, SI-4.

(3) CORRECTION DES DÉFAUTS | DÉLAIS DE CORRECTION DES ANOMALIES / REPÈRES LIÉS AUX MESURES CORRECTIVES

(a) L'organisation mesure le temps écoulé entre la détection de l'anomalie et la correction de l'anomalie;

(b) l'organisation fixe [*Affectation : repères définis par l'organisation*] pour la prise de mesures correctives.

Conseils supplémentaires sur l'amélioration : La présente amélioration des contrôles nécessite de l'organisation détermine combien de temps est nécessaire pour corriger les anomalies des systèmes

d'information, une fois que ces anomalies ont été identifiées, puis ensuite, de fixer des repères (c.-à-d. des délais de traitement) liés à la mise en œuvre de mesures correctives. Les repères peuvent être établis en fonction des types d'anomalies et de la sévérité des possibles vulnérabilités si l'anomalie est exploitable.

(4) CORRECTION DES DÉFAUTS | OUTILS AUTOMATIQUES DE GESTION DES CORRECTIFS

[Annulée : Intégrée au contrôle SI-2]

(5) CORRECTION DES DÉFAUTS | MISES À JOUR LOGICIELLES OU MICROLOGICIELLES AUTOMATIQUES

L'organisation installe [*Affectation : mises à jour logicielles et micrologicielles pertinentes en matière de sécurité définies par l'organisation*] automatiquement à [*Affectation : composants du système d'information définis par l'organisation*].

Conseils supplémentaires sur l'amélioration : Compte tenu de l'importance de maintenir l'intégrité et la disponibilité du système d'information, l'organisation doit veiller à bien choisir la méthodologie de mise à jour automatique. L'organisation doit trouver l'équilibre entre le besoin de s'assurer que les mises à jour sont installées le plus tôt possible et le besoin de maintenir la gestion de configuration, tout en veillant à résoudre les possibles répercussions que pourraient avoir des mises à jour automatiques.

(6) CORRECTION DES DÉFAUTS | SUPPRESSION DES VERSIONS ANTÉRIEURES DES LOGICIELS OU DES MICROLOGICIELS

L'organisation doit supprimer [*Affectation : éléments logiciels et micrologiciels définis par l'organisation*] une fois qu'une version mise à jour a été installée.

Conseils supplémentaires sur l'amélioration : Les versions antérieures des logiciels ou des micrologiciels qui ne sont pas supprimées des systèmes d'information après l'installation des mises à jour peuvent être exploitées par des adversaires. Certains produits de technologies de l'information suppriment automatiquement les versions antérieures des logiciels ou des micrologiciels.

Références :

Aucune

SI-3 PROTECTION CONTRE LES CODES MALVEILLANTS

Contrôle :

(A) L'organisation utilise des mécanismes de protection contre les codes malveillants aux points d'entrée et de sortie du système d'information afin de détecter et d'éradiquer les codes malveillants.

(B) L'organisation met à jour ses mécanismes de protection contre les codes malveillants dès la diffusion de nouvelles versions, conformément à sa politique et à ses procédures de gestion des configurations.

(C) L'organisation configure les mécanismes de protection contre les codes malveillants de manière à :

(a) effectuer des analyses périodiques du système d'information [*Affectation : fréquence définie par l'organisation*] et des balayages en temps réel des fichiers de sources externes au(x) [*Sélection (un ou plusieurs); point d'extrémité; point d'entrée ou point de sortie du réseau*] lors de leur téléchargement, de leur ouverture ou de leur exécution, conformément à sa politique de sécurité;

(b) [*Sélection (un ou plusieurs): bloquer le code malveillant; mettre le code malveillant en quarantaine, envoyer une alerte à l'administrateur; [Affectation : mesure définie par l'organisation]*] lors de la détection d'un code malveillant.

(D) L'organisation traite les faux positifs résultant de la détection et de l'éradication de code malveillant et leurs répercussions potentielles sur la disponibilité du système d'information.

Conseils supplémentaires : Les points d'entrée et de sortie du système d'information comprennent, par exemple, les coupe-feux, les serveurs de messagerie électronique, les serveurs Web, les serveurs mandataires, les serveurs d'accès à distance, les postes de travail, les ordinateurs bloc-notes et les appareils mobiles. Les codes malveillants comprennent, par exemple, les virus, les vers, les chevaux de Troie et les espiogiciels. Ils peuvent également être codés sous différents formats (UUENCODE, Unicode, etc.) ou contenus dans un fichier comprimé ou caché ou dissimulés dans des dossiers au moyen de la stéganographie. Les codes malveillants peuvent être transmis par différents moyens (accès Web, fichiers joints à des courriers électroniques, dispositifs de stockage portatifs). Les insertions de code malveillant peuvent se produire lors de l'exploitation de vulnérabilités d'un système d'information. Les mécanismes de protection contre les codes malveillants comprennent notamment les définitions de signature antivirus et les technologies basées sur la réputation. Il existe une variété de technologies et de méthodes pour limiter ou éliminer les effets des attaques de code malveillant. Une gestion omniprésente des configurations et des contrôles complets d'intégrité des logiciels peuvent contrer efficacement l'exécution de codes non autorisés. En plus des logiciels commerciaux, les codes malveillants peuvent également se retrouver dans des logiciels personnalisés. Ils peuvent, par exemple, prendre la forme de bombes logiques, de portes dérobées et d'autres types de cyberattaque capables de mettre en péril les missions et les fonctions opérationnelles de l'organisation. Les mécanismes traditionnels de protection contre les codes malveillants ne sont pas toujours en mesure de détecter ce type de code. Dans ces situations, les organisations doivent plutôt compter sur d'autres mesures d'atténuation des risques, par exemple les pratiques de codage sécurisées, contrôle et gestion des configurations, processus d'approvisionnement fiables, et des pratiques de surveillance pour s'assurer que les logiciels n'exécutent pas de fonctions autres que celles prévues. L'organisation peut décider de prendre différentes mesures en réponse à la détection de code malveillant. Par exemple, l'organisation peut définir des mesures à prendre lors de la détection d'un code malveillant dans le cadre d'une analyse périodique, des mesures à prendre lors de la détection de téléchargements malveillants ou de mesures à prendre lors de la détection d'éléments malveillants lorsque l'on tente d'ouvrir ou d'exécuter des dossiers. Contrôles connexes : CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7.

Améliorations de contrôle :

(1) PROTECTION CONTRE LES CODES MALVEILLANTS | GESTION CENTRALE

L'organisation centralise la gestion des mécanismes de protection contre les codes malveillants.

Conseils supplémentaires sur l'amélioration : La gestion centrale assure la gestion et la mise en œuvre des processus liés aux mécanismes de protection contre les codes malveillants dans l'ensemble de l'organisation. La gestion centrale comprend la planification, la mise en œuvre, l'évaluation, l'autorisation et la surveillance des contrôles de sécurité définis par l'organisation, gérés centralement et visant la protection contre les codes malveillants. Contrôles connexes : AU-2, SI-8.

(2) PROTECTION CONTRE LES CODES MALVEILLANTS | MISES À JOUR AUTOMATIQUES

Le système d'information met automatiquement à jour les mécanismes de protection contre les codes malveillants.

Conseils supplémentaires sur l'amélioration : Les mécanismes de protection contre les codes malveillants comprennent, par exemple, les définitions de signatures. Compte tenu de l'importance de maintenir l'intégrité et la disponibilité du système d'information, l'organisation doit veiller à bien choisir la méthodologie de mise à jour automatique. Contrôle connexe : SI-8.

(3) PROTECTION CONTRE LES CODES MALVEILLANTS | UTILISATEURS NON PRIVILÉGIÉS

[Annulée : Intégrée au contrôle AC-6 (10)]

(4) PROTECTION CONTRE LES CODES MALVEILLANTS | MISES À JOUR EFFECTUÉES SEULEMENT PAR LES UTILISATEURS PRIVILÉGIÉS

Le système d'information met à jour les mécanismes de protection contre les codes malveillants uniquement lorsqu'un utilisateur privilégié le demande.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle peut être appropriée dans les situations où, pour garantir la sécurité ou la continuité des opérations, les mises à jour ne sont effectuées qu'après avoir sélectionnées ou approuvées par le personnel désigné de l'organisation. Contrôles connexes : AC-6, CM-5.

(5) PROTECTION CONTRE LES CODES MALVEILLANTS | DISPOSITIFS DE STOCKAGE PORTATIFS

[Annulé : Intégré au contrôle MP-7]

(6) PROTECTION CONTRE LES CODES MALVEILLANTS | MISES À L'ÉPREUVE / VÉRIFICATIONS

(a) L'organisation teste les mécanismes de protection contre les codes malveillants [*Affectation : fréquence définie par l'organisation*] en en introduisant dans le système d'information un scénario de test anodin connu et non invasif;

(b) l'organisation vérifie qu'il y a effectivement, comme il se doit, détection du scénario et signalement des incidents qui lui sont associés.

Conseils supplémentaires sur l'amélioration : Contrôles connexes : CA-2, CA-7, RA-5.

(7) PROTECTION CONTRE LES CODES MALVEILLANTS | DÉTECTION NON AXÉE SUR LES SIGNATURES

Le système d'information met en œuvre des mécanismes non axés sur les signatures de détection de code malveillant.

Conseils supplémentaires sur l'amélioration : Les mécanismes de détection non axés sur les signatures comprennent, par exemple, l'utilisation de données heuristiques pour détecter, analyser et décrire les caractéristiques ou les comportements de codes malveillants et pour trouver des moyens de se protéger contre ces codes si des signatures n'existent pas encore ou si les signatures qui existent ne sont pas efficaces. Ceci comprend les codes malveillants polymorphes (c.-à-d. dont la signature change lorsqu'il se reproduit). Cette amélioration de contrôle n'exclut toutefois pas l'utilisation de mécanismes de détection axés sur la signature.

(8) PROTECTION CONTRE LES CODES MALVEILLANTS | DÉTECTION DES COMMANDES NON AUTORISÉES

Le système d'information détecte [*Affectation : commandes non autorisées du système d'exploitation définies par l'organisation*] dans l'interface de programmation d'application du noyau dans [*Affectation : composantes matérielles du système d'information définies par l'organisation*] et [*Sélection (un ou plusieurs) : émet un avertissement; vérifie l'exécution de la commande; empêche l'exécution de la commande*].

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle peut aussi être appliquée aux interfaces essentielles autres que les interfaces axées sur le noyau, y compris les interfaces avec machines virtuelles et applications privilégiées. Les commandes non autorisées des systèmes d'exploitation comprennent, par exemple, les commandes pour des fonctions du noyau provenant de processus du système d'information auxquels on n'accorde pas la confiance nécessaire pour initialiser de telles commandes, ou des commandes pour des fonctions du noyau qui semblent suspectes, mêmes si les commandes de ce type pourraient vraisemblablement être initialisées par ces processus. L'organisation peuvent faire en sorte que la détection des commandes malveillantes soit effectuée à partir d'une combinaison de types de commandes, de classes de commandes ou d'occurrences précises de commandes. L'organisation peut définir les composantes matérielles à partir de composantes précises, de types de composantes, de leur emplacement dans le réseau ou à partir d'une combinaison des éléments mentionnés précédemment. L'organisation peut choisir entre différentes mesures en fonction du type, de la classe ou de l'occurrence des commandes possiblement malveillantes. Contrôle connexe : AU-6.

(9) PROTECTION CONTRE LES CODES MALVEILLANTS | AUTHENTIFIER LES COMMANDES À DISTANCE

Le système d'information met en œuvre [*Affectation : mesures de protection de sécurité définies par l'organisation*] pour authentifier [*Affectation : commandes à distance définies par l'organisation*].

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle assure une protection contre les commandes non autorisées et la réexécution des commandes autorisées. Cette capacité est importante pour les systèmes d'information à distance dont la perte, le mauvais fonctionnement, la mauvaise conduite ou l'exploitation pourraient avoir des conséquences immédiates ou sérieuses (p. ex. blessures, mort, dommages à la propriété, perte de biens ou de renseignements sensibles, échec de missions ou de fonctions opérationnelles importantes). La protection par authentification des commandes à distance fait en sorte que le système d'information accepte et exécute les commandes dans l'ordre prévu. De plus le système ne traite que les commandes autorisées et rejette les commandes non autorisées. Des mécanismes cryptographiques peuvent être employés, par exemple, pour authentifier les commandes à distance. Contrôles connexes : SC-12, SC-13, SC-23.

(10) PROTECTION CONTRE LES CODES MALVEILLANTS | ANALYSES DES CODES MALVEILLANTS

(a) L'organisation emploie [*Affectation : outils et techniques définis par l'organisation*] pour analyser les caractéristiques et les comportements des codes malveillants;

(b) l'organisation intègre les résultats des analyses des codes malveillants à son plan des interventions en cas d'incident et à ses processus de correction des anomalies.

Conseils supplémentaires sur l'amélioration : L'application des techniques et des outils sélectionnés afin d'analyser les codes malveillants offre une connaissance plus approfondie à l'organisation du savoir-faire de ses adversaires (c.-à-d. ses tactiques, techniques et procédures) et du fonctionnement et des buts de certains codes malveillants en particulier. Comprendre les caractéristiques des codes malveillants facilite les interventions de la part de l'organisation pour contrer les menaces actuelles et à venir. L'organisation peut effectuer des analyses des codes malveillants en se servant de techniques de rétroingénierie ou en surveillant le comportement des codes malveillants que l'on exécute.

Références :

Aucune

SI-4 SURVEILLANCE DES SYSTÈMES D'INFORMATION

Contrôle :

(A) L'organisation surveille le système d'information pour y détecter :

(a) des attaques et des signes indiquant de possibles attaques conformément [*Affectation : objectifs de surveillance définis par l'organisation*];

(b) des connexions locales, réseau ou à distance non autorisées.

(B) L'organisation détermine qu'il y a une utilisation non autorisée de son système d'information [*Affectation : techniques et méthodes définies par l'organisation*].

(C) L'organisation déploie dans le système d'information des dispositifs de surveillance à la fois (i) stratégiquement pour collecter l'information qu'elle juge essentielle et (ii) de manière aléatoire pour faire le suivi des types de transaction qui l'intéressent particulièrement.

(D) L'organisation protège l'information obtenue des outils de surveillance des intrusions contre tout accès non autorisé et toute modification et suppression.

(E) L'organisation élève le niveau des activités de surveillance du système d'information dès qu'il y a indication de risque accru pour les activités et les biens de l'organisation, les personnes, les autres organisations ou le Canada selon l'information mise à sa disposition (information relative au contrôle d'application de la loi, découlant du renseignement ou provenant d'autres sources crédibles).

(F) L'organisation obtient un avis juridique concernant les activités de surveillance du système d'information conformément aux lois du GC et aux politiques, directives et normes du SCT.

(G) L'organisation fournit [*Affectation: types de renseignements liés à la surveillance du système d'information définis par l'organisation*] à [*Affectation : personnel ou rôles définis par l'organisation*], et ce, [*Sélection (un ou plusieurs) : au besoin;* [*Affectation : fréquence définie par l'organisation*]].

Conseils supplémentaires : La surveillance du système d'information est à la fois externe et interne. La surveillance externe comprend l'observation des événements qui se produisent à la frontière du système d'information (c.-à-d. fait partie de la défense du périmètre et de la protection des frontières). La surveillance interne comprend l'observation des événements qui se produisent à l'intérieur du système. L'organisation peut surveiller son système d'information, par exemple, en observant les activités de surveillance en temps réel ou en observant d'autres aspects du système, comme les profils types des accès, les caractéristiques des accès et d'autres actions. Les objectifs de la surveillance peuvent orienter la détermination des événements. La capacité de surveillance du système d'information est possible grâce à une variété d'outils et de techniques (p. ex. systèmes de détection et de prévention des intrusions, logiciels de protection contre les codes malveillants, outils de balayage, logiciel de surveillance des enregistrements de vérification, logiciel de surveillance des réseaux). Les dispositifs de surveillance sont insérés à des endroits stratégiques comme, par exemple, dans des emplacements particuliers du périmètre et près de grappes de serveurs prenant en charge des applications essentielles, et sont normalement utilisés dans les interfaces gérées associées aux contrôles SC-7 et AC-17. La granularité de l'information de surveillance collectée est déterminée par les objectifs de surveillance de l'organisation et la capacité du système d'information de prendre en charge ces activités. Des types précis de transactions d'intérêt comprennent, par exemple, le trafic HTTP qui contourne les mandataires HTTP. La surveillance du système d'information fait partie intégrante des programmes organisationnels de surveillance et d'intervention en cas d'incident. Les résultats de la surveillance du système servent de fondement aux programmes de surveillance continue et d'intervention en cas d'incident. Par connexion réseau, on entend toute connexion avec un appareil qui communique par l'intermédiaire d'un réseau (p. ex. réseau local, Internet). Une connexion réseau à distance est toute connexion à un dispositif qui communique par un réseau externe (p. ex. Internet). Les connexions locales, réseau et à distances peuvent être câblées ou sans fil. Contrôles connexes : AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7.

Améliorations de contrôle :

(1) SURVEILLANCE DES SYSTÈMES D'INFORMATION | SYSTÈME DE DÉTECTION D'INTRUSIONS DANS L'ENSEMBLE DU SYSTÈME

L'organisation connecte et configure les outils individuels de détection d'intrusion en un système organisationnel unique.

(2) SURVEILLANCE DES SYSTÈMES D'INFORMATION | OUTILS AUTOMATISÉS AUX FINS D'ANALYSE EN TEMPS RÉEL

L'organisation utilise des outils automatisés pour prendre en charge l'analyse des événements en temps quasi réel.

Conseils supplémentaires sur l'amélioration : Les outils automatisés comprennent, par exemple, les outils de surveillances des événements sur l'hôte, sur le réseau, sur le transport ou sur le stockage, ou les solutions de gestion des informations et des événements de sécurité (SIEM pour *Security Information and Event Management*) offrant des analyses en temps réel des alertes ou des notifications générées par les systèmes d'information organisationnels.

(3) SURVEILLANCE DES SYSTÈMES D'INFORMATION | INTÉGRATION DES OUTILS AUTOMATISÉS

L'organisation utilise des outils automatisés pour intégrer les outils de détection d'intrusion aux mécanismes de contrôle d'accès et de flux afin de permettre la reconfiguration de ces mécanismes en vue d'isoler et d'éliminer rapidement les attaques.

(4) SURVEILLANCE DES SYSTÈMES D'INFORMATION | TRAFIC DE COMMUNICATION ENTRANT ET SORTANT

Le système d'information surveille le trafic de communications entrantes et sortantes [*Affectation : fréquence définie par l'organisation*] pour détecter toute activité ou condition inhabituelle ou non autorisée.

Conseils supplémentaires sur l'amélioration : Les activités ou conditions inhabituelles ou non autorisées liées au trafic de communications entrant et sortant comprennent, par exemple, le trafic interne qui indique la présence d'un code malveillant dans un système d'information organisationnel ou sa propagation dans les composants connexes, l'exportation non autorisée d'information et l'envoi d'un signal vers un système d'information externe. Les preuves de l'existence d'un code malveillant permettent d'identifier les systèmes d'information ou les composants connexes qui pourraient avoir été compromis.

(5) SURVEILLANCE DES SYSTÈMES D'INFORMATION | ALERTES GÉNÉRÉES PAR LE SYSTÈME

Le système d'information produit des alertes [*Affectation : personnel ou rôles définis par l'organisation*] lorsque les indications de compromission réelle ou potentielle suivantes se présentent : [*Affectation : indicateurs de compromission définis par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les alertes peuvent provenir de sources diverses comme, par exemple, des enregistrements de vérification ou des mécanismes de protection contre les codes malveillants, des mécanismes de détection ou de prévention des intrusions, ou des dispositifs de protection des frontières tels les coupe-feux, les passerelles et les routeurs. Les alertes peuvent être communiquées par téléphone, par courriel ou par messages textes. Le personnel de l'organisation se trouvant sur la liste de notification peut comprendre, par exemple, les administrateurs de système, les propriétaires de la mission ou des activités, les propriétaires des systèmes ou les agents de sécurité des systèmes d'information. Contrôles connexes : AU-5, PE-6.

(6) SURVEILLANCE DES SYSTÈMES D'INFORMATION | RESTREINDRE LES UTILISATEURS NON PRIVILÉGIÉS

[Annulée : Intégrée au contrôle AC-6 (10)]

(7) SURVEILLANCE DES SYSTÈMES D'INFORMATION | INTERVENTIONS AUTOMATISÉES EN CAS D'ÉVÉNEMENT SUSPECT

Le système d'information informe [*Affectation : liste définie par l'organisation des employés (identifiés par nom ou rôle) chargés d'intervenir en cas d'incident*] des événements suspects qui ont été détectés et prend les [*Affectation : liste définie par l'organisation des mesures les moins perturbatrices visant à mettre fin aux événements suspects*].

Conseils supplémentaires sur l'amélioration : Les mesures les moins perturbatrices peuvent comprendre, par exemple, remplir des demandes d'interventions de la part de personnes.

(8) SURVEILLANCE DES SYSTÈMES D'INFORMATION | PROTECTION DES RENSEIGNEMENTS DE SURVEILLANCE

[Annulée : Intégrée au contrôle SI-4]

(9) SURVEILLANCE DES SYSTÈMES D'INFORMATION | MISE À L'ESSAI DES OUTILS DE SURVEILLANCE

L'organisation teste les outils de surveillance des intrusions [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires sur l'amélioration : Il est nécessaire de tester les outils de surveillance des intrusions pour s'assurer qu'ils fonctionnent correctement et qu'ils répondent toujours aux objectifs de l'organisation en matière de surveillance. La fréquence des tests dépend du type d'outils dont l'organisation se sert et des méthodes de déploiement des outils. Contrôle connexe : CP-9.

(10) SURVEILLANCE DES SYSTÈMES D'INFORMATION | VISIBILITÉ DES COMMUNICATIONS CHIFFRÉES

L'organisation prend les mesures nécessaires pour rendre [*Affectation : trafic de communications chiffrées défini par l'organisation*] visible aux [*Affectation : outils de surveillance du système d'information définis par l'organisation*].

Conseils supplémentaires sur l'amélioration : L'organisation doit trouver l'équilibre entre le besoin chiffrer le trafic de communication et le besoin d'avoir accès au trafic pour en effectuer la surveillance.

Certaines organisations jugent essentiel d'assurer la confidentialité du trafic de communication tandis que d'autres considèrent qu'il est plus important de protéger la mission. L'organisation détermine si l'exigence en matière de visibilité s'applique au trafic chiffré interne, au trafic chiffré qui sera envoyé à l'externe ou à un sous-ensemble de types de trafic.

(11) SURVEILLANCE DES SYSTÈMES D'INFORMATION | ANALYSER LES ANOMALIES DU TRAFIC DE COMMUNICATION

L'organisation analyse le trafic des communications sortantes à la frontière externe du système [*Affectation : certains de ses points intérieurs (p. ex. sous-réseaux, sous-systèmes) définis par l'organisation*] pour découvrir des anomalies.

Conseils supplémentaires sur l'amélioration : Les anomalies à l'intérieur du système d'information de l'organisation comprennent, par exemple, les transferts de fichiers volumineux, les connexions persistantes de longue durée, les protocoles et ports inhabituels utilisés, et les tentatives de communications avec des adresses externes malveillantes suspectes.

(12) SURVEILLANCE DES SYSTÈMES D'INFORMATION | ALERTES AUTOMATISÉES

L'organisation utilise des mécanismes automatisés pour alerter le personnel de sécurité des répercussions potentielles des activités inhabituelles ou inappropriées suivantes : [*Affectation : liste définie par l'organisation des activités inhabituelles ou inappropriées qui déclenchent des alertes*].

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle met l'accent sur les alertes de sécurité générées par l'organisation et diffusées par l'intermédiaire de moyens automatisés. Contrairement aux alertes générées par le système d'information dans SI-4 (5) qui ont tendance à mettre l'accent sur les sources internes (p. ex. enregistrements de vérification), les sources d'informations liées à cette amélioration peuvent inclure d'autres entités (p. ex. rapports sur les activités suspectes, rapports sur les possibles menaces internes). Contrôles connexes : AC-18, IA-3.

(13) SURVEILLANCE DES SYSTÈMES D'INFORMATION | ANALYSE DU TRAFIC DES COMMUNICATIONS / TENDANCE DES ÉVÉNEMENTS

(a) L'organisation analyse le trafic des communications ou la tendance des événements pour le système d'information;

(b) l'organisation développe des profils représentant les modèles de trafic ou les événements communs;

(c) l'organisation utilise le trafic / les profils des événements pour calibrer les dispositifs de surveillance afin de réduire le nombre de faux positifs et le nombre de faux négatifs.

(14) SURVEILLANCE DES SYSTÈMES D'INFORMATION | SYSTÈME DE DÉTECTION D'INTRUSIONS SUR LES RÉSEAUX SANS FIL

L'organisation utilise un système de détection d'intrusions sans fil pour identifier les dispositifs sans fil indésirables et détecter les tentatives d'attaque et les compromissions ou infractions potentielles liées au système d'information.

Conseils supplémentaires sur l'amélioration : Dans certaines situations, les signaux sans fil peuvent se propager au-delà des frontières des installations contrôlées par l'organisation. L'organisation doit rechercher proactivement les connexions sans fil non autorisées, et exécutent des balayages rigoureux pour détecter les points d'accès sans fil non autorisés. Le balayage ne se limite pas nécessairement aux installations qui hébergent les systèmes d'information, mais peut être effectué à l'extérieur au besoin pour vérifier que des points d'accès sans fil non autorisés ne sont pas connectés au système. Contrôles connexes : AC-18, IA-3.

(15) SURVEILLANCE DES SYSTÈMES D'INFORMATION | COMMUNICATIONS ENTRE UN RÉSEAU SANS FIL ET UN RÉSEAU FILAIRE

L'organisation utilise un système de détection d'intrusions pour surveiller le trafic de communications sans fil lorsqu'il passe d'un réseau sans fil à un réseau filaire.

Conseils supplémentaires sur l'amélioration : Contrôle connexe : AC-18.

(16) SURVEILLANCE DES SYSTÈMES D'INFORMATION | ÉTABLIR DES CORRÉLATIONS ENTRE LES RÉSULTATS DES ACTIVITÉS DE SURVEILLANCE

L'organisation établit des corrélations entre les informations provenant des outils de surveillance employés dans l'ensemble du système d'information.

Conseils supplémentaires sur l'amélioration : Établir des corrélations entre les résultats des différents outils de surveillance peut fournir une vue d'ensemble plus complète des activités se déroulant dans le système d'information. Établir des corrélations entre des outils de surveillances qui travaillent habituellement de manière isolée (p. ex. surveillance des hôtes, surveillance des réseaux, logiciel antivirus) peut, en fournissant une vue d'ensemble de l'organisation, révéler des modèles d'attaques qui seraient autrement restés inaperçus. Comprendre les capacités et les limites de différents outils de surveillance et savoir comment maximiser l'utilité des renseignements générés par ces outils peut aider l'organisation à mettre sur pied, exploiter et maintenir des programmes de surveillance efficaces. Contrôle connexe : AU-6.

(17) SURVEILLANCE DES SYSTÈMES D'INFORMATION | CONNAISSANCE INTÉGRÉE DE LA SITUATION

L'organisation met en corrélation les résultats de la surveillance des activités physiques, des cyberactivités et des activités de la chaîne d'approvisionnement pour développer une connaissance intégrée de la situation à l'échelle organisationnelle.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle établit des corrélations entre des informations résultant d'activités de surveillance provenant de sources plus diverses afin d'obtenir une connaissance intégrée de la situation. Une connaissance intégrée de la situation basée sur des activités de surveillance physique, de cybersurveillance et de surveillance de la chaîne d'approvisionnement améliore la capacité de l'organisation de détecter plus rapidement les cyberattaques sophistiquées et d'enquêter sur les méthodes et techniques utilisées par les attaquants. Contrairement à SI-4 (16) qui vise à établir des corrélations entre les différentes informations liées à la cybersurveillance, la présente amélioration met en corrélation des éléments qui n'appartiennent pas uniquement au cyberdomaine. Une telle surveillance peut aider à révéler des attaques contre des organisations dont les opérations s'étendent dans plusieurs vecteurs d'attaque. Contrôle connexe : SA-12.

(18) SURVEILLANCE DES SYSTÈMES D'INFORMATION | ANALYSE DU TRAFIC / EXFILTRATIONS MASQUÉES

L'organisation analyse le trafic des communications sortantes à la frontière externe du système (c.-à-d. périmètre du système) et [*Affectation : certains de ses points intérieurs (p. ex. sous-réseaux, sous-systèmes) définis par l'organisation*] pour y détecter des exfiltrations masquées d'informations.

Conseils supplémentaires sur l'amélioration : Par « masqué », on entend un procédé qui peut être utilisé pour l'exfiltration non autorisée d'informations de l'organisation, par exemple, la stéganographie.

(19) SURVEILLANCE DES SYSTÈMES D'INFORMATION | LES PERSONNES QUI POSENT UN GRAND RISQUE

L'organisation met en œuvre [*Affectation : surveillance supplémentaire définie par l'organisation*] des personnes qui ont été identifiées par [*Affectation : sources définies par l'organisation*], car elles représentent un plus grand risque.

Conseils supplémentaires sur l'amélioration : On peut se fier à plusieurs sources pour déterminer si une personne pose de plus grands risques qu'une autre, par exemple, des dossiers des ressources humaines, des agences de renseignement, des organisations d'application de la loi ou d'autres sources crédibles. La surveillance des personnes doit être coordonnée de près avec des représentants de la direction, des services juridiques, de la sécurité et des ressources humaines des organisations qui effectuent une telle surveillance et elle doit être conforme aux lois du GC ainsi qu'aux politiques, directives et normes applicables du SCT.

(20) SURVEILLANCE DES SYSTÈMES D'INFORMATION | UTILISATEURS PRIVILÉGIÉS

L'organisation met en œuvre [*Affectation : surveillance supplémentaire définie par l'organisation*] des utilisateurs privilégiés.

(21) SURVEILLANCE DES SYSTÈMES D'INFORMATION | PÉRIODES PROBATOIRES

L'organisation met en œuvre [*Affectation : surveillance supplémentaire définie par l'organisation*] des personnes pendant [*Affectation : période probatoire définie par l'organisation*].

(22) SURVEILLANCE DES SYSTÈMES D'INFORMATION | SERVICES NON AUTORISÉS LIÉS AU RÉSEAU

Le système d'information détecte les services de réseau qui n'ont pas été autorisés ou approuvés par [*Affectation : autorisation ou processus d'approbation définis par l'organisation*] et [*Sélection (un ou plusieurs) : vérifications; alertes; [Affectation : personnel ou rôles désignés par l'organisation]*].

Conseils supplémentaires sur l'amélioration : Les services de réseau non autorisés ou non approuvés comprennent, par exemple, les services dans les architectures axées sur le service qui manquent de vérification ou de validation organisationnelle et qui pourraient donc être non fiables ou servir d'agent malveillant inséré dans un service légitime. Contrôles connexes : AC-6, CM-7, SA-5, SA-9.

(23) SURVEILLANCE DES SYSTÈMES D'INFORMATION | APPAREILS GÉRÉS PAR LE SYSTÈME CENTRAL

L'organisation met en œuvre [*Affectation : mécanismes de protection au niveau de l'hôte définis par l'organisation*] à [*Affectation : composants des systèmes d'information désignés par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les éléments du système d'information pouvant faire l'objet d'une surveillance sur hôte comprennent notamment les serveurs, les postes de travail et les appareils mobiles. L'organisation doit considérer employer des mécanismes de surveillance sur hôte provenant de différents développeurs de produits des technologies de l'information.

(24) SURVEILLANCE DES SYSTÈMES D'INFORMATION | INDICATEURS DE COMPROMISSION

Le système d'information découvre, recueille, distribue et utilise les indicateurs de compromission.

Conseils supplémentaires sur l'amélioration : Les indicateurs de compromissions sont des traces incriminantes d'intrusions qui ont été identifiées dans le système d'information de l'organisation (au niveau de l'hôte ou du réseau). Ces indicateurs fournissent à l'organisation des informations précieuses sur les articles ou les systèmes d'information qui ont été compromis. Les indicateurs de compromission d'hôtes compromis peuvent comprendre, notamment, la création de valeurs de clés du registre. Les indicateurs de compromission des réseaux comprennent, par exemple, des éléments du Universal Resource Locator (URL) ou du protocole qui indiquent que les serveurs ont reçu des instructions de commandement et de contrôle d'un maliciel. L'adoption et la distribution rapides des indicateurs de compromission peuvent améliorer la sécurité de l'information en réduisant le laps de temps pendant lequel les systèmes et les organisations sont vulnérables aux mêmes exploits ou attaques.

Références :

Aucune

SI-5 ALERTES, AVIS ET DIRECTIVES DE SÉCURITÉ

Contrôle :

(A) L'organisation reçoit régulièrement [*Affectation : l'organisation doit désigner des organisations externes*] des alertes, avis et directives de sécurité concernant le système d'information.

(B) L'organisation produit des alertes, avis et directives de sécurité internes lorsqu'elle le juge nécessaire.

(C) L'organisation diffuse des alertes, des avis et des directives de sécurité à : [*Sélection (un ou plusieurs*) : [*Affectation : personnel ou rôles définis par l'organisation*]; [*Affectation : éléments au sein de l'organisation définis par l'organisation*]; [*Affectation : organisations externes désignées par l'organisation*]].

(D) L'organisation met en œuvre les directives de sécurité dans les délais prescrits ou informe l'organisation émettrice du degré de non-respect.

Conseils supplémentaires : Le respect des directives de sécurité est essentiel compte tenu de la nature critique de plusieurs d'entre elles, sans parler des effets négatifs immédiats qui pourraient se faire sentir sur les activités et les biens de l'organisation, les personnes, les autres organisations et le Canada au cas où les directives ne seraient pas mises en œuvre en temps opportun. Les organisations externes comprennent, par exemple, les partenaires externes de la mission ou des opérations, les partenaires de la chaîne d'approvisionnement, les fournisseurs de services externes, les homologues de l'organisation et les autres organisations qui l'appuient dans ses opérations/sa mission. Contrôle connexe : SI-2.

Améliorations de contrôle :

(1) ALERTES, CONSEILS ET DIRECTIVES DE SÉCURITÉ | ALERTES ET AVIS AUTOMATISÉS

L'organisation utilise des mécanismes automatisés pour diffuser de l'information contenue dans les alertes et les avis de sécurité à l'ensemble de l'organisation.

Conseils supplémentaires sur l'amélioration : Le nombre important de changements aux systèmes d'information organisationnels et aux environnements dans lesquels ces systèmes sont exploités font en sorte qu'il est nécessaire de diffuser des informations concernant la sécurité à une vaste gamme d'entités organisationnelles pour qui la réussite des missions et des opérations de l'organisation est de première importance. En fonction des informations fournies par les alertes et les avis de sécurité, il peut s'avérer nécessaire d'effectuer des changements à chacun des trois niveaux hiérarchiques de la gestion des risques en matière de sécurité de l'information, c.-à-d. le niveau gouvernance, le niveau de l'architecture d'entreprise du processus lié à une mission/une activité, ou le niveau du système d'information.

Références :

SCT, *Plan de gestion des incidents des technologies de l'information du gouvernement du Canada* [Référence 67].

SI-6 VÉRIFICATION DE LA FONCTIONNALITÉ DE SÉCURITÉ

Contrôle :

(A) Le système d'information vérifie l'exploitation correcte de [*Affectation : fonctions de sécurité définies par l'organisation*].

(B) Le système d'information vérifie le bon fonctionnement des fonctions de sécurité [*Sélection (un ou plusieurs): [Affectation : états transitionnels du système définis par l'organisation]; à la demande d'un utilisateur qui possède les privilèges appropriés; [Affectation : période définie par l'organisation]*].

(C) Le système d'information avertit [*Affectation : personnel ou rôles définis par l'organisation*] lorsque des tests de vérification de sécurité sont échoués.

(D) Le système d'information [*Sélection (un ou plusieurs) : arrête le système; redémarre le système; [Affectation : autre(s) mesure(s) définie(s) par l'organisation]*] lorsque des anomalies sont relevées.

Conseils supplémentaires : Les états transitionnels des systèmes d'information comprennent notamment le démarrage, le redémarrage, l'arrêt et l'interruption. Les notifications fournies par les systèmes d'information comprennent, entre autres, des alertes électroniques à l'intention des administrateurs des systèmes, des messages à l'intention des consoles locales et des indications matérielles, comme des témoins lumineux. Contrôles connexes : CA-7, CM-6.

Améliorations de contrôle :

(1) VÉRIFICATION DES FONCTIONS DE SÉCURITÉ | NOTIFICATIONS D'ÉCHEC DES TESTS DE SÉCURITÉ

[Annulée : Intégrée au contrôle SI-6]

(2) VÉRIFICATION DES FONCTIONS DE SÉCURITÉ | SOUTIEN AUTOMATISÉ POUR LES TESTS DISTRIBUÉS

Le système d'information met en œuvre un soutien automatisé pour la gestion des tests de sécurité distribués.

Conseils supplémentaires sur l'amélioration : Contrôle connexe : SI-2.

(3) VÉRIFICATION DES FONCTIONS DE SÉCURITÉ | ÉLABORER DES RAPPORTS SUR LES RÉSULTATS DES VÉRIFICATIONS

L'organisation signale les résultats de la vérification des fonctions de sécurité à [*Affectation : personnel ou rôles définis par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les membres du personnel organisationnel pouvant avoir un possible intérêt envers les résultats de la vérification des fonctions de sécurité sont notamment les agents principaux de sécurité de l'information, les gestionnaires de la sécurité des systèmes d'information et les agents de sécurité des systèmes d'information. Contrôles connexes : SA-12, SI-4, SI-5.

Références :

Aucune

SI-7 INTÉGRITÉ DES LOGICIELS, DES MICROLOGICIELS ET DE L'INFORMATION

Contrôle :

(A) L'organisation emploie des outils de vérification pour détecter les cas où des changements non autorisés sont apportés à [*Affectation : logiciels, micrologiciels et information définis par l'organisation*].

Conseils supplémentaires : Des changements non autorisés aux logiciels, aux micrologiciels et aux informations peuvent être dus à des erreurs ou à des activités malveillantes (c.-à-d. trafiquage). Les logiciels comprennent, notamment, les systèmes d'exploitation (y compris les composants internes comme les noyaux, les pilotes de périphériques), les intergiciels et les applications. Les micrologiciels comprennent, entre autres, le système d'entrée-sortie de base (BIOS). Les informations comprennent les métadonnées, à l'instar des attributs de sécurité associés aux informations. Les mécanismes de vérification de l'intégrité les plus évolués (p. ex. vérifications de la parité, vérifications cycliques de la redondance, hachages cryptographiques) et les outils connexes peuvent automatiquement surveiller l'intégrité des systèmes d'information et des applications hébergées. Contrôles connexes : SA-12, SC-8, SC-13, SI-3.

Améliorations de contrôle :

(1) INTÉGRITÉ DES LOGICIELS, DES MICROLOGICIELS ET DE L'INFORMATION | CONTRÔLES D'INTÉGRITÉ

Le système d'information effectue un contrôle de l'intégrité de [*Affectation : logiciels, micrologiciels et information définis par l'organisation] [Sélection (un ou plusieurs) : au lancement; à [Affectation : états transitionnels ou événements touchant la sécurité définis par l'organisation]; [Affectation : fréquence définie par l'organisation]*].

Conseils supplémentaires sur l'amélioration : Les événements touchant la sécurité comprennent, notamment, l'identification d'une nouvelle menace envers laquelle les systèmes d'information sont vulnérables et l'installation de nouveaux logiciels, matériels ou micrologiciels. Les états transitionnels de système d'information comprennent notamment le démarrage, le redémarrage, l'arrêt et l'interruption.

(2) INTÉGRITÉ DES LOGICIELS, DES MICROLOGICIELS ET DE L'INFORMATION | AUTOMATISATION DES NOTIFICATIONS DE MANQUEMENT À L'INTÉGRITÉ

L'organisation utilise des outils automatisés qui notifient [*Affectation : personnel ou rôles définis par l'organisation*] lors de la découverte d'écarts durant la vérification de l'intégrité.

Conseils supplémentaires sur l'amélioration : L'utilisation d'outils automatisés pour rapporter les atteintes à l'intégrité et pour avertir le personnel organisationnel en temps opportun est un précurseur essentiel d'une intervention efficace contre les risques. Parmi les membres du personnel pour qui les atteintes à l'intégrité représentent une question d'intérêt, on compte les propriétaires de la mission ou des activités, les propriétaires du système d'information, les administrateurs des systèmes, les développeurs de logiciels, les intégrateurs de systèmes et les agents de sécurité de l'information.

(3) INTÉGRITÉ DES LOGICIELS, DES MICROLOGICIELS ET DE L'INFORMATION | OUTILS DE VÉRIFICATION DE L'INTÉGRITÉ GÉRÉS CENTRALEMENT

L'organisation utilise des outils de vérification de l'intégrité gérés centralement.

Conseils supplémentaires sur l'amélioration : Contrôle connexe : AU-3, SI-2, SI-8.

(4) INTÉGRITÉ DES LOGICIELS, DES MICROLOGICIELS ET DE L'INFORMATION | CONDITIONNEMENT INVIOLABLE DES PRODUITS

[Annulé : Intégré au contrôle SA-12]

(5) INTÉGRITÉ DES LOGICIELS, DES MICROLOGICIELS ET DE L'INFORMATION | AUTOMATISATION DES INTERVENTIONS EN CAS D'ATTEINTE À L'INTÉGRITÉ

Le système d'information [*Sélection (un ou plusieurs) : arrête le système; redémarre le système; [Affectation : autre(s) mesure(s) définie(s) par l'organisation]*] lorsque des atteintes à l'intégrité sont relevées.

Conseils supplémentaires sur l'amélioration : L'organisation peut définir différentes vérifications de l'intégrité et interventions lorsque des anomalies sont relevées : (i) en fonction du type d'information (p. ex. micrologiciel, logiciel, données utilisateur); (ii) en fonction d'informations précises (p. ex. microprogramme de démarrage, microprogramme de démarrage pour un type particulier de machine); ou (iii) une combinaison des deux. La mise en œuvre automatique des mesures de protection comprend, par exemple, le retour en arrière du changement, l'arrêt du système d'information ou le déclenchement d'une alerte de vérification dès qu'un changement non autorisé s'effectue dans un fichier de sécurité essentiel.

(6) INTÉGRITÉ DES LOGICIELS, DES MICROLOGICIELS ET DE L'INFORMATION | PROTECTION CRYPTOGRAPHIQUE

Le système d'information met en œuvre des mécanismes cryptographiques pour détecter les changements non autorisés apportés aux logiciels, aux micrologiciels et à l'information.

Conseils supplémentaires sur l'amélioration : Les mécanismes cryptographiques de protection de l'intégrité comprennent notamment les signatures numériques, le calcul et l'application d'un hachage signé cryptographiquement faisant appel à la cryptographie asymétrique, la protection de la confidentialité de la clé utilisée pour produire le hachage, et l'utilisation de la clé publique pour vérifier l'information de hachage. Contrôle connexe : SC-13.

(7) INTÉGRITÉ DES LOGICIELS, DES MICROLOGICIELS ET DE L'INFORMATION | INTÉGRATION DE LA DÉTECTION ET DES INTERVENTIONS

L'organisation intègre la détection de [*Affectation : changements de sécurité apportés au système d'information définis par l'organisation*] à sa capacité d'intervention en cas d'incident.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle aide à s'assurer que les événements sont suivis, surveillés, corrigés et conservés à des fins historiques. Conserver des documents historiques est important pour être mesure de reconnaître et de discerner les actions adversaires pendant une longue période et pour de possibles actions en justice. Les changements qui influent sur la sécurité comprennent, par exemple, les changements non autorisés aux paramètres de configuration, ou l'augmentation non autorisée des privilèges. Contrôles connexes : IR-4, IR-5, SI-4.

(8) INTÉGRITÉ DES LOGICIELS, DES MICROLOGICIELS ET DE L'INFORMATION | VÉRIFICATION DES CAPACITÉS EN CAS D'ÉVÉNEMENT IMPORTANT

Le système d'information, après avoir détecté une possible atteinte à l'intégrité, fournit les capacités nécessaires pour vérifier l'événement et met en œuvre les mesures suivantes : [*Sélection (un ou plusieurs) : générer un enregistrement de vérification; alerter les utilisateurs actuels; alertes [Affectation : personnel désigné par l'organisation]; [Affectation : autres mesures définies par l'organisation]*].

Conseils supplémentaires sur l'amélioration : L'organisation sélectionne des mesures d'intervention du type de logiciel, du logiciel en particulier ou de l'information qui sont possiblement touchés par une atteinte à l'intégrité. Contrôles connexes : AU-2, AU-6, AU-12.

(9) INTÉGRITÉ DES LOGICIELS, DES MICROLOGICIELS ET DE L'INFORMATION | VÉRIFICATION DU PROCESSUS DE DÉMARRAGE

Le système d'information vérifie l'intégrité du processus de démarrage de [*Affectation : appareils désignés par l'organisation*].

Conseils supplémentaires sur l'amélioration : Assurer l'intégrité des processus de démarrage est essentiel pour veiller à ce que les appareils dont on se sert sont sécurisés dès qu'on les allume. Les mécanismes de vérification de l'intégrité assurent les membres du personnel organisationnel que seulement du code sûr est exécuté pendant le processus de démarrage d'un appareil.

(10) INTÉGRITÉ DES LOGICIELS, DES MICROLOGICIELS ET DE L'INFORMATION | PROTECTION DES MICROLOGICIELS DE DÉMARRAGE

Le système d'information met en œuvre [*Affectation : mesures de protection définies par l'organisation*] afin de protéger l'intégrité des micrologiciels de démarrage dans [*Affectation : appareils désignés par l'organisation*].

Conseils supplémentaires sur l'amélioration : Des modifications non autorisées aux micrologiciels de démarrage peuvent être un signe indiquant une attaque ciblée sophistiquée. Ce type de cyberattaque peut avoir comme conséquence un déni de service permanent (p. ex. si le micrologiciel est corrompu) ou la présence persistante d'un code malveillant (p. ex. si le code est intégré au micrologiciel). Des appareils peuvent protéger l'intégrité des micrologiciels de démarrage des systèmes d'information organisationnels en : (i) vérifiant l'intégrité de l'authenticité de toutes les mises à jour des micrologiciels de démarrage avant d'appliquer les changements au moment du démarrage des appareils; (ii) empêchant les processus non autorisés de modifier les micrologiciels de démarrage.

(11) INTÉGRITÉ DES LOGICIELS, DES MICROLOGICIELS ET DE L'INFORMATION | ENVRIONNEMENTS CLOS AUX PRIVILÈGES RESTREINTS

L'organisation nécessite que [*Affectation : logiciels installés par l'utilisateur désignés par l'organisation*] soient exécutés dans un environnement physique clos ou un environnement clos de machine virtuelle dont les privilèges sont restreints.

Conseils supplémentaires sur l'amélioration : L'organisation détermine quels sont les logiciels dont la provenance est une source de préoccupations ou qui pourraient contenir des codes malveillants. Pour ce type de logiciel, l'installation par l'utilisateur a lieu dans un environnement opérationnel clos pour limiter ou contenir les dommages des codes malveillants qui pourraient être exécutés.

(12) INTÉGRITÉ DES LOGICIELS, DES MICROLOGICIELS ET DE L'INFORMATION | VÉRIFICATION DE L'INTÉGRITÉ

L'organisation exige que l'intégrité de [*Affectation : logiciels installés par l'utilisateur désignés par l'organisation*] soit vérifiée avant son exécution.

Conseils supplémentaires sur l'amélioration : L'organisation vérifie l'intégrité des logiciels installés par l'utilisateur avant leur exécution afin de réduire les risques d'exécuter des codes malveillants ou des codes qui contiennent des erreurs dus à des modifications non autorisées. L'organisation considère l'aspect pratique des approches visant à vérifier l'intégrité des logiciels, par exemple, la disponibilité de totaux de contrôle suffisamment fiables émis par les développeurs ou les fournisseurs de logiciels.

(13) INTÉGRITÉ DES LOGICIELS, DES MICROLOGICIELS ET DE L'INFORMATION | EXÉCUTION DE CODE DANS DES ENVIRONNEMENTS PROTÉGÉS

L'organisation permet l'exécution de code binaire ou exécutable sur machine provenant de sources qui n'offrent pas de garantie ou qui offrent une garantie limitée dans les cas où ils n'offrent pas le code source uniquement dans un environnement physique clos ou dans un environnement clos de machine virtuelle avec l'approbation explicite de [*Affectation : personnel ou rôles définis par l'organisation*].

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle s'applique à toutes les sources de code binaire ou exécutable sur machine, notamment, les logiciels et micrologiciels commerciaux et les logiciels de source ouverte.

(14) INTÉGRITÉ DES LOGICIELS, DES MICROLOGICIELS ET DE L'INFORMATION | CODE BINAIRE OU EXÉCUTABLE SUR MACHINE

(a) L'organisation interdit l'utilisation de code binaire ou exécutable sur machine provenant de fournisseurs qui n'offrent pas de garantie ou qui offrent une garantie limitée dans les cas où ils n'offrent pas le code source;

(b) l'organisation prévoit des exceptions à l'exigence relative au code source uniquement dans situations urgentes liées à la mission ou aux besoins opérationnels et avec le consentement écrit exprès de l'autorité responsable.

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle s'applique à toutes les sources de code binaire ou exécutable sur machine, notamment, les logiciels et micrologiciels commerciaux et les logiciels de source ouverte. Les produits logiciels sans code source provenant de fournisseurs qui n'offrent pas de garantie ou qui offrent une garantie limitée, sont évalués au plan de leurs répercussions potentielles sur la sécurité. L'évaluation tient compte du fait que ces types de produits peuvent être très difficiles à examiner, à réparer ou à développer puisque l'organisation n'a pas accès au code source original et qu'aucun propriétaire n'est en mesure d'effectuer ces réparations au nom de l'organisation. Contrôle connexe : SA-5.

(15) INTÉGRITÉ DES LOGICIELS, DES MICROLOGICIELS ET DE L'INFORMATION | AUTHENTIFICATION DES CODES

Le système d'information met en œuvre des mécanismes cryptographiques pour authentifier [*Affectation : composants logiciels ou micrologiciels désignés par l'organisation*] avant leur installation.

Conseils supplémentaires sur l'amélioration : Par authentification cryptographique on entend, notamment, la vérification des composants de logiciels ou de micrologiciels signés numériquement avec des certificats reconnus et approuvés par l'organisation. La signature du code est une méthode efficace de protection contre les codes malveillants.

(16) INTÉGRITÉ DES LOGICIELS, DES MICROLOGICIELS ET DE L'INFORMATION | LIMITE DE TEMPS IMPOSÉE À L'EXÉCUTION SANS SUPERVISION D'UN PROCESSUS

L'organisation interdit l'exécution sans supervision d'un processus pendant plus de [*Affectation : durée définie par l'organisation*].

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle touche les processus dont le délai normal d'exécution peut être déterminé et les situations où ces délais d'exécution sont dépassés au sein de l'organisation. La supervision peut être effectuée notamment à l'aide des horloges des système d'exploitation, des interventions automatisées ou de la surveillance et des interventions manuelles en cas d'anomalies du processus du système d'information.

Références :

Aucune

SI-8 PROTECTION ANTIPOURRIEL

Contrôle :

(A) L'organisation utilise des mécanismes de protection antipourriel aux points d'entrée et de sortie du système d'information pour détecter (et intervenir, le cas échéant) les messages non sollicités.

(B) L'organisation met à jour les mécanismes de protection antipourriel dès la diffusion de nouvelles versions, conformément à sa politique et à ses procédures de gestion des configurations.

Conseils supplémentaires : Les points d'entrée et de sortie du système d'information comprennent, par exemple, les coupe-feux, les serveurs de messagerie électronique, les serveurs Web, les serveurs mandataires et les serveurs d'accès à distance, les postes de travail, les appareils mobiles et les ordinateurs portables. Les pourriels sont transmis par différents moyens, y compris la messagerie électronique, les pièces jointes aux messages électroniques et les accès Web. Les mécanismes de protection contre les pourriels comprennent notamment les définitions de signature. Contrôles connexes : AT-2, AT-3, SC-5, SC-7, SI-3.

Améliorations de contrôle :

(1) PROTECTION CONTRE LES POURRIELS | GESTION CENTRALE

L'organisation centralise la gestion des mécanismes de protection antipourriel.

Conseils supplémentaires sur l'amélioration : La gestion et la mise en œuvre des mécanismes de protection contre les pourriels sont centralisées et effectuées à l'échelle de l'organisation. La gestion centrale comprend la planification, la mise en œuvre, l'évaluation, l'autorisation et la surveillance des contrôles de sécurité antipourriels définis par l'organisation et gérés centralement. Contrôles connexes : AU-3, SI-2, SI-7.

(2) PROTECTION CONTRE LES POURRIELS | MISES À JOUR AUTOMATIQUES

Le système d'information met automatiquement à jour les mécanismes de protection antipourriel.

(3) PROTECTION CONTRE LES POURRIELS | CAPACITÉ DE PERFECTIONNEMENT CONTINU

Le système d'information met en œuvre des mécanismes de protection contre les pourriels ayant une capacité de perfectionnement qui leur permettent d'identifier efficacement le trafic de communications légitime.

Conseils supplémentaires sur l'amélioration : Les mécanismes de perfectionnement comprennent, entre autres, les filtres bayésiens qui mettent à jour les paramètres des algorithmes séparant le trafic légitime et les pourriels en se basant sur les données entrées par les utilisateurs.

Références :

Aucune

SI-9 RESTRICTIONS RELATIVES À LA SAISIE D'INFORMATION

[Annulé : Intégré aux contrôles AC-2, AC-3, AC-5 et AC-6]

SI-10 VALIDATION DE LA SAISIE D'INFORMATION

Contrôle :

(A) Le système d'information vérifie la validité des [*Affectation : saisies d'information définies par l'organisation*].

Conseils supplémentaires : Des règles de vérification de la validité de la syntaxe et des valeurs sémantiques des saisies du système d'information (p. ex. jeu de caractères, longueur, plage numérique, valeurs acceptables) sont mises en place afin d'assurer qu'elles respectent les définitions précisées en matière de format et de contenu. Les applications logicielles suivent habituellement des protocoles bien définis qui utilisent des messages structurés (c.-à-d. des commandes ou des requêtes) pour communiquer entre les modules logiciels ou les composants de système. Les messages structurés peuvent contenir des données brutes ou non structurées parsemées de métadonnées ou d'informations de contrôle. Si des applications logicielles utilisent des données saisies par un attaquant pour construire des messages structurés sans encoder de tels messages de manière adéquate, l'attaquant peut alors insérer des commandes malveillantes ou des caractères spéciaux qui pourraient faire en sorte que les données soient interprétées comme des informations de contrôle ou des métadonnées. Par conséquent, le module ou le composant qui reçoit les saisies corrompues effectuera des opérations erronées ou interprètera les données incorrectement. Les saisies transmises aux interpréteurs sont filtrées au préalable pour empêcher que leur contenu soit interprété accidentellement comme des commandes. La validation des saisies permet de s'assurer que les saisies sont exactes et correctes et de prévenir des attaques, comme les scripts inter-sites (XSS) et toute une gamme d'attaques par injection.

Améliorations de contrôle :

(1) VALIDATION DE LA SAISIE D'INFORMATION | FONCTION DE CORRECTION MANUELLE

(a) Le système d'information a une fonction de correction manuelle liée à la validation des saisies [*Affectation : saisies définies par l'organisation*].

(b) Le système d'information restreint l'utilisation de la fonction de correction manuelle à [*Affectation : personnes autorisées désignées par l'organisation*].

(c) Le système d'information effectue une surveillance de l'utilisation de la fonction de correction manuelle.

Conseils supplémentaires sur l'amélioration : Contrôle connexe : CM-3, CM-5.

(2) VALIDATION DE LA SAISIE D'INFORMATION | EXAMEN / RÉSOLUTION DES ERREURS

L'organisation s'assure que les erreurs de validation de saisies font l'objet d'un examen et sont résolues [*Affectation : délai défini par l'organisation*].

Conseils supplémentaires sur l'amélioration : La résolution des erreurs de validation de saisies comprend, par exemple, la correction des causes d'erreurs systémiques et la répétition des transactions une fois la saisie corrigée.

(3) VALIDATION DE LA SAISIE D'INFORMATION | COMPORTEMENTS PRÉVISIBLES

Lorsque des saisies non valides sont reçues, le système d'information se comporte d'une manière prévisible et informée à l'image des objectifs de l'organisation et du système.

Conseils supplémentaires sur l'amélioration : Une vulnérabilité que l'on retrouve souvent dans les systèmes d'information des organisations est le comportement imprévisible des systèmes lorsque des saisies non valides sont reçues. Cette amélioration de contrôle fait en sorte que le comportement du système est prévisible en cas de saisies non valides en précisant les interventions que le système d'information doit mettre en œuvre, ce qui facilite la transition du système vers un état connu sans incidences négatives ou imprévues.

(4) VALIDATION DE LA SAISIE D'INFORMATION | EXAMEN / CHRONOMÉTRAGE DES INTERACTIONS

L'organisation est responsable de chronométrer les interactions entre les composants du système d'information lorsque vient le temps de déterminer les interventions appropriées en cas de saisies non valides.

Conseils supplémentaires sur l'amélioration : Le chronométrage des interfaces prend toute son importance lors des interventions requises quand des saisies non valides sont reçues dans les interfaces de protocole du système d'information et quand un protocole doit mesurer l'incidence de l'intervention sur les

autres protocoles de la pile de protocoles. Par exemple, les protocoles réseau sans fil de la norme 802.11 n'interagissent pas très bien avec les protocoles de contrôle de transmission (TCP) lorsque des paquets sont supprimés (ce qui pourrait être causé par l'entrée d'un paquet non valide). Les TCP laissent présumer que les pertes de paquets sont dues à la congestion, tandis que les paquets perdus sur les liens 802.11 le sont habituellement en raison de collisions ou de bruit sur le lien. Si le TCP intervient pour une congestion, il effectue précisément la mauvaise intervention pour régler un événement de collision. Les adversaires peuvent être en mesure d'utiliser des comportements de protocoles apparemment acceptables de concert pour atteindre des résultats nuisibles grâce à la construction de saisies non valides.

(5) VALIDATION DE LA SAISIE D'INFORMATION | PERMETTRE UNIQUEMENT LES SAISIES PROVENANT DE SOURCES DE CONFIANCE ET DE FORMATS APPROUVÉS

L'organisation ne permet que l'utilisation de saisies d'information de [*Affectation : sources de confiance désignées par l'organisation*] ou [*Affectation : formats désignés par l'organisation*].

Conseils supplémentaires sur l'amélioration : Cette amélioration de contrôle applique le concept de la liste blanche aux saisies d'information. Préciser les sources de confiance pour la saisie d'information et les formats acceptables de ces saisies réduit les risques d'activités malveillantes.

Références :

Aucune

SI-11 TRAITEMENT DES ERREURS

Contrôle :

(A) Le système d'information génère des messages d'erreur qui fournissent les informations nécessaires à l'application de mesures correctives sans toutefois révéler des informations qui pourraient être exploitées par des adversaires.

(B) Le système d'information révèle les messages d'erreur seulement [*Affectation : personnel ou rôles définis par l'organisation*].

Conseils supplémentaires : L'organisation élabore soigneusement la structure et le contenu des messages d'erreur. La mesure dans laquelle le système d'information peut identifier et traiter les conditions d'erreur est dictée par les politiques et les exigences opérationnelles de l'organisation. Les adversaires pourraient notamment exploiter les informations suivantes : tentative échouée de connexion où le mot de passe est saisi dans le champ du nom d'utilisateur, des renseignements opérationnels ou liés à la mission pouvant être déduits (ou se retrouvant explicitement) dans des informations consignées, et des renseignements personnels comme des numéros de compte, numéros d'assurance sociale ou des numéros de carte de crédit. En outre, les messages d'erreur peuvent servir de voie clandestine pour la transmission d'informations. Contrôles connexes : AU-2, AU-3, SC-31.

Améliorations de contrôle :

Aucune

Références :

Aucune

SI-12 TRAITEMENT ET CONSERVATION DES SORTIES D'INFORMATION

Contrôle :

(A) L'organisation traite et conserve l'information interne et celle produite par le système d'information conformément aux lois du GC, aux politiques, directives et normes applicables du SCT et aux exigences opérationnelles.

Conseils supplémentaires : Les exigences de traitement et de conservation des sorties s'appliquent à l'ensemble du cycle de vie de l'information et, dans certains cas, vont au-delà du retrait du système d'information lui-même. Bibliothèque et Archives Canada donne des conseils sur la conservation des dossiers. Contrôles connexes : AC-16, AU-5, AU-11, MP-2, MP-4.

Améliorations de contrôle :

Aucune

Références :

Aucune

SI-13 PRÉVENTION DES PANNES PRÉVISIBLES

Contrôle :

(A) L'organisation détermine la durée moyenne de fonctionnement avant défaillance (MTTF pour *mean time to failure*) [*Affectation : composants de systèmes d'information désignés par l'organisation*] dans des environnements d'exploitation donnés.

(B) L'organisation fournit des composants de système d'information de remplacement et un mécanisme d'échange des rôles actifs et passifs des composants [*Affectation : critères de remplacement MTTF définis par l'organisation*].

Conseils supplémentaires : La durée moyenne de fonctionnement avant défaillance est avant tout un élément de fiabilité; ce contrôle met l'accent sur les défaillances potentielles de composants de système d'information particuliers qui fournissent les capacités de sécurité. Les taux de défaillance sont propres aux installations et ne tiennent pas compte des moyennes définies par l'industrie. L'organisation définit les critères de substitution des composants du système d'information en se basant sur la durée moyenne de fonctionnement avant défaillance et en considérant les dommages que causerait une éventuelle défaillance des composants. Le transfert des responsabilités entre les composants de système d'information actifs et passifs ne compromet en rien la sûreté, l'état de préparation opérationnelle ni la sécurité (p. ex. les variables d'état sont préservées). Le composant passif est accessible en permanence, sauf pendant une procédure de reprise après défaillance ou pour des motifs de maintenance. Contrôles connexes : CP-2, CP-10, MA-6.

Améliorations de contrôle :

(1) PRÉVENTION DES PANNES PRÉVISIBLES | TRANSFERT DES RESPONSABILITÉS D'UN COMPOSANT

L'organisation met le composant de système d'information hors service en transférant ses responsabilités à un composant de remplacement à l'intérieur de [*Affectation : fraction ou pourcentage définis par l'organisation*] de la durée moyenne de fonctionnement avant défaillance.

(2) PRÉVENTION DES PANNES PRÉVISIBLES | LIMITE DE TEMPS IMPOSÉE À L'EXÉCUTION DU PROCESSUS SANS SUPERVISION

[Annulée : Intégrée au contrôle SI-7 (16)]

(3) PRÉVENTION DES PANNES PRÉVISIBLES | TRANSFERT MANUEL ENTRE LES COMPOSANTS

L'organisation lance manuellement un transfert entre les composants actifs et passifs [*Affectation : fréquence définie par l'organisation*] si la durée moyenne de fonctionnement avant défaillance est supérieure à [*Affectation : durée définie par l'organisation*].

(4) PRÉVENTION DES PANNES PRÉVISIBLES | INSTALLATION DES COMPOSANTS PASSIFS / NOTIFICATION

(a) L'organisation, lors de la détection d'une défaillance d'un composant de système d'information s'assure que le composant de système d'information passif est installé en moins de [*Affectation : durée définie par l'organisation*];

(b) L'organisation, lors de la détection d'une défaillance d'un composant de système d'information [*Sélection (un ou plusieurs): active [Affectation : alarme définie par l'organisation]; arrête automatiquement le système*].

Conseils supplémentaires sur l'amélioration : Le transfert automatique ou manuel de composants du mode passif au mode actif peut survenir, par exemple, lorsque la défaillance d'un composant est détectée.

(5) PRÉVENTION DES PANNES PRÉVISIBLES | CAPACITÉ DE BASCULEMENT

L'organisation offre [*Affectation : capacité de basculement définie par l'organisation]* pour le système d'information en [*Sélection : temps réel; temps quasi réel*].

Conseils supplémentaires sur l'amélioration : Par basculement, on entend le passage automatique à un système d'information de remplacement lors de la défaillance du système d'information principal. La capacité de basculement comprend, par exemple, le miroitage des opérations du système d'information dans un site de traitement de secours ou le miroitage périodique des données à intervalles réguliers durant une période définie par la durée de reprise de l'organisation.

Références :

Aucune

SI-14 NON-PERSISTANCE

Contrôle :

(A) L'organisation met en œuvre des [*Affectation : comsposants du système d'information et services définis par l'organisation*] non persistants initialisés dans un état connu et interrompus [*Sélection (un ou plusieurs) : à la fin de la période d'utilisation; périodiquement [Affectation : fréquence déterminée par l'organisation]*].

Conseils supplémentaires : Ce contrôle atténue les risques liés aux menaces persistantes évoluées en réduisant considérablement la capacité de ciblage des adversaires (p. ex. les créneaux et la surface d'attaque) qui préparent et lancent des cyberattaques. En mettant en œuvre le concept de non-persistance à des composants sélectionnés du système d'information, l'organisation dispose de ressources informatiques dont l'état est connu, et ce, pendant une période précise qui ne laisse pas le temps aux adversaires d'exploiter les vulnérabilités des systèmes d'information de l'organisation ni des environnements dans lesquels ces systèmes sont exploités. Puisque la menace persistante sophistiquée est une menace de pointe en ce qui a trait à ses capacités, à ses intentions et à l'établissement de cibles, les organisations présument qu'à long terme, un certain pourcentage de cyberattaques sont réussies. Les composants et services non persistants du système d'information sont activés au besoin à l'aide d'information protégées et sont interrompus périodiquement ou à la fin de la session. La non-persistance accroît la somme de travail des adversaires qui tentent de compromettre ou de pénétrer les systèmes d'information organisationnels.

Des composants non persistants du système peuvent être mis en œuvre, par exemple, en effectuant un redéploiement périodique de l'image ou en utilisant différentes de techniques communes de virtualisation. Des services non persistants peuvent être mis en œuvre grâce à des techniques de virtualisation dans des machines virtuelles ou comme nouvelles instances de processus dans des machines physiques (persistantes ou non persistantes). L'avantage des changements périodiques des composants ou services du système d'information est que l'organisation n'a pas besoin de d'abord déterminer si des compromissions ont eu lieu dans les composants ou services (ce qui est souvent difficile à déterminer). Les composants et services sont changés en respectant une fréquence équilibrée pour prévenir le déploiement d'attaques tout en conservant la stabilité du système d'information. Dans certains cas, la restauration de composants et services essentiels peut être effectuée périodiquement afin d'empêcher les adversaires d'exploiter les vulnérabilités optimales du système. Contrôles connexes : SC-30, SC-34.

Améliorations de contrôle :

(1) NON-PERSISTANCE | RESTAURATIONS EFFECTUÉES À PARTIR DE SOURCES DE CONFIANCE

L'organisation s'assure que les logiciels et les données utilisés pour la restauration des composants et services du système d'information proviennent de [*Affectation : sources de confiance désignées par l'organisation*].

Conseils supplémentaires sur l'amélioration : Les sources de confiance comprennent, par exemple, les disques optiques non réinscriptibles provenant d'installations sélectionnées de stockage hors ligne.

Références :

Aucune

SI-15 FILTRAGE DES SORTIES D'INFORMATION

Contrôle :

(A) Le système d'information valide les sorties d'information de [*Affectation : programmes ou applications logiciels désignés par l'organisation*] pour s'assurer que l'information est conforme au contenu auquel l'on s'attend.

Conseils supplémentaires : Certains types de cyberattaques (p. ex. injections SQL) produisent des sorties d'information inattendues ou en contradiction avec les résultats auxquels l'on s'attend en temps normal de la part des applications ou programmes logiciels. Cette amélioration de contrôle met l'accent sur la détection de contenu étranger ou superflu pour l'empêcher de s'afficher, tout en alertant les outils de surveillance que des comportements anormaux ont été découverts. Contrôles connexes : SI-3, SI-4.

Améliorations de contrôle :

Aucune

Références :

Aucune

SI-16 PROTECTION DE LA MÉMOIRE

Contrôle :

(A) Le système d'information met en œuvre [*Affectation : mesures de sécurité définies par l'organisation*] pour protéger sa mémoire de l'exécution de codes non autorisés.

Conseils supplémentaires : Certains adversaires lancent des attaques dans l'intention d'exécuter des codes dans des régions de mémoire non exécutables ou dans des régions de mémoire interdites. Les mesures de sécurité employées pour protéger la mémoire comprennent, par exemple, la prévention de l'exécution de données et le mécanisme de distribution aléatoire de l'espace d'adressage (*Address Space Layout Randomization*). Les mesures de sécurité contre l'exécution de données peuvent être renforcées par du matériel ou des logiciels auxquels sont ajoutés des éléments matériels qui renforcent le mécanisme. Contrôles connexes : AC-25, SC-3.

Améliorations de contrôle :

Aucune

Références :

Aucune

SI-17 PROCÉDURES DE SÉCURITÉ INTÉGRÉE

Contrôle :

(A) Le système d'information met en œuvre [*Affectation : procédures de sécurité intégrée définies par l'organisation*] lorsque [*Affectation : l'organisation doit définir quelles défaillances précises se produisent*].

Conseils supplémentaires : Les conditions de défaillance comprennent, notamment, la perte de communication entre des composants essentiels du système ou entre des composants du système et les installations opérationnelles. Les mesures de sécurité intégrée comprennent, entre autres, les alertes à l'intention du personnel et la diffusion de consignes claires sur les prochaines étapes à suivre (p. ex. ne rien faire, réétablir les paramètres de système, arrêter les processus, redémarrer le système ou communiquer avec le personnel désigné de l'organisation). Contrôles connexes : CP-12, CP-13, SC-24, SI-13.

Améliorations de contrôle :

Aucune

Références :

Aucune

4. Références

Numéro de la référence	Titre du document	Contrôles de sécurité concernés
[Référence 1]	National Institute of Standards and Technology (NIST). Special Publication 800-53 Revision 4 *Security and Privacy Controls for Federal Information Systems*. Avril 2013. Comprend les mises à jour en date du 15 janvier 2014.	s.o.
[Référence 2]	Travaux publics et Services gouvernementaux Canada. *Manuel de la sécurité industrielle.* Juillet 2009.	PE-3, PS-3
[Référence 3]	Centre de la sécurité des télécommunications Canada et Gendarmerie royale du Canada. *Méthodologie harmonisée d'évaluation des menaces et des risques* (TRA-1). Octobre 2007.	RA-3
[Référence 4]	National Institute of Standards and Technology (NIST). FIPS PUB 140-2, *Security Requirements for Cryptographic Modules.* Le 25 mai 2001.	IA-7
[Référence 5]	Secrétariat du Conseil du Trésor du Canada. *Politique sur l'utilisation acceptable des dispositifs et des réseaux*. Le 1er octobre 2013.	AC-8
[Référence 6]	Secrétariat du Conseil du Trésor du Canada. *Norme opérationnelle sur la sécurité micrologicielle.* Le 1er décembre 2004.	AC-17, CP-9, MP-1, MP-5, PE-1, PE-2, PE-3, PE-17
[Référence 7]	Secrétariat du Conseil du Trésor du Canada. *Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information.* Le 31 mai 2004.	AC-1, AC-17, AC-19, AT-1, AT-2, AU-1, AU-6, CA-1, CA-2, CA-5, CA-6, CM-1, CP-1, CP-2, CP-9, CP-10, IA-1, IR-1, IR-5, MA-1, MP-1, PE-1, PL-1, PL-2, PS-1, RA-1, SA-1, SA-2, SA-3, SC-1, SI-1
[Référence 8]	Centre de la sécurité des télécommunications. ITSA-11 *Algorithmes cryptographiques approuvés par le CST pour la protection des renseignements protégés et pour les applications d'autorisation et d'authentification électroniques au sein du gouvernement du Canada*. Mars 2011.	IA-7, MP-5, SA-4, SC-12, SC-13, SC-28
[Référence 9]	Secrétariat du Conseil du Trésor du Canada. *Norme sur le filtrage de sécurité.* Le 20 octobre 2014.	PS-2, PS-3, PS-4, PS-5, PS-7
[Référence 10]	Secrétariat du Conseil du Trésor du Canada. *Directive sur la gestion de la sécurité ministérielle.* Le 1er juillet 2009.	CA-1, CA-2, CA-6, CA-7
[Référence 11]	Secrétariat du Conseil du Trésor du Canada. *Norme de sécurité opérationnelle – Programme de planification de la continuité des activités.* Le 23 mars 2004.	CP-1, CP-2
[Référence 12]	Secrétariat du Conseil du Trésor du Canada. *Norme opérationnelle de sécurité – Niveaux de préparation des installations du gouvernement fédéral*. Le 1er novembre 2002.	CP-2, IR-1
[Référence 13]	Secrétariat du Conseil du Trésor du Canada. *Norme de sécurité relative à l'organisation et l'administration.* Le 1er juin 1995.	AC-21, IR-1, MP-3, RA-3

Numéro de la référence	**Titre du document**	**Contrôles de sécurité concernés**
[Référence 14]	Centre de la sécurité des télécommunications. ITSD-01A *Directives pour l'application de la sécurité des communications au sein du gouvernement du Canada.* Janvier 2005.	PE-19, SC-13
[Référence 15]	Gendarmerie royale du Canada. Guide G1-001, *Guide d'équipement de sécurité.* (*Diffusion retreinte*)	MP-4, MP-6
[Référence 16]	Centre de la sécurité des télécommunications. ITSG-06 *Effacement et déclassification des supports d'information électroniques.* Juillet 2006.	MP-4, MP-6, MP-8
[Référence 17]	Gendarmerie royale du Canada. G1-009 *Transport et transmission de renseignements protégés ou classifiés*. Décembre 2006. (*Diffusion retreinte*)	MP-5
[Référence 18]	Centre de la sécurité des télécommunications. ITSG-31 *Guide sur l'authentification des utilisateurs pour les systèmes TI.* Mars 2009.	AU-10, IA-2, IA-5, IA-7, IA-8, MA-4
[Référence 19]	Conseil national de recherche du Canada. *Code national du bâtiment – Canada (CNB)*. 2010.	PE-3
[Référence 20]	Conseil national de recherches du Canada. *Code national de prévention des incendies – Canada (CNPI)*. 2010.	PE-3
[Référence 21]	Gendarmerie royale du Canada. Guide G1-010, *Éléments du Code national du bâtiment 1995 touchant la sécurité*. Avril 1998. (*Archivé*)	PE-3
[Référence 22]	Supprimé	
[Référence 23]	Gendarmerie royale du Canada. G1-029, *Pièces sécuritaires*. Avril 2006. (*Diffusion retreinte*)	MP-4, PE-3
[Référence 24]	Secrétariat du Conseil du Trésor du Canada. *Directive sur l'évaluation des facteurs relatifs à la vie privée.* Le 1er avril 2010.	PL-5
[Référence 25]	Secrétariat du Conseil du Trésor du Canada. *Norme de sécurité et de gestion des marchés.* Le 9 juin 1996.	PS-7, SA-4, SA-9
[Référence 26]	Supprimé	
[Référence 27]	Centre de la sécurité des télécommunications. ITSPSR-21A *Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802,11*. Mai 2009.	AC-18, AC-19
[Référence 28]	Centre de la sécurité des télécommunications. ITSB-40A *Politique du gouvernement du Canada pour la protection de l'information classifiée à l'aide d'algorithmes Suite B.* Mars 2011.	IA-7, MP-5, SA-4, SC-12, SC-13, SC-28
[Référence 29]	Secrétariat du Conseil du Trésor du Canada. *Lignes directrices sur les responsabilités des dirigeants de la vérification*. Septembre 1995. (*Archivé*)	PL-2
[Référence 30]	Centre de la sécurité des télécommunications. ITSA-23 *Services de soutien des produits de sécurité offerts par les fournisseurs*. Janvier 2002. (*Diffusion retreinte*)	MA-5
[Référence 31]	Supprimé	
[Référence 32]	Supprimé	
[Référence 33]	Centre de la sécurité des télécommunications. ITSB-57B *Sécurité de la messagerie Blackberry NIP à NIP.* Mars 2011.	AC-18, AC-19

Numéro de la référence	Titre du document	Contrôles de sécurité concernés
[Référence 34]	Centre de la sécurité des télécommunications. ITSB-60 *Conseils sur l'utilisation du protocole TLS (Transport Layer Security) au sein du gouvernement du Canada*. Novembre 2008.	AC-18, IA-2
[Référence 35]	Centre de la sécurité des télécommunications. ITSG-02 *Critères pour la conception, la fabrication, l'approvisionnement, l'installation et les essais de réception des enceintes blindées contre les radiofréquences*. Août 1999.	AC-18, PE-18
[Référence 36]	Centre de la sécurité des télécommunications. ITSD-03A *Directive sur le contrôle du micrologiciel COMSEC au sein du gouvernement du Canada*. Mars 2014.	AU-1, CP-1, CP-2, IR-1, IR-4, IR-6, MP-1, MP-5, MP-6, PE-2, PE-3, SC-12
[Référence 37]	Centre de la sécurité des télécommunications. ITSG-11 *Planification des installations COMSEC – Conseils et critères TEMPEST*. Septembre 2002. (*Diffusion retreinte*)	PE-19
[Référence 38]	Centre de la sécurité des télécommunications. ITSG-12 *Procédures d'évaluation Facilité du gouvernement du Canada*. Septembre 2005. (*Diffusion retreinte*)	PE-19
[Référence 39]	Centre de la sécurité des télécommunications. ITSG-13 *Manuel sur la commande de clés cryptographiques*. Mai 2006.	SC-12
[Référence 40]	Centre de la sécurité des télécommunications. ITSG-20 *Sécurité de base recommandée pour Windows Server 2003*. Mars 2004.	CM-6
[Référence 41]	Centre de la sécurité des télécommunications. ITSG-22 *Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada*. Juin 2007.	AC-4, CA-3, SC-5, SC-7
[Référence 42]	Centre de la sécurité des télécommunications. ITSG-23 *Isolement d'un serveur d'entreprise BlackBerry dans un environnement Microsoft Exchange*. Mars 2007.	CM-6, SC-3, SC-7
[Référence 43]	Centre de la sécurité des télécommunications. ITSG-38 *Établissement des zones de sécurité dans un réseau – Considérations de conception relatives au positionnement des services dans les zones*. Mai 2009.	CA-3, SC-3, SC-7
[Référence 44]	Gendarmerie royale du Canada. B2-002, *Produits de réécriture des supports de TI et d'effacement sécurisé*. Mai 2009.	MP-6
[Référence 45]	Gendarmerie royale du Canada. G1-005 *Guide pour la préparation d'un énoncé de sécurité micrologicielle*. Janvier 2000.	PE-2, PE-3, PE-4
[Référence 46]	Gendarmerie royale du Canada. G1-006, *Cartes d'identité / Insignes d'accès*. Juillet 2006.	PE-2
[Référence 47]	Gendarmerie royale du Canada. G1-007, *Scellage de protection des clés d'urgence et passe-partout ou des serrures à code d'immeubles*. (*Archivé*)	PE-3
[Référence 48]	Gendarmerie royale du Canada. G1-008, *Lignes directrices visant les services de gardiens*. Avril 2001. (*Archivé*)	PE-3
[Référence 49]	Gendarmerie royale du Canada. G1-016, *Les systèmes de clés maîtresses*. Décembre 1981. (*Archivé*)	PE-3
[Référence 50]	Gendarmerie royale du Canada. G1-024, *Contrôle de l'accès*. Août 2004.	PE-2, PE-3, PE-16

Numéro de la référence	**Titre du document**	**Contrôles de sécurité concernés**
[Référence 51]	Gendarmerie royale du Canada. G1-025, *Protection, détection et intervention*. Décembre 2004. (*Diffusion retreinte*)	PE-1, PE-2, PE-3, PE-6
[Référence 52]	Gendarmerie royale du Canada. G1-026, *Guide pour l'établissement des zones de sécurité micrologicielle*. Septembre 2005.	PE-3, PE-4, PE-5, PE-18
[Référence 53]	Gendarmerie royale du Canada. G1-031, *Protection micrologicielle des serveurs informatiques*. Mars 2008.	PE-3
[Référence 54]	Gendarmerie royale du Canada. G2-003, *Lignes directrices sur l'élimination et la destruction des renseignements protégés sur disques durs*. Octobre 2003. (*Archivé*)	MP-6
[Référence 55]	Committee on National Security Systems. CNSSI 5000, *Guidelines For Voice Over Internet Protocol (VOIP) Computer Telephony*. Avril 2007 (remplace National Telecommunications Security Working Group. TSG Standard 2 Guidelines for Computerized Telephone Systems. Mars 1990.)	SC-101
[Référence 56]	Committee on National Security Systems. CNSSI 5006 *National Instruction for Approved Telephone Equipment*. Septembre 2011. (remplace National telecommunications Security working Group. *TSG Standard 6 TSG-Approved Equipment*. Juin 2006.)	SC-101
[Référence 57]	Centre de la sécurité des télécommunications. ITSG-33 *Gestion des risques de la sécurité des TI : Approche cycle de vie (ITSG-33)* – Aperçu. Le 1er novembre 2012.	s.o.
[Référence 58]	Centre de la sécurité des télécommunications. ITSG-33 – *Annexe 2, La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie – Activités de gestion des risques liés à la sécurité des systèmes d'information.* Le 1er novembre 2012.	CA-5, RA-2, RA-3, SA-13
[Référence 59]	Committee on National Security Systems. CNSSI 5002 *National Information Assurance (IA) Instruction for Computerized Telephone Systems*. Le 24 février 2012.	SC-101
[Référence 60]	Secrétariat du Conseil du Trésor du Canada. *Norme sur l'assurance de l'identité et des justificatifs.* Le 1er février 2013.	IA-8
[Référence 61].	Secrétariat du Conseil du Trésor du Canada. *Ligne directrice sur la définition des exigences en matière d'authentification.* (pas de date)	IA-8
[Référence 62]	Secrétariat du Conseil du Trésor du Canada. *Guideline on Identity Assurance.* (pas de date)	IA-8
[Référence 63]	Secrétariat du Conseil du Trésor du Canada. *Politique sur la sécurité du gouvernement* (PSG). Le 1er juillet 2009.	AT-3, AC-16
[Référence 64]	Centre de la sécurité des télécommunications. ITSB-104 *Répercussions sur la sécurité de l'exposition de systèmes TI classifiés à des dispositifs mobiles et à des signaux sans fil. Octobre 2014.*	AC-19
[Référence 65]	Centre de la sécurité des télécommunications. ITSB-95 *Utilisation d'une liste blanche des applications - Conseils à l'intention du gouvernement du Canada.* Janvier 2013.	CM-10

Numéro de la référence	**Titre du document**	**Contrôles de sécurité concernés**
[Référence 66]	Centre de la sécurité des télécommunications. ITSB-89 Version *3 Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information du gouvernement du Canada*. Novembre 2014.	CM-10, SC-44
[Référence 67]	Secrétariat du Conseil du Trésor du Canada. *Plan de gestion des incidents des technologies de l'information du gouvernement du Canada.* Le 10 mai 2012.	IR-1, IR-4, IR-5, IR-6, IR-8, IR-9, IR-10, SI-5
[Référence 68]	Secrétariat du Conseil du Trésor du Canada. *Avis de mise en œuvre de la Politique sur la technologie de l'information 2014-01*. Janvier 2015	MP-1, MP-4, MP-5, MP-6, MP-7, MP-8
[Référence 69]	Centre de la sécurité des télécommunications. ITSB-112 *Questions de sécurité relatives à l'utilisation de supports amovibles pour les renseignements Protégé C et classifiés.* Août 2015.	MP-4
[Référence 70]	Secrétariat du Conseil du Trésor du Canada. *Politique sur l'utilisation acceptable des dispositifs et des réseaux.* Le 1er octobre 2013	PL-4
[Référence 71]	Centre de la sécurité des télécommunications. ITSB-66 *Les risques à la cybersécurité associés à l'utilisation de médias sociaux*. Septembre 2013.	PL-4
[Référence 72]	Centre de la sécurité des télécommunications. TSCG-01\G *Clauses contractuelles liées à l'équipement et aux services de télécommunication*. Le 15 octobre 2010.	SA-12, SA-19
[Référence 73]	Secrétariat du Conseil du Trésor du Canada. *Norme de sécurité relative à l'organisation et l'administration.* (pas de date)	AC-16
[Référence 74]	Secrétariat du Conseil du Trésor du Canada. *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI).* (pas de date)	SC-17
[Référence 75]	Secrétariat du Conseil du Trésor du Canada. *Cadre de politique sur la gestion des actifs et services acquis.* Le 1er novembre 2016.	PE-20

4.1 Références supplémentaires

Cette section établit une correspondance entre les publications de tiers (non gouvernementales) et les publications sur la sécurité de l'information et les contrôles de sécurité mentionnés dans la présente annexe. Les praticiens de la sécurité, lorsqu'il n'existe aucune publication équivalente du GC, peuvent consulter ces publications pour la conception, la mise en œuvre et la sélection de solutions de sécurité. Au fur et à mesure que des documents équivalents du GC deviendront disponibles, la section des références sera mise à jour.

Titre du document	**Contrôles de sécurité concernés**
NIST Special Publication 800-16. *A Role Based Model for Federal Information/Cybersecurity Training*. Mars 2014. Première révision (Ébauche).	AT-1, AT-2, AT-3
NIST Special Publication 800-34. *Contingency Planning Guide for Federal Information Systems*. Mai 2010. Première révision.	CP-1, CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, IR-1, IR-2, IR-3, IR-8, RA-3, PL-6
NIST Special Publication 800-57. *Recommendation for Key Management Part 3: Application-Specific Key Management Guidance*. Mai 2014. Première révision (Ébauche).	AC-3, IA-2, IA-5, IA-6, IA-8, MP-2, MP-4, MP-5, SC-8, SC-9, SC-12, SC-13, SC-17, SC-20, SC-21, NC-1
NIST Special Publication 800-61. *Computer Security Incident Handling Guide*. Août 2012. Deuxième révision.	Tous les contrôles des familles AU et IR
NIST Special Publication 800-81-2. *Secure Domain Name System (DNS) Deployment Guide.* Septembre 2013. Première révision.	SC-20, SC-21, SC-22
NIST Special Publication 800-118. *Guide to Enterprise Password Management*. Avril 2009. Ébauche.	AC-3, AC-7, IA-5, IA-6