CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Les meilleures mesures pour renforcer la cybersécurité des petites et moyennes entreprises

Février 2024 | ITSAP.10.035

Vous êtes à la recherche de mesures que vous pouvez prendre pour protéger les réseaux et l'information de votre entreprise contre les cybermenaces? Pour vous aider, nous avons résumé les treize catégories de contrôles de sécurité que nous avons identifiées dans Contrôles de cybersécurité de base pour les petites et moyennes organisations. En mettant en œuvre ces contrôles, vous pouvez réduire les risques et améliorer votre capacité de réagir aux incidents de sécurité. Nous vous encourageons à en adopter le plus grand nombre possible pour renforcer votre cybersécurité.

Comment utiliser ces contrôles

Ces contrôles ne font pas partie d'une approche universelle à l'égard de la cybersécurité. Ce sont des lignes directrices à utiliser pour créer le cadre de cybersécurité propre à votre organisation.

Vous devriez délimiter et adapter ces contrôles en fonction des besoins et des exigences de votre organisation. Adoptez autant de ces contrôles que possible pour renforcer votre posture de cybersécurité et aider à réduire les risques de cyberattaques. Commencez par les quatre contrôles ci-dessous pour améliorer la sécurité de votre organisation :

- Élaborer un plan d'intervention en cas d'incident;
- Appliquer des correctifs aux applications et aux systèmes d'exploitation;
- Adopter une authentification robuste des utilisateurs;
- Faire des sauvegardes et chiffrer les données.

Avant de mettre en œuvre ces contrôles, ayez en tête les conseils suivants :

- Veillez à identifier les ressources opérationnelles et les systèmes essentiels auxquels vous appliquerez ces contrôles;
- Assurez-vous de bien comprendre les principales menaces qui pèsent sur votre organisation;
- Identifiez vos informations et vos systèmes importants, et appliquez-leur des plans de gestion des risques pour améliorer votre posture de sécurité;
- Adoptez certains ou l'ensemble de ces contrôles, et vous serez en mesure d'observer un impact notable sur la résilience de votre organisation et sa protection contre les cybermenaces.

Élaborer un plan d'intervention en cas d'incident

Lorsque vous disposez d'un plan, vous pouvez rapidement faire face aux incidents, restaurer les données et les systèmes essentiels, et limiter le plus possible les interruptions de services et la perte de données. Dans le cas d'une petite organisation, par exemple, cela pourrait vouloir dire de conserver une liste de personnes avec lesquelles communiquer en cas d'incident. Votre plan devrait comprendre des stratégies pour sauvegarder vos données.

Élaboration d'un plan de reprise informatique personnalisé (ITSAP.40.004)

Élaborer un plan d'intervention en cas d'incident (ITSAP.40.003)

Êtes-vous victime de piratage? (ITSAP.00.015)

Comment prévenir les rançongiciels et s'en remettre (ITSAP.00.099)

Appliquer des correctifs aux applications et aux systèmes d'exploitation

Lorsque des problèmes ou des vulnérabilités sont repérés, les fournisseurs publient des correctifs pour corriger les bogues, résoudre les vulnérabilités et améliorer l'utilisabilité ou la performance. Dans la mesure du possible, activez l'application automatique de correctifs et de mises à jour pour tous les logiciels et tout le matériel, afin d'empêcher les auteures et auteurs de menace d'exploiter ces problèmes ou ces vulnérabilités.

Application des mises à jour sur les dispositifs (ITSAP.10.096)

Adopter une authentification robuste des utilisateurs

Mettez en œuvre des politiques d'authentification des utilisateurs qui permettent un équilibre entre la sécurité et l'utilisabilité. Vous devez vous assurer que les dispositifs authentifient les utilisateurs avant qu'ils n'accèdent à vos systèmes. Dans la mesure du possible, utilisez l'authentification à deux facteurs (A2F) ou l'authentification multifacteur (AMF).

Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)

Étapes à suivre pour déployer efficacement l'authentification multifacteur (AMF) ITSAP.00.105)

Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)

Repensez vos habitudes en regard de vos mots de passe de manière à protéger vos comptes des pirates informatiques (ITSAP.30)

Sauvegarder et chiffrer les données

Copiez vos informations et vos applications essentielles vers au moins un emplacement sécurisé, comme le nuage ou un disque dur externe. Dans l'éventualité d'un cyberincident ou d'une catastrophe naturelle, ces copies vous permettront de poursuivre vos activités commerciales et d'éviter les pertes de données. Les sauvegardes peuvent se faire en ligne ou hors ligne, et elles peuvent également être réalisées en trois itérations différentes : complète, différentielle ou incrémentielle. Effectuez régulièrement des tests des sauvegardes pour vous assurer de pouvoir restaurer les données, le cas échéant.

Sauvegarder et récupérer vos données (ITSAP.40.002)

Utiliser le chiffrement pour assurer la sécurité des données sensibles (ITSAP.40.016)

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

Les meilleures mesures pour renforcer la cybersécurité des petites et moyennes entreprises

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Février 2024 | ITSAP.10.035

Activer les logiciels de sécurité

Activez des coupe-feux et installez un antivirus et un anti-maliciel sur vos appareils pour contrecarrer les attaques malveillantes et assurer une protection contre les maliciels. Assurez-vous de télécharger les logiciels à partir d'un réseau sécurisé et auprès de fournisseurs reconnus. Installez un filtre de système d'adressage par domaines (DNS) sur vos appareils mobiles pour bloquer les sites Web malveillants et filtrer le contenu dangereux.

Les outils de sécurité préventive (ITSAP.00.058)

Système d'adressage par domaine de protection (ITSAP.40.019)

Former les employés

Adaptez vos programmes de formation pour répondre aux protocoles, aux politiques et aux procédures de cybersécurité de l'organisation. Selon la taille de votre organisation, la formation pourrait être élaborée à l'interne ou achetée par l'entremise d'un fournisseur reconnu. Pouvoir compter sur un personnel averti peut réduire la possibilité que surviennent des cyberincidents.

Offrir aux employés une formation sur mesure en cybersécurité (ITSAP.10.093)

Sécuriser les services infonuagiques et externalisés

Avant de signer un contrat avec un fournisseur de services, apprenez à le connaître. Assurez-vous que le fournisseur de services a des mesures en place pour répondre à vos exigences et à vos besoins en matière de sécurité. Renseignez-vous pour savoir où se trouvent les centres de données d'un fournisseur de services. Les exigences en matière de protection de la vie privée et de protection des données peuvent varier d'un pays à l'autre.

Avantages et risques liés à l'adoption des services fondés sur l'infonuagique par votre organisation (ITSE.50.060)

Modèles de l'infonuagique (ITSAP.50.111)

Facteurs à considérer par les clients de services gérés en matière de cybersécurité (ITSM.50.030)

Sécuriser les supports amovibles

Les supports amovibles, comme les clés USB, offrent un moyen pratique et économique pour stocker et transférer des données. Par contre, il est possible de les perdre ou de se les faire voler. Conservez un inventaire de tous vos actifs. Utilisez des dispositifs de stockage amovibles chiffrés et nettoyez-les correctement avant de les réutiliser ou de les mettre hors service.

Conseils de sécurité pour les dispositifs périphériques (ITSAP.70.015)

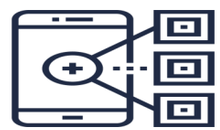
Nettoyage et élimination d'appareils électroniques (ITSAP.40.006)

Configurer les dispositifs pour assurer leur sécurité

Prenez le temps voulu pour vérifier les paramètres par défaut de votre appareil, et pour y apporter les modifications voulues. Nous recommandons tout au moins de changer les mots de passe par défaut (plus particulièrement les mots de passe administratifs) et de désactiver les services de localisation ainsi que les fonctions inutiles.

La cybersécurité à la maison et au bureau – Sécuriser vos dispositifs, vos ordinateurs et vos réseaux (ITSAP.00.007)

Sécuriser les appareils mobiles



Choisissez un modèle de déploiement des appareils mobiles. Fournirez-vous les dispositifs aux membres de votre personnel, ou leur permettrez-vous d'utiliser leurs dispositifs personnels pour le travail? Veillez à ce que les employés ne puissent utiliser que les applications approuvées et qu'ils ne puissent télécharger que des applications provenant de sources de confiance.

Considérations de sécurité pour les modèles de déploiement de dispositifs mobiles (ITSAP.70.002)

Mettre en œuvre le contrôle et l'autorisation de l'accès

Apply Appliquez le principe de droit d'accès minimal afin d'empêcher des accès non autorisés et des fuites de données. Les employés ne devraient avoir accès qu'aux renseignements dont ils ont besoin pour exécuter leurs tâches. Chaque utilisateur doit détenir son propre ensemble de justificatifs de connexion, et les administrateurs doivent avoir des comptes d'administrateur et d'utilisateur général distincts.

Gestion et contrôle des privilèges administratifs (ITSAP.10.094)

Sécuriser les sites Web

Protégez votre site Web et les renseignements sensibles qu'il recueille. Chiffrez les données sensibles, mettez à jour vos certificats au besoin, utilisez des mots de passe ou des phrases de passe robustes en arrière-plan, et utilisez le protocole HTTPS pour votre site. Si vous avez externalisé votre site Web, assurez-vous que l'hôte a des mesures de sécurité en place.

Défiguration de site Web (ITSAP.00.060)

Établissement de défenses de base sur le périmètre

Protégez vos réseaux contre les cybermenaces. Par exemple, utilisez un coupe-feu pour vous protéger des intrusions extérieures en surveillant le trafic entrant et sortant, et en filtrant les sources malveillantes. Lorsque les employés travaillent à distance, recourez à un réseau privé virtuel (RPV) pour sécuriser la connexion et protéger les renseignements sensibles.

Les réseaux privés virtuels (ITSAP.80.101)

Conseils de sécurité pour les organisations dont les employés travaillent à distance (ITSAP.10.016)

Centre de la sécurité des télécommunications
Communications Security Establishment

 No de cat.D97-1/10-035-2024F-PDF ISBN 978-0-660-69931-8

Canada