Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Protéger votre organisation contre les menaces de la chaîne d'approvisionnement des logiciels

Gestionnaires

ITSM.10.071

Canada

Avant-propos

La présente publication est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour obtenir de plus amples renseignements, veuillez communiquer par téléphone ou par courriel avec le Centre d'appel du Centre pour la cybersécurité :

contact@cyber.gc.ca
613-949-7048 ou 1-833-CYBER-88

Date d'entrée en vigueur

Le présent document entre en vigueur le 8 février 2023.

Historique des révisions

Révision	Modifications	Date
1	Première diffusion.	8 février 2023

ISBN 978-0-660-45702-4
CAT D97-4/10-071-2022F-PDF

Vue d'ensemble

Les attaques de la chaîne d'approvisionnement sont des menaces en évolution qui ciblent les fournisseurs de logiciels tiers. Une attaque de la chaîne d'approvisionnement des logiciels survient lorsqu'un auteur de cybermenace compromet un logiciel avant que le fournisseur ait envoyé ce dernier aux clients. Une intrusion peut provoquer un effet de ricochet et toucher des milliers de victimes.

Un auteur de menace peut exploiter la relation de confiance entre le client et le fournisseur de logiciels afin d'obtenir un accès privilégié et persistant aux réseaux des victimes. Selon ses intentions et ses compétences, l'auteur de menace peut ainsi accéder à des données sensibles du client pendant une période prolongée, sans être détecté. La compromission d'un système n'est souvent détectée qu'après que des dommages importants ont été causés.

Dans le présent document, nous discuterons des risques de sécurité associés à la chaîne d'approvisionnement des logiciels, de l'importance de ces risques et des mesures que le client peut prendre afin d'éviter d'être victime d'une telle attaque. Peu importe la taille de votre organisation, si vous faites affaire avec des fournisseurs de logiciels, vous devez considérer les risques associés à la chaîne d'approvisionnement des logiciels et prendre les précautions nécessaires pour cerner, évaluer et atténuer ces risques. Afin de gérer efficacement les risques associés à la chaîne d'approvisionnement des logiciels, vous devez intégrer des pratiques de sécurité associées à la chaîne d'approvisionnement des logiciels dans votre programme de sécurité des TI et dans votre cadre de gestion des risques.

Table des matières

Liste des figures

1 Introduction

Une chaîne d'approvisionnement comprend chaque phase de transformation des matières premières, des composants et des ressources en vue d'obtenir un produit ainsi que le processus de livraison jusqu'à l'utilisateur final. Les entités de la chaîne d'approvisionnement incluent les concepteurs, les développeurs, les fournisseurs, les entrepôts, les centres de distribution et les détaillants. Dans le cas des logiciels, les matières premières sont les bibliothèques courantes, le code, le matériel et les outils qui transforment le code en un produit fini. Le produit peut être déployé à titre d'application pour l'utilisateur final ou encore comme élément intermédiaire servant à différents produits.

Les consommateurs de logiciels doivent comprendre que tout logiciel comporte des vulnérabilités pouvant être exploitées par un auteur de menace, qui pourra alors altérer les propriétés de sécurité et les fonctionnalités du logiciel à des fins malveillantes. Contrairement aux composants électroniques physiques et aux systèmes des TI, qui sont rarement modifiés après avoir quitté la chaîne de production, les logiciels sont révisés, mis à jour et corrigés sur une base continue. Ces modifications constantes rendent la chaîne d'approvisionnement des logiciels vulnérable à des intégrations malveillantes à tout point dans son cycle de vie.

Il existe plusieurs manières d'attaquer une chaîne d'approvisionnement des logiciels, notamment en insérant du code malveillant dans le code source d'un logiciel, en piratant le compte d'un développeur sans que personne ne s'en rende compte ou en compromettant une clé de signature afin de distribuer un logiciel qui ne fait pas officiellement partie d'un composant. À tout point dans le cycle de vie de la chaîne d'approvisionnement des logiciels, de mauvaises pratiques de sécurité augmentent les risques de cybersécurité pour l'organisation.

Les développeurs utiliseront souvent une variété de composants logiciels et de dépendances libres pour créer leurs programmes et leurs applications. L'accès à des bibliothèques, à des cadres et à des processus gratuits permet aux développeurs d'économiser du temps et des frais, car ils n'ont pas à écrire leur code à partir de zéro. C'est la raison pour laquelle l'utilisation de logiciels ouverts est devenue une pratique standard dans les processus de développement d'applications. En contrepartie, l'utilisation de logiciels ouverts pour créer du code signifie que n'importe qui y a accès et peut y apporter des modifications. De la sorte, les programmes et les applications développés en utilisant du code ouvert peuvent présenter des vulnérabilités insoupçonnées par les développeurs et des risques importants pour la sécurité.
Les logiciels propriétaires peuvent également présenter des vulnérabilités si les développeurs n'adoptent pas des pratiques de développement sécuritaires.

Dans *l'Évaluation des cybermenaces nationales 2023-2024* [1], le Centre pour la cybersécurité note que plutôt que de cibler directement les organisations, les auteurs de cybermenace visent de plus en plus les outils et les services logiciels qu'utilisent les organisations en compromettant la chaîne d'approvisionnement. La menace émanant de compromissions de la chaîne d'approvisionnement augmente lorsque les fournisseurs ont un accès de niveau élevé aux réseaux de leurs clients. Ce type de relation devient de plus en plus courant avec la prolifération des logiciels infonuagiques, des infrastructures dans le nuage et des modèles de plateforme-service.

Afin de protéger votre organisation des attaques de la chaîne d'approvisionnement des logiciels, vous devez intégrer la gestion des risques ainsi que des mesures de sécurité permettant d'atténuer les risques inhérents à votre chaîne d'approvisionnement des logiciels. Les conseils du présent document sont alignés sur les activités de gestion des risques

décrites dans l'ITSG-33, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* [2] ainsi que sur l'ITSM.10.089, *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information* [3] et l'ITSAP.10.035, *Les meilleures mesures pour renforcer la cybersécurité des petites et moyennes entreprises* [4]. Pour de plus amples renseignements à propos des contrôles de sécurité, nous recommandons également de consulter la publication *Contrôles de cybersécurité de base pour les petites et moyennes organisations* [5] à titre de référence pour améliorer votre résilience envers les cybermenaces.

2 Menaces pour la chaîne d'approvisionnement des logiciels

Que ce soit pour l'installation des mises à jour ou la réparation des vulnérabilités logicielles, les communications entre les fournisseurs de logiciels tiers et les réseaux des clients sont fréquentes. Un auteur de menace peut exploiter ces communications pour envoyer des mises à jour malveillantes ou encore bloquer l'application des correctifs et ainsi exploiter des vulnérabilités non corrigées. Une attaque de la chaîne d'approvisionnement des logiciels contre votre organisation peut avoir une incidence sur la confidentialité, l'intégrité et la disponibilité (les trois piliers de la sécurité des TI) des ressources et des systèmes d'information de votre organisation. Il est impératif de garder à l'esprit que votre organisation est légalement responsable de protéger ses informations, même lorsque vous utilisez des services tiers.

Fondamentalement, les attaques de la chaîne d'approvisionnement des logiciels ont le même effet que toute autre cyberattaque (exfiltration des données, surveillance, rançongiciel, etc.). La différence est que les attaques de la chaîne d'approvisionnement sont difficiles à prévenir, car vous avez très peu d'incidence sur les contrôles de sécurité de vos fournisseurs de logiciels. Une seule attaque en amont peut compromettre en aval plusieurs réseaux de client.

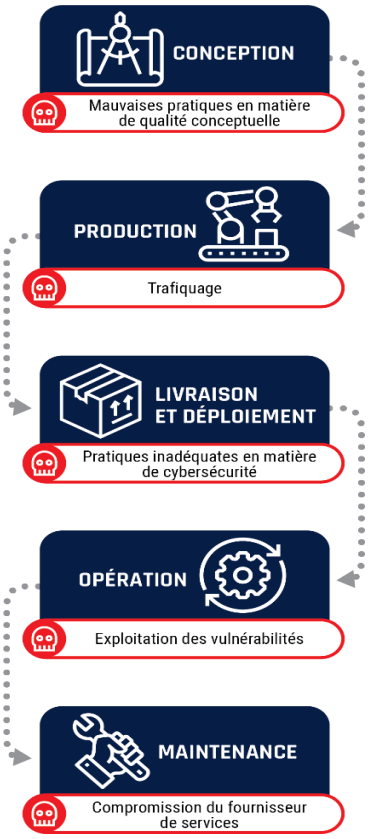
Un auteur de menace peut exploiter la relation de confiance entre les organisations et les fournisseurs de logiciels afin d'obtenir un accès privilégié et persistant aux réseaux des victimes. Selon ses intentions et ses compétences, l'auteur de menace peut être en mesure d'accéder à des données sensibles de votre organisation pendant une période prolongée, sans être détecté. La compromission d'un système n'est souvent détectée qu'après que des dommages importants ont été causés. Ces dommages peuvent être dévastateurs pour la réputation et la crédibilité de votre organisation puisque l'auteur de menace peut réaliser différentes activités malveillantes, par exemple :

- surveiller les communications et les actions de l'organisation;
- voler des données, des renseignements financiers et des informations propriétaires;
- désactiver les réseaux ou les systèmes, et plus encore.

2.1 Cycle de vie de la chaîne d'approvisionnement (CCA) des logiciels

Les chaînes d'approvisionnement des logiciels font partie du cycle de vie de la chaîne d'approvisionnement (CCA) des technologies de l'information et des communications (TIC). Tel qu'il est illustré à la figure 1, le CCA des TIC présente cinq phases, tout comme le CCA des logiciels. La figure 1 illustre une faille de sécurité potentielle à chacune des phases : conception, production, livraison et déploiement, opération et maintenance. Une telle faille peut permettre à un auteur de menace de mener des activités malveillantes et de compromettre le logiciel.

Figure 1 : Cycle de vie de la chaîne d'approvisionnement



2.1.1 Exemples d'attaques réussies à différentes phases du CCA

SolarWinds est une entreprise de gestion des TI dont le serveur de création, qui est une machine dédiée servant à créer des applications, a été infiltré par un auteur de menace en 2020. L'auteur de menace est resté indétecté sur le réseau de SolarWinds pendant des mois. Il a inséré un maliciel dans le processus de mise à jour du logiciel afin d'infiltrer les réseaux des clients infectés. Il s'agit d'un exemple où les phases de production et de maintenance du CCA ont été compromises. Après avoir piraté des mises à jour ou des appareils, l'auteur de menace peut insérer des maliciels ou altérer la mise à jour de base afin de contrôler des systèmes.

En décembre 2021, une vulnérabilité critique a été découverte dans Log4j, une bibliothèque ouverte de journalisation largement utilisée par des millions d'ordinateurs partout dans le monde et exécutant des applications logicielles et des services en ligne. Il s'agit d'un exemple parfait de vulnérabilité dans un logiciel libre. Si une telle vulnérabilité n'est pas corrigée, les attaquants pourraient accéder à des systèmes, voler des mots de passe et autres données d'identification, extraire des données et infecter les réseaux de logiciels malveillants. Plusieurs organisations canadiennes et agences fédérales ont dû mettre hors service leurs sites Web et leurs infrastructures de service par précaution. La mesure d'intervention la plus rapide recommandée consistait à mettre à niveau toutes les instances de Log4j à la version la plus récente. Cette mesure permettait de réduire les attaques futures, sans toutefois remédier aux dommages causés avant la mise à niveau de la bibliothèque. Comme cette vulnérabilité était très repandue, on a tenu pour acquis que l'écosystème d'une organisation était compromis avant la mise à niveau de la bibliothèque. Ainsi, il fallait activer le plan d'intervention en cas d'incident de violation de données immédiatement.

La liste ci-dessous présente d'autres exemples d'attaques réussies à différentes phases du CCA des TIC. Les publications *Defending Against Software Supply Chain Attacks* [6] du National Institute of Standards and Technology (NIST) et *Software Supply Chain Attacks* [7] du National Counterintelligence and Security Center (NCSC) contiennent d'autres exemples et de plus amples renseignements sur ces attaques.

1. GoldenSpy est un maliciel dissimulé dans un logiciel fiscal [8]. En 2020, un segment identifié de maliciel a été découvert dans un logiciel de paiement d'impôts que certaines entreprises étrangères menant des opérations en Chine étaient forcées d'installer.

    - Point d'entrée: Logiciel de création avec maliciel dissimulé
    - Phase du CCA: Conception

2. L'attaque ShadowHammer est une attaque perfectionnée de la chaîne d'approvisionnement touchant l'utilitaire de mise à jour ASUS Live Update [9]. En 2019, au moins six infrastructures des TI ont été infiltrées. Un groupe chevronné d'auteurs de menace a modifié une ancienne version du logiciel utilitaire ASUS Live Update et a inséré une copie modifiée dans des ordinateurs ASUS dans le monde entier.

    - Point d'entrée: Infrastructure de production compromise
    - Phase du CCA: Production

3. En 2017, un service de renseignement étranger a exploité Kaspersky Lab, un fournisseur d'antivirus basé à Moscou, afin de secrètement balayer des ordinateurs partout dans le monde et de repérer des documents et des renseignements confidentiels du gouvernement américain [10]. Les clients du gouvernement américain ont reçu la consigne d'arrêter d'utiliser les produits du fournisseur et de bannir l'acquisition de produits subséquents.

    - Point d'entrée: Logiciel compromis utilisé à titre d'outil d'espionnage
    - Phase du CCA: Livraison et déploiement

4. En 2020, un auteur de menace a compromis l'outil de signature numérique de l'autorité de certification du gouvernement vietnamien (VGCA pour Vietnamese Government Certification Authority) [11]. Cet auteur de menace a exploité les programmes d'installation de logiciel hébergés sur le site de la VGCA en injectant le logiciel espion PhantomNet ou Smanager.

    - Point d'entrée: Site Web d'une autorité de certification numérique compromis
    - Phase du CCA: Opération

5. En 2021, un groupe d'opérateurs de rançongiciel a inséré du code malveillant dans une mise à jour du logiciel Virtual System Administrator (VSA) de Kaseya [12]. Après la mise à jour, les systèmes de centaines d'entreprises sont devenus inaccessibles en raison du rançongiciel.

    - Point d'entrée: Mise à jour logicielle
    - Phase du CCA: Maintenance

2.2 Vecteurs d'attaque courants pour la chaîne d'approvisionnement des logiciels

Une attaque de la chaîne d'approvisionnement de logiciels est rarement l'objectif final d'un auteur de menace. Il se sert plutôt de l'attaque pour infiltrer de nombreux réseaux afin de compromettre les opérations de plusieurs organisations. La section suivante détaille les vecteurs d'attaque courants de la chaîne d'approvisionnement des logiciels.

2.2.1 Mises à jour compromises

Les fournisseurs envoient normalement à leurs clients des correctifs de bogues et de sécurité qui sont importants pour assurer le bon fonctionnement et la sécurité des logiciels. Un auteur de menace peut exploiter ce mécanisme de mise à jour afin de distribuer des maliciels à des utilisateurs non avertis, particulièrement après avoir compromis le réseau des développeurs. Comme il n'existe aucune politique ou norme de sécurité pour les processus de mise à jour, il est impossible pour les utilisateurs qui n'ont pas la signature numérique de valider ou de vérifier l'intégrité de la mise à jour diffusée et téléchargée. Une signature valide l'authenticité et l'intégrité d'un logiciel lors de l'installation et de l'exécution.

Lors de la mise à jour de votre logiciel en utilisant une connexion réseau, un auteur de menace peut intercepter la mise à jour et envoyer un maliciel afin de prendre le contrôle des fonctionnalités normales du logiciel.

2.2.2 Composants et dépendances des logiciels ouverts

On remarque de plus en plus que les développeurs ont recours à des composants et à des dépendances associés à des logiciels ouverts pour créer du code. Les logiciels ouverts sont offerts à partir de bibliothèques ou de référentiels logiciels en ligne où les utilisateurs peuvent installer les versions et les mises à jour les plus récentes des logiciels. De nombreux développeurs choisissent de travailler avec des logiciels ouverts pour gagner du temps en n'ayant pas besoin de développer eux-mêmes les capacités de base. Les logiciels ouverts permettent également d'économiser des ressources, car les logiciels et les mises à jour sont gratuits. L'utilisation de ces composants logiciels comporte toutefois des risques, surtout lorsque les fournisseurs n'offrent plus de maintenance et de correctifs. Si un auteur de menace obtient l'accès à ces référentiels ouverts, il peut offrir des versions compromises de logiciels sans même que les développeurs en aient connaissance. De plus, il peut obtenir un accès non autorisé non seulement au réseau des développeurs, mais également aux réseaux, aux systèmes et aux données sensibles des utilisateurs. On demande de plus en plus aux développeurs de valider l'intégrité de leur produit au moyen d'outils de suivi des composants (SBOM pour Software Bill of Material) ou d'un inventaire de tous les composants utilisés à la création de leur produit. Un SBOM permet de s'assurer que les obligations de licence de ces composants sont respectées et que les correctifs sont appliqués, lorsque nécessaire.

2.2.3 Clés de signature de code

La signature de code est une méthode de chiffrement servant aux développeurs pour créer des signatures numériques et prouver l'intégrité du logiciel. La signature numérique représente une preuve pour les utilisateurs finaux que le code n'a pas été altéré depuis qu'il a été acheminé par le fournisseur. Elle est particulièrement importante dans le cas des téléchargements de logiciel depuis des sites Web tiers, plutôt que directement du fournisseur.

Les auteurs de menace peuvent saboter la signature du code en utilisant les méthodes suivantes :

- utiliser des certificats autosignés, c'est-à-dire des certificats de clé publique qui ne sont pas signés par une autorité de certification (AC) fiable, mais plutôt par une clé privée;
- pirater les systèmes de signature;
- manipuler les contrôles d'accès des comptes mal configurés;
- acheter des certificats volés;
- compromettre l'infrastructure de signature et émettre des certificats qui peuvent paraître légitimes;

3 Pratiques exemplaires en matière de sécurité des logiciels pour votre organisation

Nous vous recommandons de prendre les mesures répertoriées dans la présente section pour vous aider à sélectionner les bons fournisseurs et à renforcer votre posture de cybersécurité lorsque vous utilisez des logiciels et des applications.

1. **Recherche sur les fournisseurs** : Vous devriez effectuer une recherche sur les fournisseurs pour mieux comprendre leur mode de fonctionnement. Demandez-leur leurs certifications, leurs normes de sécurité et les processus en place pour vérifier s'ils peuvent appuyer vos besoins opérationnels et vos exigences de sécurité. Un autre élément à considérer est la présence de commandites ou d'affiliations avec des acteurs étatiques pouvant avoir des motifs cachés lors de l'entente de niveau de service avec votre organisation.
2. **Établissement des rôles :** Collaborez avec vos fournisseurs et distributeurs pour définir clairement les rôles, les responsabilités et les processus de signalement et de réponse aux incidents de sécurité dans la chaîne d'approvisionnement. Une bonne relation avec vos fournisseurs assurera de bonnes communications lors des processus de mise à jour ou de changement, une intervention robuste en cas d'incident et une mise en œuvre rapide des processus de migration.
3. **Documentation de vos politiques de sécurité et d'acquisition des logiciels :** En plus de compter sur l'autocertification du fournisseur, qui repose souvent sur des questionnaires pour la diligence raisonnable, vous devez mener vos propres audits, vérifications de code source et tests de pénétration. Vous devriez aussi tenir à jour un inventaire des licences logicielles de votre organisation, actuelles et à venir.
4. **Surveillance des fournisseurs :** Une surveillance statique n'est pas suffisante pour protéger vos données et vos réseaux d'un auteur de menace, qui peut cibler les logiciels et les applications exécutés sur vos réseaux. Établissez des paramètres de surveillance qui permettront une surveillance continue de vos fournisseurs et de leurs contrôles de sécurité ayant une incidence sur votre organisation.
5. **Moment de l'application des mises à jour et des correctifs pour vos logiciels :** Les mises à jour et les correctifs ne doivent pas être mis en œuvre avant que le fournisseur ait confirmé qu'il n'a relevé aucun problème lors des tests de préproduction.
6. **Renforcement des contrôles et des autorisations d'accès de sécurité :** Votre organisation doit utiliser le principe du droit d'accès minimal et accorder aux utilisateurs le niveau d'accès minimal requis pour réaliser leurs tâches. L'application du principe du droit d'accès minimal permet de réduire considérablement la zone d'attaque en éliminant les droits d'accès non nécessaires, lesquels peuvent mener à toute une gamme de compromissions.
7. **Sécurité des contrats :** Intégrez les exigences de sécurité, de confidentialité, de gestion des documents et de conformité dans chaque demande de proposition (DP) et dans chaque contrat de fournisseur.
8. **Formation et sensibilisation des employés au sujet de la sécurité des logiciels :** Disposer d'un programme de formation sur la sécurité bien organisé et établi pour vos employés est essentiel à la protection de votre organisation contre les cybermenaces. Vous devriez fournir de la formation à vos employés sur une base périodique. Pour en savoir plus sur la formation, veuillez consulter l'ITSM.10.093, *Les 10 mesures de sécurité des TI : No 6, Miser sur une formation sur mesure en matière de cybersécurité* [13].

9. **Mise en œuvre d'un plan d'intervention en cas d'incident** : Même si vous avez appliqué toutes les pratiques exemplaires en matière de sécurité des logiciels, il existe toujours des possibilités de violation. Un état de préparation optimal peut empêcher un auteur de menace de réaliser sa mission, même après une violation, en limitant les dommages.
10. **Renforcement de la surveillance du réseau et des journaux :** La surveillance du réseau et des journaux permet de détecter les comportements atypiques et offre une possibilité de suivi dans le cas des changements apportés au système.

3.1 Vérification des fournisseurs de logiciel

La vérification adéquate d'un fournisseur peut s'avérer difficile en raison du nombre élevé de fournisseurs de logiciel. La liste suivante répertorie quelques paramètres utiles pour évaluer la conformité à la sécurité des fournisseurs de logiciel potentiels.

1. Utilisent-ils un cadre de cycle de développement des logiciels sécurisés (CDLS)? Est-il documenté?
2. Ont-ils un processus de documentation pour prouver que les activités décrites dans le CDLS se déroulent comme prévu?
3. Les pratiques de sécurité sont-elles intégrées à chaque étape du CDL?
4. Des normes et contrôles de sécurité robustes sont-ils appliqués à chaque étape du cycle de développement afin de surveiller et de gérer les processus de production?
5. Disposent-ils d'une équipe de sécurité logicielle à temps plein compétente?
6. Les membres de l'équipe sont-ils formés sur le développement de logiciels sécurisés, la sécurité des logiciels ouverts et les pratiques DevSecOps?
7. Mènent-ils une vérification des antécédents des employés?
8. Tous les développeurs conservent-ils des registres détaillés des dépendances utilisées dans les logiciels? Les développeurs sont-ils à jour et utilisent-ils les dernières versions des dépendances de bibliothèque?
9. L'atténuation des vulnérabilités connues est-elle considérée dans la conception du produit?
10. Sont-ils à l'affût de l'évolution des nouvelles vulnérabilités? Reçoivent-ils des alertes lors des divulgations de vulnérabilité?
11. Ont-ils un système bien documenté pour appliquer les correctifs de sécurité et corriger les défauts de sécurité?
12. Les vulnérabilités sont-elles activement identifiées et divulguées? Ont-ils un programme de réponse aux vulnérabilités ainsi qu'une équipe associée en place?
13. Les produits et les activités de sécurité des logiciels sont-ils passés en revue par une tierce partie?
14. Ont-ils des processus de gestion de la configuration logicielle (GCL) en place pour les activités de suivi, de gestion et de contrôle des modifications apportées aux logiciels/au code durant le CDL?
15. Garantissent-ils que les données de votre organisation seront protégées?
    Utilisent-ils le chiffrement des données? Suppriment-ils les données lorsque la relation avec leur client est terminée?
16. Ont-ils des procédures de vérification interne pour toutes les opérations de sécurité?
17. Peuvent-ils confirmer l'intégrité du logiciel au moyen d'un mécanisme pour authentifier le code?
18. Disposent-ils d'un inventaire des composants logiciels ou d'un outil de suivi des composants (SBOM)? Vérifient-ils leurs contrôles afin d'assurer la sécurité des logiciels? Quels sont les détails consignés dans le SBOM?

19. Ont-ils des protocoles pour aviser les intervenants appropriés dans l'éventualité d'une violation chez le fournisseur?

4 Considérations relatives à la gestion des risques de la chaîne d'approvisionnement pour les grandes organisations et les infrastructures essentielles

L'identification, l'évaluation et l'atténuation des risques de cybersécurité liés à la chaîne d'approvisionnement sont des étapes impératives pour les infrastructures essentielles et les organisations. Elles permettent d'améliorer la résilience et la protection contre les cyberincidents. L'approche multidisciplinaire pour la gestion de ces types de risques se nomme C-SCRM (pour *Cyber Supply Chain Risk Management*). La sécurité de la chaîne d'approvisionnement des logiciels va de pair avec la C-SCRM. Dans le cas des grandes organisations et des infrastructures essentielles, il est important de mettre en œuvre les contrôles de sécurité, les vérifications, ainsi que les politiques et processus de gestion des risques nécessaires afin d'atténuer les risques associés à leur chaîne d'approvisionnement. Ces mesures leur permettront de préserver la confidentialité, l'intégrité et la disponibilité des informations et des systèmes.

L'intégration des logiciels dans le cadre de la C-SCRM aidera les organisations à comprendre les risques que présentent les logiciels. Les organisations peuvent gérer ces risques en identifiant différentes exigences techniques et non techniques pour la C-SCRM en lien avec les logiciels. L'établissement d'un cadre de gestion des risques adapté à l'organisation permettra d'assurer un approvisionnement sécurisé des logiciels et des applications, et une gestion adéquate à chaque étape de leur cycle de vie. Un plan de gestion des risques intégrant les logiciels représente un composant important de toute stratégie globale de cybersécurité d'une organisation.

Voici quelques étapes préliminaires requises pour mettre au point votre C-SCRM :

1. déterminer les processus essentiels à votre mission ou à vos activités ainsi que les services essentiels fournis par votre organisation;
2. comprendre les exigences de sécurité de votre organisation;
3. définir la stratégie de risque et le niveau de tolérance au risque global de votre organisation;
4. créer un programme C-SCRUM en fonction du risque et des exigences de sécurité correspondantes.

Le NIST suggère huit pratiques de base pour élaborer un cadre de C-SCRM pouvant être appliqué à un logiciel. L'application de ces mesures permettra de prévenir et d'atténuer les vulnérabilités logicielles pouvant avoir été introduites dans la chaîne d'approvisionnement et exploitées par des auteurs malveillants. Elles aideront également à répondre à ces vulnérabilités.

1. intégrer le cadre de C-SCRM au sein de votre organisation;
2. établir un programme de C-SCRM évalué et mis à jour en temps réel;
3. déterminer les fournisseurs essentiels et la gestion de ceux-ci;
4. comprendre la chaîne d'approvisionnement de votre organisation;
5. collaborer étroitement avec les fournisseurs essentiels et les intégrer à votre programme de gestion des risques associés aux fournisseurs;
6. inclure les fournisseurs essentiels dans vos activités d'amélioration et de résilience afin qu'ils fassent partie de votre processus d'évaluation des risques associés aux fournisseurs;
7. évaluer et surveiller la relation avec les fournisseurs en effectuant une surveillance continue de votre C-SCRM;
8. planifier le cycle de vie complet de vos ressources.

5 Amélioration de la cyberrésilience

La cyberrésilience aide les organisations à se préparer à faire face aux cyberattaques, à répondre à ces attaques, à se défendre contre celles-ci et à se rétablir après coup. Ces attaques comprennent celles contre la chaîne d'approvisionnement des logiciels. Une organisation cyberrésiliente peut s'adapter aux crises et aux menaces, connues ou inconnues, et assurer la continuité de ses opérations malgré des événements défavorables.

De nos jours, la question n'est plus de savoir ce que ferait une organisation « si elle subissait » une cyberattaque, mais plutôt ce qu'elle fera « quand elle subira » une telle attaque. Ainsi, plutôt que de concentrer vos efforts et vos ressources à garder les auteurs de menace à l'extérieur de votre réseau, vous devez tenir pour acquis qu'ils profiteront éventuellement d'une faille dans vos mesures de défense et élaborer une stratégie pour réduire l'impact d'une telle intrusion.

5.1 Renforcement de la posture de sécurité de votre organisation

Pour renforcer la cybersécurité et la posture de sécurité de votre organisation, nous vous recommandons d'utiliser un cadre de gestion des risques liés à la sécurité des TI, notamment La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33) [2], *ISO-27001 Information Security Management* [14], ou *NIST SP 800-37 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [15]. Toutefois, ces profils coûtent cher à mettre en œuvre et dépassent le seuil budgétaire ou de ressources humaines de la plupart des petites et moyennes organisations au Canada.

Les organisations peuvent atténuer la plupart des cybermenaces grâce à la sensibilisation et à l'adoption des pratiques exemplaires en matière de cybersécurité et de continuité des activités. La publication du Centre pour la cybersécurité intitulée *Contrôles de cybersécurité de base pour les petites et moyennes organisations* [5] présente un ensemble condensé de contrôles de sécurité permettant aux organisations d'optimiser leurs investissements en cybersécurité. Ces contrôles sont tirés des contrôles de sécurité répertoriés à l'Annexe 3A de ITSG-33 [2]. L'ITSG-33 [2] décrit les rôles, les responsabilités et les activités qui aident les organisations à gérer leurs risques liés à la sécurité des TI. Il comprend un catalogue des contrôles de sécurité (exigences de sécurité normalisées pour protéger la confidentialité, l'intégrité et la disponibilité des actifs TI). Ces contrôles sont regroupés en trois classes, puis subdivisés en plusieurs familles de contrôles de sécurités connexes.

- **Contrôles de sécurité techniques** : 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;
- **Contrôles de sécurité opérationnels** : Contrôles de sécurité de système d'information mis en œuvre et exécutés principalement par des personnes et qui s'appuient normalement sur des technologies comme les logiciels de soutien;
- **Contrôles de sécurité de gestion** : Contrôles de sécurité misant sur la gestion de la sécurité des TI et des risques liés à la sécurité des TI.

Ces contrôles fourniront à votre organisation les outils pour réaliser ce qui suit :

- gérer et protéger vos informations et vos systèmes en établissant, évaluant et gérant les risques associés au réseau et aux systèmes d'information, y compris ceux de la chaîne d'approvisionnement;
- détecter les anomalies et les incidents de cybersécurité potentiels avant qu'ils ne causent des dommages grâce à une surveillance continue de votre réseau et de vos systèmes d'information;
- élaborer un plan d'urgence pour la mise en œuvre de logiciels de rechange en cas d'incident de cybersécurité;
- réagir aux cyberincidents et s'en remettre dans le but d'assurer la continuité des activités.

5.2 Continuité des activités

Pour assurer la continuité des activités après un temps d'arrêt minimal, nous vous recommandons d'intégrer un plan de rétablissement des TI [16] dans le cadre de la gestion des risques et de la continuité des activités de votre organisation. Votre organisation doit cerner les données, applications et processus essentiels et définir la façon dont elle pourra assurer le rétablissement des services des TI qui appuient les opérations, les produits et les services.

Votre plan de rétablissement doit clairement définir et documenter les éléments à rétablir, par qui, quand et où. Vous devez envisager d'élaborer l'un des deux types de plans suivants pour vos activités :

1. **Plan de reprise après sinistre :** Ce plan vise principalement à assurer la continuité des activités en cas de panne ou d'interruption de service imprévue. Pour plus d'information sur la mise au point d'un plan de reprise, consultez *l'ITSAP.40.004, Élaboration d'un plan de reprise informatique personnalisé* [16].
2. **Plan d'intervention en cas d'incident :** Ce plan vise principalement à protéger les informations sensibles en cas de violation de sécurité. Pour plus d'information sur la mise au point d'un plan d'intervention en cas d'incident, consultez l'ITSAP.40.003, *Élaborer un plan d'intervention en cas d'incident* [17].

Ces deux plans tiennent compte de deux événements majeurs qui pourraient provoquer une panne imprévue et obliger un organisme à activer ses mesures d'intervention et de reprise.

Votre plan de rétablissement des TI doit être mis à l'épreuve afin de cerner les incohérences et de fournir des possibilités pour traiter les points qui nécessitent une révision. Nous vous recommandons de mettre à l'épreuve le plan de rétablissement des TI de votre organisation dans un environnement de test afin d'éviter d'interrompre les activités.

6 Résumé

Ce document présente les risques de sécurité associés à la chaîne d'approvisionnement des logiciels et les raisons pour lesquelles il est important de les gérer. Les organisations doivent adopter les pratiques exemplaires en matière de sécurité des logiciels afin d'éviter les attaques contre la chaîne d'approvisionnement des logiciels. En outre, nous avons ajouté une liste de paramètres pour aider les organisations à sélectionner les bons fournisseurs et à évaluer leur conformité à la sécurité. Nous recommandons aux organisations d'intégrer ces pratiques de sécurité des logiciels dans leur programme de sécurité des TI et leur cadre de gestion des risques. Elles profiteront alors d'une meilleure cyberrésilience et pourront assurer la continuité de leurs activités, même en cas d'événement indésirable.

7 Contenu complémentaire

7.1 Liste des acronymes, des abréviations et des sigles

Acronyme, abréviation ou sigle	Expression au long
AC	Autorité de certification
CCA	Cycle de vie de la chaîne d'approvisionnement
CDLS	Cycle de développement des logiciels sécurisés
C-SCRM	Gestion des risques de cybersécurité liés à la chaîne d'approvisionnement (*Cyber Supply Chain Risk Management*)
CST	Centre de la sécurité des télécommunications
DoS	Déni de service (*Denial of Service*)
DP	Demande de proposition
GC	Gouvernement du Canada
ISO	Organisation internationale de normalisation (*International Organization for Standardization*)
NCSC	*National Cyber Security Centre*
NIST	*National Institute for Standards and Technology*
SBOM	Outil de suivi des composants logiciels (*Software Bill of Materials*)
TI	Technologies de l'information
TIC	Technologies de l'information et des communications
VGCA	*Vietnamese Government Certification Authority*
VSA	*Virtual System Administrator*

7.2 Glossaire

Terme	Définition
Auteurs de menace	États, groupes ou personnes malintentionnés qui cherchent à profiter des vulnérabilités, d'un faible niveau de sensibilisation à la cybersécurité ou des progrès technologiques afin d'obtenir un accès non autorisé à des systèmes d'information dans le but d'accéder ou sinon de nuire aux données, aux appareils, aux systèmes et aux réseaux des victimes.
Chaîne d'approvisionnement	Processus requis pour concevoir, fabriquer et distribuer de l'équipement ou des commodités, y compris du matériel et des logiciels des technologies de l'information [1].
Compromission	Divulgation intentionnelle ou non intentionnelle d'information mettant en péril sa confidentialité, son intégrité ou sa disponibilité.
Confidentialité	Caractéristique de l'information sensible protégée contre tout accès non autorisé.
Contrôle de sécurité	Exigence technique, opérationnelle ou gestionnelle de haut niveau relative à la sécurité, qu'il convient d'appliquer à un système d'information afin de protéger la confidentialité, l'intégrité et la disponibilité des actifs TI connexes. Ces contrôles peuvent être appliqués

Terme	Définition
	au moyen de diverses solutions de sécurité, notamment des produits, des politiques, des pratiques et des procédures de sécurité.
Cyberattaque	Recours à des techniques électroniques visant à perturber, à manipuler, à détruire ou à scruter clandestinement un système informatique, un réseau ou un appareil.
Cybermenace	Situation où un auteur de menace, utilisant Internet, profite d'une vulnérabilité connue dans un produit dans le but d'exploiter un réseau et les informations sur ce réseau.
Cybersécurité	Capacité de protéger ou de défendre l'utilisation du cyberespace contre les cyberattaques.
Disponibilité	Caractéristique de l'information ou des systèmes qui sont accessibles aux personnes autorisées au moment où celles-ci en ont besoin. La disponibilité est un attribut des actifs informationnels, des logiciels et du matériel informatique (l'infrastructure et ses composantes). Il est également entendu que la disponibilité comprend la protection des actifs contre les accès non autorisés et les compromissions.
Données	Représentation électronique de l'information. Quantité, caractères ou symboles sur lesquels les opérations sont réalisées par un ordinateur, stockés et transmis sous la forme de signaux électroniques et enregistrés sur des supports d'enregistrement magnétiques, optiques ou mécaniques.
Évaluation des risques	Processus d'identification, d'estimation et d'établissement des priorités associés aux opérations organisationnelles (y compris la mission, les fonctions, l'image et la réputation), aux actifs organisationnels, aux personnes, aux autres organisations et à la nation, résultant de l'exploitation d'un système d'information.
Gestion des risques	Processus continu, proactif et systématique permettant l'identification, l'évaluation, la compréhension, les réactions nécessaires et la communication des risques.
Intégrité	Aptitude à protéger l'information contre les modifications ou les suppressions non intentionnelles et inopportunes. L'intégrité permet de savoir si l'information est conforme à ce qu'elle est censée être. Elle s'applique également aux processus opérationnels, à la logique des applications logicielles, au matériel et au personnel.
Maliciel	Logiciel malveillant conçu pour infiltrer ou endommager un système informatique sans le consentement du propriétaire. Les maliciels les plus courants sont les virus informatiques, les vers, les chevaux de Troie, les logiciels espions et les logiciels publicitaires.
Organisation	Entité, peu importe la taille, la complexité ou le positionnement, avec une structure organisationnelle (par exemple, une agence fédérale ou, selon le cas, l'un de ses constituants opérationnels).
Pirate	Personne utilisant des ordinateurs et Internet pour accéder à des ordinateurs et à des serveurs sans autorisation.

Terme	Définition
Risque	Mesure de la portée de la menace que fait peser une circonstance ou un événement potentiel sur une entité. Dépend typiquement de ce qui suit : (i) l'incidence négative pouvant survenir si les circonstances ou l'événement se produisent; (ii) la probabilité d'occurrence.
Sécurité des TI	Discipline visant à appliquer des contrôles de sécurité, des solutions de sécurité, des outils et des techniques afin de protéger les actifs TI contre les menaces d'attaque pendant leur cycle de vie, selon la catégorie de sécurité des activités opérationnelles prises en charge et conformément aux politiques, aux directives, aux normes et aux lignes directrices ministérielles et du GC.
Technologies de l'information (TI)	Technologies ayant trait à la fois à l'infrastructure et aux applications TI.
Technologies de l'information et des communications (TIC)	Tous les moyens techniques utilisés pour traiter des informations et faciliter les communications, ce qui comprend à la fois le matériel informatique et réseau, ainsi que les logiciels.
Vulnérabilité	Défectuosité ou lacune inhérente à la conception ou à la mise en œuvre d'un système d'information ou à son environnement, qui pourrait être exploitée en vue de compromettre les biens actifs ou les activités d'une organisation.

7.3 Références

Numéro	Référence
1	Centre canadien pour la cybersécurité. *Évaluation des cybermenaces nationales 2023-2024*.
2	Centre canadien pour la cybersécurité. *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33)*, novembre 2018.
3	Centre canadien pour la cybersécurité. *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089),* septembre 2021.
4	Centre canadien pour la cybersécurité. *Les meilleures mesures pour renforcer la cybersécurité des petites et moyennes entreprises (ITSAP.10.035)*, juin 2021.
5	Centre canadien pour la cybersécurité. *Contrôles de cybersécurité de base pour les petites et moyennes organisations*, mai 2021.
6	National Institute for Standards and Technology. *Defending Against Software Supply Chain Attacks*, avril 2021.
7	The National Cyber Security Centre. *Software Supply Chain Attacks*, mars 2021.
8	Darkreading. *GoldenSpy' Malware Hidden in Tax Software Spies on Companies Doing Business in China*, juin 2020.
9	Securelist. *Operation ShadowHammer: a high-profile supply chain attack*, avril 2019.
10	The Wall Street Journal. *Russia Has Turned Kaspersky Software into Tool for Spying*, octobre 2017.

Numéro	Référence
11	The Hacker News. *Software Supply-Chain Attack Hits Vietnam Government Certification Authority*, décembre 2020.
12	Secpod. *Kaseya's Virtual System/Server Administrator (VSA) Zero-Day Under Active Exploitation By REvil Ransomware*, juillet 2021.
13	Centre canadien pour la cybersécurité. *Les 10 mesures de sécurité des TI : No 6, Miser sur une formation sur mesure en matière de cybersécurité (ITSM.10.093)*, février 2020.
14	International Organization for Standardization. *ISO 27001: Information Security Management*, 2018.
15	National Institute of Standards and Technology. *Special Publication Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, 2018.
16	Centre canadien pour la cybersécurité. *Élaboration d'un plan de reprise informatique personnalisé (ITSAP.40.004)*, 2021.
17	Centre canadien pour la cybersécurité. *Élaborer un plan d'intervention en cas d'incident (ITSAP.40.003)*, mai 2021.