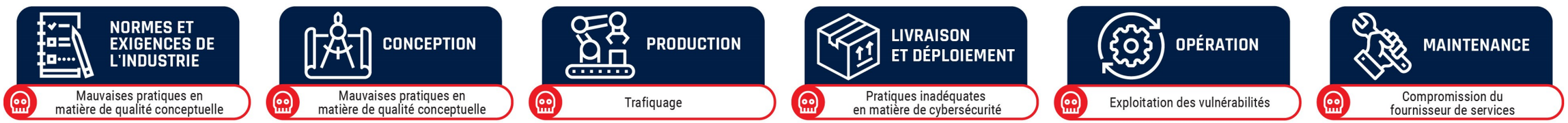
La cybersécurité et la chaîne d'approvisionnement : évaluation des risques

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

JUILLET 2022 | ITSAP.10.070

Dans notre monde numérique, les auteurs de cybermenaces profitent des failles de la chaîne d'approvisionnement pour lancer leurs attaques et chaque maillon de la chaîne mondiale d'approvisionnement peut représenter un risque contre la cybersécurité. Les organisations disposant d'informations ou de services de grande valeur doivent renforcer leurs défenses en matière de cybersécurité en identifiant, évaluant et atténuant les risques associés à la nature mondiale et distribuée des chaînes d'approvisionnement des produits et services des technologies de l'information et de la communication (TIC). Ensemble, ces éléments forment la base d'une stratégie robuste de gestion des risques de cybersécurité liés à la chaîne d'approvisionnement. On encourage les organisations à suivre l'approche du Centre pour la cybersécurité décrite dans la présente publication pour évaluer les risques de cybersécurité liés à la chaîne d'approvisionnement.

Cycle de vie des risques liés à la chaîne d'approvisionnement



Les auteurs de menaces peuvent influencer les produits avant même qu'ils ne soient conçus.

Des vulnérabilités peuvent être introduites délibérément ou accidentellement lors de la conception et de la production d'un produit.

Une fois le produit déployé, les vulnérabilités peuvent être découvertes et exploitées par les auteurs de menace. Il est essentiel à cette étape de mettre en œuvre des contrôles de sécurité appropriés dans l'environnement du produit.

Les produits peuvent être compromis lors d'activités régulières de maintenance ou de l'application de correctifs, et être infectés par de nouvelles vulnérabilités ou voir des vulnérabilités existantes exploitées.

Programme ICA du Centre pour la cybersécurité : fournir des connaissances utiles au gouvernement du Canada (GC)

Le cadre d'évaluation des risques liés à l'intégrité de la chaîne d'approvisionnement (ICA) du Centre pour la cybersécurité est un programme exhaustif conçu en vue d'effectuer des évaluations des produits et services des TIC qui seront déployés dans l'infrastructure du GC. Ce programme a pour objectif de protéger la confidentialité, l'intégrité et la disponibilité des communications et des données du GC en favorisant la résilience contre les vulnérabilités et les compromissions de la chaîne d'approvisionnement.

Les évaluations des risques de cybersécurité liés à la chaîne d'approvisionnement comprennent des recommandations de stratégies d'atténuation et de mesures visant à réduire les risques envers des technologies potentiellement vulnérables, ainsi qu'à assurer la protection des informations, des réseaux et de l'infrastructure des TI du GC.

Le Centre pour la cybersécurité recommande le recours à l'évaluation des risques liés à l'ICA, car elle constitue un élément essentiel du cadre de gestion des risques de toute organisation. Dans le cas des organisations qui appliquent les principes de La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG33), les évaluations des risques liés à l'ICA fournissent les renseignements nécessaires pour l'application des contrôles de sécurité SA-12(8). « Charter of Trust » est un autre document de référence qui s'aligne sur les normes internationales d'approche commune basée sur les risques envers la chaîne d'approvisionnement numérique.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

Évaluer les risques de la chaîne d'approvisionnement

Il y a de nombreux éléments à considérer lorsque vous évaluez votre chaîne d'approvisionnement. Le Centre pour la cybersécurité utilise une approche à plusieurs étapes pour évaluer les risques de cybersécurité liés à la chaîne d'approvisionnement des produits et services connectés.

Étape 1 : Déterminer la sensibilité de la technologie

Cette évaluation sera spécifique au produit et doit être effectuée au cas par cas. La sensibilité variera en fonction du contexte spécifique. La sensibilité doit être évaluée sur une échelle faible/moyenne/élevée en fonction de facteurs technologiques et contextuels.

Le produit

- **La fonction de la technologie** – Le rôle que jouent un produit ou un service, et l'impact sur la confidentialité, la disponibilité et l'intégrité des données en cas de compromission ou d'interruption.
- **Données traitées** – Le type de données traitées par un produit ou un service peut rendre un système plus intéressant pour les auteurs de cybermenace. La classification et l'agrégation des données ont une influence sur le niveau de sensibilité et les risques connexes.

Le contexte

L'importance dans l'écosystème – Des éléments de l'infrastructure essentielle, les réseaux gouvernementaux importants et les technologies perturbatrices émergentes, comme l'informatique quantique ou l'intelligence artificielle, peuvent être considérés comme très sensibles.

L'approvisionnement – Valeur monétaire et diversité des options.

Étape 2 : Évaluer la fiabilité du fournisseur

Cette évaluation sera spécifique au fournisseur et doit être effectuée au cas par cas. Niveau de confiance envers le fournisseur : pour déterminer le niveau de confiance envers vos fournisseurs, tenez compte des facteurs propres à leur entreprise, ainsi que de leurs pratiques de cybersécurité conformément aux normes internationales. ***Le niveau d'effort lié à l'étape 2 dépend du niveau de sensibilité.***

Les propriétaires du fournisseur

- **Propriété, contrôle et influence de l'étranger (PCIE)** – Dans quelle mesure une entreprise et le gouvernement d'un pays où elle réside sont-ils étroitement liés, y compris la probabilité potentielle d'être contraint de mener des activités contraires aux intérêts canadiens.
- **Contexte géopolitique** – L'emplacement de l'administration centrale et des centres des opérations de l'entreprise, le cadre législatif auquel l'entreprise est tenue de se conformer en ce qui a trait à la protection des données et les lois nationales qui limitent l'exercice des pouvoirs du gouvernement.
- **Pratiques opérationnelles** – Le comportement éthique et le respect des cadres juridiques et politiques peuvent indiquer à quel point une entreprise est digne de confiance. Il faut aussi examiner la transparence des propriétaires de l'entreprise, des investissements et de la passation de marchés.

Maturité de la cybersécurité

Normes et certifications – Respect des normes technologiques internationales et des certifications lors de la conception, la production et la maintenance des produits et services.

Protection des données – Produits ou services conçus pour assurer la confidentialité, l'authenticité, l'intégrité et la disponibilité des données. Les données doivent être protégées contre les accès non autorisés tout au long de leur cycle de vie.

Politiques de cybersécurité – Les politiques et mesures de protection proactives en matière de cybersécurité et la gestion des vulnérabilités de sécurité aident à déterminer la maturité d'une entreprise en matière de cybersécurité.

Étape 3 : Définir le déploiement

Les modèles de déploiement doivent être évalués pour chaque produit et correspondre à la posture interne de votre organisation. Considérez le déploiement dans le contexte de la posture de sécurité de votre organisation. Déterminez si l'exposition aux risques d'un fournisseur spécifique est acceptable, si des mesures d'atténuation plus rigoureuses doivent être mises en place ou si une autre technologie ou un autre fournisseur doit être sélectionné pour réaliser la fonction opérationnelle. Les résultats de l'évaluation permettront de déterminer les mesures d'atténuation appropriées et basées en grande partie sur les contrôles de sécurité de l'ITSG-33, *Gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie.*

Votre organisation

Les auteurs de menace, leurs tactiques, techniques et procédures – En examinant le cycle de vie de la chaîne d'approvisionnement, évaluez les menaces auxquelles l'organisation pourrait être confrontée.

Capacités de cyberdéfense – Évaluez les contrôles de sécurité que l'organisation a mis en place pour se protéger contre ces menaces.

Mesures d'atténuation – La capacité de mettre en œuvre des conseils liés aux mesures d'atténuation afin de réduire les risques résiduels.

Impact des compromissions et résilience –Gestion efficace des incidents liés aux tentatives de piratage ou aux violations de données auxquelles l'entreprise a été confrontée.

En fonction des capacités de votre organisation, l'exposition aux risques est-elle acceptable?

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada