SÉCURITÉ DE LA CHAÎNE D'APPROVISIONNEMENT POUR LES PETITES ET MOYENNES ORGANISATIONS

MARS 2019

ITSAP.00.070

SÉCURITÉ DE LA CHAÎNE D'APPROVISIONNEMENT

À titre de propriétaire d'organisation, avez-vous déjà songé au type d'information que vous fournissez à votre chaîne d'approvisionnement ? Savez-vous de quelle façon les fournisseurs traitent votre information et celle de vos clients, ou encore où cette information est enregistrée ? Vous avez tout intérêt à poser ces questions et d'autres questions afin de protéger votre organisation. Tout comme les grandes organisations, les petites et moyennes organisations sont vulnérables aux cyberattaques parce qu'ils possèdent beaucoup d'information de nature délicate qui attire les auteurs de menace. En plus d'être coûteuses à éradiquer, les cybermenaces peuvent mettre en péril votre organisation.

Une chaîne d'approvisionnement est le lien essentiel entre votre organisation et les autres organisations qui vous aident à servir vos clients. Que vous soyez propriétaire d'une boutique de fleurs ou d'une agence de publicité, la réussite de votre organisation dépend de la qualité et de la sécurité de votre chaîne d'approvisionnement.

POURQUOI VOTRE CHAÎNE D'APPROVISIONNEMENT EST-ELLE MENACÉE ?

Si vous dirigez une petite ou moyenne organisation, vous pensez peut-être que votre organisation n'est pas ciblée par des auteurs de menace, mais détrompez-vous. Selon Innovation, Sciences et Développement économique Canada, on compte plus de 1,14 million de petites et moyennes organisations au Canada. Ces organisations détiennent un grand volume d'information. Ainsi, il est pertinent de penser que votre organisation est une cible alléchante pour les auteurs de cybermenace. Votre chaîne d'approvisionnement peut être ciblée par des auteurs de menace compte tenu des raisons suivantes :

- Votre organisation recueille des renseignements personnels de clients (p. ex. nom, adresse, numéro de téléphone, courriel, date de naissance).
- Votre organisation a des secrets commerciaux ou toute autre propriété intellectuelle.
- Vos concurrents veulent savoir qui sont vos clients.
- Votre organisation se sert de systèmes de points de vente pour les données sur les paiements qui contient des informations de carte de crédit et client.
- Vous utilisez des logiciels ou du matériel vulnérable.
- Vous êtes possiblement lié, par l'entremise de votre chaîne d'approvisionnement, à des données ou à des systèmes auxquels s'intéresse un auteur de menace.

N'oubliez pas que même si la sécurité de votre organisation est irréprochable, un seul partenaire vulnérable dans votre chaîne d'approvisionnement est un risque pour vous et pour tous les autres partenaires dans la chaîne.

COMMENT VOUS APPROVISIONNER EN TOUTE SÉCURITÉ ET RÉDUIRE LES RISQUES ?

La première étape consiste à examiner la chaîne d'approvisionnement pour déceler les faiblesses. Il se peut que vous trouviez des vulnérabilités dans vos dispositifs et votre équipement TI. Vous découvrirez peut-être que d'autres aspects de votre chaîne d'approvisionnement sont vulnérables, comme les contrôles d'accès (aux lieux ou aux systèmes), le transport et la source des produits. Au moment d'évaluer votre chaîne d'approvisionnement, considérez d'abord les mesures suivantes :

- Sachez qu'il est possible que le trafiquage et l'utilisation de pièces de remplacement non autorisées se produisent lors de la maintenance ou de la réparation de l'équipement électronique.
- Veillez à ce que seuls des employés de confiance aient accès aux données de nature délicate (p. ex. les secrets commerciaux, l'information financière et les renseignements personnels).
- Sachez ce que vous devez protéger (p. ex. les actifs organisationnels, l'information de nature délicate).
- Prenez le temps d'évaluer le type d'information que vous transmettez aux fournisseurs et aux entrepreneurs.
- Demander et évaluer le plan de sécurité du fournisseur de l'installation si vous avez l'intention de stocker des informations ou des dispositifs sensibles hors site.
- Évaluez le personnel contractuel qui travaillera avec l'information de nature délicate.

SÉRIE SENSIBILISATION

PRÉOCCUPATIONS EN MATIÈRE DE SÉCURITÉ DES TI

Vous devriez collaborer avec vos fournisseurs de services pour prendre des mesures à l'égard des préoccupations relatives à la chaîne d'approvisionnement. Les fournisseurs de services peuvent être la société qui héberge votre magasin en ligne ou l'équipe des services TI à laquelle vous faites appel pour la maintenance de votre équipement.

Exemples de question à poser :

- Quelles mesures prenez-vous afin de protéger les données des clients ?
- Quelle solution de chiffrement des données employez-vous ?
- Où sera stockée toute information sur les clients que nous vous transmettons (dans le nuage, sur place, sur un ordinateur) ?
- Combien de temps conservez-vous l'information que nous vous fournissons ?
- Quelle est votre procédure de destruction des données que nous vous acheminons ?
- Transmettez-vous de l'information à des entrepreneurs de tierce partie ?
- Comment protégez-vous votre réseau et vos dispositifs contre les attaques ?

Vous devriez également avoir des processus et des plans clairs en place afin d'éviter les problèmes de sécurité.

Échantillons de processus :

- Évaluez les entrepreneurs et les fournisseurs continuellement pour vous assurer qu'ils satisfont toujours à vos exigences de sécurité.
- Modifiez la sécurité de votre chaîne d'approvisionnement à mesure que votre organisation évolue.
- Communiquez régulièrement avec les fournisseurs.
- Ajouter des clauses contractuelles pour réduire les risques de la chaîne d'approvisionnement lors de la passation de marchés pour des produits et services qui peut avoir un impact sur votre infrastructure ou vos données.

QU'EST-CE QUE TOUT CELA SIGNIFIE ?

Une chaîne ne peut être plus forte que son maillon le plus faible. La sécurité des TI et la sécurité physique devraient faire partie de vos activités opérationnelles. Vous devriez toujours confirmer que l'équipement que vous achetez et le fournisseur de cet équipement sont fiables et sécurisés. Lorsque vous prenez le temps de comprendre et de protéger votre chaîne d'approvisionnement, vous réduisez la possibilité que des auteurs de menace mettent la main sur votre information de nature délicate. Vos clients seront ainsi plus à l'aise de faire affaire avec vous parce qu'ils savent que vous avez pris les mesures nécessaires pour protéger leur information.

Vous avez des questions où vous avez besoin d'aide ? Vous voulez en savoir plus sur les questions de cybersécurité ? Consultez le site Web du Centre canadien pour la cybersécurité (CCC) à cyber.gc.ca.