CONSEIL CANADIEN DU COMMERCE DE DÉTAIL

CYBERSÉCURITÉ AU DÉTAIL

MODULE 3

CYBERSÉCURITÉ POUR LES RESPONSABLES DES TI DU SECTEUR DU DÉTAIL

Protégez vos équipes, vos appareils, vos biens et votre entreprise.

Un guide pour aider les responsables des TI du secteur du détail et les décideurs d'organisation à protéger leurs équipes et leur entreprise contre la cybercriminalité

CCCD CONSEIL CANADIEN DU COMMERCE DE DÉTAIL

RCC RETAIL COUNCIL OF CANADA

À propos du Conseil canadien du commerce de détail

Nous sommes le plus grand employeur du secteur privé au Canada, avec plus de 2 millions de Canadiens travaillant dans notre secteur. Le secteur génère annuellement plus de 85 G$ en salaires et avantages sociaux. Les ventes au détail de base (à l'exclusion des véhicules et de l'essence) s'élevaient à plus de 462 G$ en 2022. Nos membres représentent plus des deux tiers des ventes au détail du pays. Nous sommes une association à but non lucratif financée par l'industrie qui regroupe des petites, moyennes et grandes entreprises de vente au détail dans toutes les collectivités du pays. Reconnus comme la Voix des détaillantsMC au Canada, nous représentons fièrement plus de 143 000 vitrines dans tous les formats de commerces de vente au détail, y compris les grands magasins, les épiceries, les magasins spécialisés, les magasins à rabais, les détaillants indépendants, les marchands en ligne et les établissements de restauration rapide.

Le Conseil canadien du commerce de détail remercie pour son appui le Programme de subventions pour des collectivités sûres et dynamiques 2022-2024 du ministère du Solliciteur général.

Ontario

© Conseil canadien du commerce de détail 2023. Tous droits réservés.

Toutes les marques commerciales mentionnées dans le présent document appartiennent à leurs propriétaires respectifs. Il est illégal de copier cette ressource sous quelque forme ou par quelque moyen que ce soit, électronique ou mécanique, y compris la photocopie. En acceptant de recevoir ce document, vous vous engagez à respecter la loi sur les droits d'auteur.

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite ou transmise sous quelque forme ou par quelque moyen que ce soit, ou stockée dans une base de données et un système de recherche, sans l'autorisation écrite préalable du Conseil canadien du commerce de détail. Novembre 2023 – Version 1

Coordonnées du Conseil canadien du commerce de détail :

1881 rue Yonge, bureau 800

Toronto (Ontario) M4S 3C4

Sans frais : 888 373-8245

Courriel : education@retailcouncil.org

Table des matières

i. **Introduction** 2

ii. **Évaluation des cybermenaces et des risques connexes** 3

iii. **Élaboration de politiques et de procédures** 4

iv. **Configuration logicielle sécurisée** 6

v. **Sécurisation des comptes** 7

vi. **Sécurité Web** 9
- Navigateur Web 9
- Hébergement Web et sécurité Web de l'entreprise 9
- Communication électronique 11
- Défense contre les maliciels (logiciels malveillants) 11
- Mise en place de pratiques d'authentification appropriées 12
- Signalement des attaques 13

vii. **Sécurisation d'un système de point de vente** 14

viii. **Sécurité des données** 15
- Sauvegarde des données 15
- Traitement des données de nature délicate 16
- Classification et désignation des données de nature délicate 16
- Sécurité de l'infonuagique 17

ix. **Accès à distance** 18
- Notions de base de la téléinformatique 18
- Télétravail à domicile et en déplacement 19

x. **Appareils numériques** 20

xi. **Gestion des interventions en cas d'attaque** 21
- Élaboration d'un plan 21
- Tests d'intrusion 21
- Surveillance et défense du réseau 22

xii. **Sensibilisation et formation à la cybersécurité** 23

xiii. **Assistance** 24

xiv. **Autoévaluation de la cybersécurité** 25

xv. **Ressources pour les détaillants** 29

i. Introduction

Lorsqu'il s'agit de soutenir l'écosystème numérique de la vente au détail d'aujourd'hui, il n'existe pas de rôle plus essentiel que celui du professionnel des technologies de l'information (TI). Étant impliqué dans chaque aspect du parcours numérique d'un détaillant, il supervise et orchestre presque tous les ajustements, adaptations et installations effectués sur son réseau numérique et son infrastructure technologique en constante expansion et évolution, et est responsable de leur maintenance et de leur optimisation. Par ailleurs, le professionnel des TI du secteur du détail se charge de procéder à la sécurisation de l'organisation à l'aide de divers outils, mesures et protocoles qui la protègent des menaces posées par les cybercriminels.

Quelle que soit la taille de votre service des TI ou de votre organisation, il est essentiel d'élaborer et d'appliquer un ensemble de procédures normalisées en vertu desquelles les employés agiront, garantissant ainsi l'uniformité des tâches et des résultats et l'adoption d'un comportement sécuritaire au sein de l'écosystème numérique de la vente au détail. Il est également important que les professionnels des TI, ou les personnes responsables de la maintenance et de l'entretien techniques, mettent en place les outils et les logiciels nécessaires à la protection des ordinateurs, des appareils, des réseaux et des systèmes de l'organisation.

Compte tenu de la prolifération et de la fréquence croissante des cyberattaques (une étude récente de Mastercard estime que la cybercriminalité a augmenté de 600 % depuis le début de la pandémie), le professionnel des TI du secteur du détail joue désormais un rôle beaucoup plus important dans le bon fonctionnement et la réussite de l'organisation de vente au détail.

Pour appuyer les efforts des employés du secteur responsables de la protection de l'écosystème numérique de leur organisation et du développement de leur marque, le Conseil canadien du commerce de détail a élaboré le guide intitulé « Cybersécurité pour les responsables des TI du secteur du détail ». Ce guide axé sur les principaux aspects et couches de l'écosystème numérique de la vente au détail à protéger renferme des renseignements utiles, des orientations et des pratiques exemplaires. Il est destiné à devenir la ressource et la référence de prédilection des professionnels des TI du secteur du détail luttant contre la cybercriminalité.

Conséquences de la cybercriminalité :

- Le coût moyen des atteintes à la sécurité des données au Canada est de 5,64 M$, soit 1 M$ de plus que les moyennes mondiales, et 99 % des victimes reconnaissent que le piratage a nui à leurs activités commerciales*.
- Les détaillants ont indiqué qu'une atteinte à la sécurité des données entraîne principalement la perte de données clients*.
- Seulement en 2022, la cybercriminalité et la fraude ont coûté plus de 500 M$ aux Canadiens**.
- Chaque année, 24 % des cyberattaques ciblent les détaillants – de tous les secteurs, celui du détail est le plus visé***.
- Lors d'une attaque, 42 % des données compromises sont liées au paiement, et 41 % sont des renseignements qui permettent l'identification d'une personne****.

** Selon l'étude « Securing the digital economy » de Mastercard.*

*** Selon les données de la GRC.*

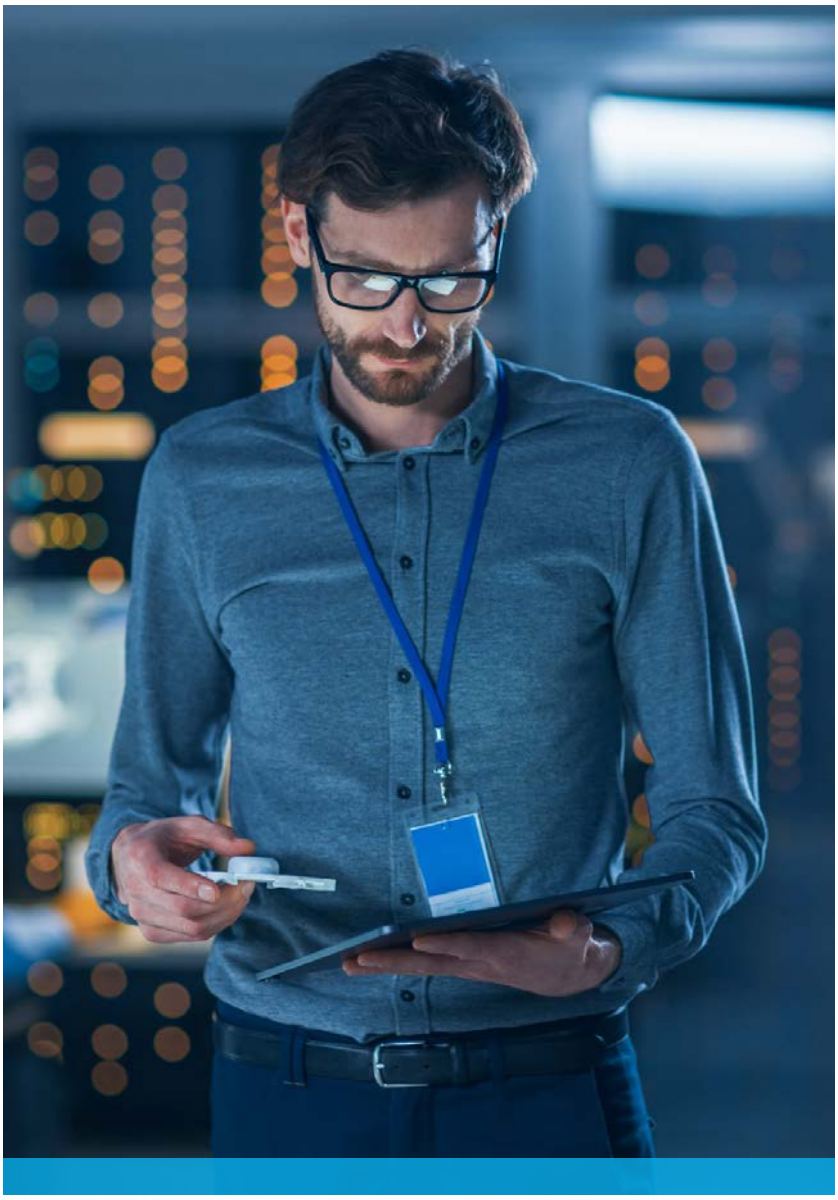
**** Selon Trustwave.*

***** Selon Verizon.*

ii. Évaluation des cybermenaces et des risques connexes

Le détaillant recevra le soutien de la fonction des TI de son organisation à chaque étape de son parcours numérique, et ce, dès le lancement de celui-ci. Chacune de ces étapes joue un rôle crucial dans la sécurisation de l'écosystème numérique, en particulier celles d'entame, comme l'élaboration de la politique de sécurité de l'entreprise.

Détermination et hiérarchisation



Avant d'élaborer tout plan, la fonction des TI est de cerner les cybermenaces potentielles auxquelles fait face le détaillant et les risques qui peuvent en découler, afin de déterminer les outils et les pratiques à mettre en place pour assurer la sécurité de son environnement numérique.

Une fois cette tâche terminée, la fonction des TI est de travailler avec la direction à la hiérarchisation des menaces en fonction d'un certain nombre de facteurs, dont la probabilité de leur occurrence, ainsi que la nature et la gravité des risques encourus.

Élaboration d'un plan

Dès que les menaces et les risques connexes auront été cernés, il sera temps d'élaborer un plan de cybersécurité complet qui décrira les politiques, les procédures et les protocoles à suivre, lesquels préciseront les mesures de protection, les outils et les ressources nécessaires à l'atténuation des menaces et à la limitation des risques pour l'entreprise.

Le plan établira clairement les rôles et les responsabilités des employés de l'organisation, ainsi que les attentes à leur égard pour ce qui est du maintien de la sécurité de l'entreprise.

iii. Élaboration de politiques et de procédures

Une fois que toutes les cybermenaces auront été répertoriées et catégorisées par l'entreprise, le responsable des TI devra œuvrer à l'élaboration de politiques et de procédures opérationnelles normalisées qui aideront les employés à accomplir presque toutes leurs tâches ayant trait à l'écosystème numérique. Ces politiques et procédures contribueront grandement à favoriser l'uniformité opérationnelle, tout en devenant des ressources de référence en appui de l'objectif d'un plan officiel et complet de cybersécurité.

Choses que les employés doivent faire et ne doivent pas faire

Pour avoir un véritable sens et être efficace, tout plan de cybersécurité doit établir un ensemble solide de politiques, de procédures et de protocoles indiquant clairement aux employés les choses à faire et à ne pas faire en matière de cybersécurité. Le responsable des TI, qui est chargé de l'élaboration de ces politiques et procédures, veillera à leur respect avec l'aide de la direction.

Le plan de cybersécurité comprendra notamment des politiques liées à l'utilisation d'Internet et des médias sociaux, au traitement des données, à l'usage approprié des appareils mobiles et des ordinateurs et à la communication à distance. Du point de vue des détaillants, ce type de plan a une double finalité : 1) protéger leurs actifs, leurs employés et leurs clients; et 2) créer des normes en vertu desquelles ils mèneront leurs activités dans le domaine et le paysage numériques, ce qui permettra de diminuer leur marge d'erreur interne.

Il est possible de réaffirmer ces normes dans des documents de compilation des procédures opérationnelles normalisées auxquels les employés se référeront à tout moment.

Lorsqu'il commencera à élaborer des politiques et des procédures de cybersécurité propres à son organisation, le responsable des TI devra tenir compte des éléments suivants :

Faire simple dans un premier temps – Il est préférable de commencer par mettre au point un plan de cybersécurité relativement basique contenant des politiques et des procédures fondamentales, auxquelles viendront ensuite s'ajouter des renseignements plus détaillés et complexes.

Cerner et adapter les normes existantes – Le responsable des TI s'attachera d'emblée à intégrer dans le plan de cybersécurité le plus grand nombre possible de politiques et de procédures efficaces existantes afin de préserver l'uniformité opérationnelle et de lever toute incertitude.

Expliquer le raisonnement – Pour que les politiques et les procédures soient les plus efficaces possible, il faut que les employés comprennent les raisons pour lesquelles elles sont en place et la manière dont elles contribuent à protéger l'entreprise, ses actifs, ses employés et ses clients.

Relire, réétudier et réviser – Comme dans le cas de presque tous les autres documents existants, chaque détaillant doit régulièrement réétudier son plan de cybersécurité, et le réviser au besoin.

En dépit de l'expertise et des connaissances qui sous-tendent tout plan de cybersécurité, l'exécution de ce dernier et l'application de ses pratiques exemplaires nécessitent un leadership de la part du responsable des TI, notamment la communication à tous les employés de conseils et de directives concernant les activités de cybersécurité, leur participation active à divers projets liés à la cybersécurité et la collaboration avec des experts externes, comme des conseillers juridiques, au besoin.

Bien que le processus d'élaboration d'un plan de cybersécurité puisse sembler intimidant au premier abord, n'oubliez pas que vous pouvez toujours réviser et développer votre plan au fil du temps.

iv. Configuration logicielle sécurisée

Dans l'environnement du commerce de détail, le responsable des TI a également l'importante responsabilité de veiller à ce que tous les nouveaux appareils et logiciels soient intégrés au réseau ou système d'appareils et de logiciels existant de manière sécuritaire et qu'ils ne compromettent pas l'organisation ou ne créent pas des vulnérabilités imprévues.

Il est particulièrement important que les petites organisations prêtent attention aux configurations de leurs appareils et logiciels, car les configurations par défaut du fabricant ne tiennent généralement pas compte de la sécurité de l'utilisateur final. Les commandes de base, les services et ports ouverts, les comptes ou mots de passe par défaut et les paramètres DNS (systèmes de noms de domaine) préconfigurés sont autant de facteurs qui peuvent exposer un détaillant à la cybercriminalité. De plus, les équipes des TI devront systématiquement gérer les mises à jour de leurs configurations afin d'empêcher toute dégradation du niveau de sécurité.

Il existe un certain nombre de mesures de protection et de pratiques exemplaires qui peuvent aider les responsables des TI et leurs équipes à assurer la sécurité et la maintenance de leurs configurations logicielles :

- Établir et maintenir un processus de configuration sécurisé
- Établir et maintenir un processus de configuration sécurisé pour l'infrastructure réseau
- Configurer le verrouillage automatique des sessions sur les actifs d'entreprise
- Installer et gérer un pare-feu sur les serveurs et les appareils
- Gérer en toute sécurité les actifs et les logiciels d'entreprise
- Gérer les comptes par défaut sur les actifs et les logiciels d'entreprise
- Désinstaller ou désactiver les services inutiles sur les actifs d'entreprise
- Configurer des serveurs DNS fiables sur les actifs d'entreprise
- Activer le verrouillage automatique sur les appareils portables des utilisateurs finaux
- Activer la fonctionnalité d'effacement à distance sur les appareils portables des utilisateurs finaux
- Créer des espaces de travail distincts sur les appareils mobiles des utilisateurs finaux

v. Sécurisation des comptes

Les cybercriminels emploient des tactiques de plus en plus sophistiquées pour obtenir un accès non autorisé à des données de nature délicate. Cependant, aucune d'entre elles ne sera jamais aussi efficace que l'utilisation d'identifiants utilisateur valides. Dans ce contexte, il est extrêmement important que le responsable des TI garantisse le bon fonctionnement et la sécurité de l'écosystème numérique de la vente au détail dans son ensemble en ayant recours à des processus et à des outils d'attribution et de gestion de l'autorisation des identifiants pour tous les comptes utilisateur et administrateur de l'entreprise. Il est particulièrement utile de ne gérer que les comptes administratifs étant donné qu'il est possible d'ajouter des utilisateurs et d'apporter des modifications aux actifs de l'entreprise à partir de ceux-ci.

Suivi des comptes

Le responsable des TI devra inventorier les différents comptes utilisés au sein de son organisation de vente au détail et en faire le suivi pour les gérer de façon convenable et efficace. Il est également important d'inventorier les activités de journalisation des comptes et d'en faire le suivi, car nombre d'entre eux offrent des points d'accès principaux au réseau et aux systèmes d'une organisation, donnant ainsi aux cybercriminels un moyen facile d'y accéder.

Gestion de l'accès

En plus d'inventorier les comptes et d'en faire le suivi, le responsable des TI devra utiliser des processus et des outils de création, d'attribution, de gestion et de révocation des identifiants de tous les comptes utilisés au sein de l'organisation et des droits d'accès à ceux-ci.

Afin d'assurer l'efficacité des mécanismes de contrôle de sécurité des comptes, le responsable doit également attribuer des autorisations en fonction des rôles, ce qui réduit autant que possible l'accès aux comptes. Pour appuyer ce processus, il convient donc d'attribuer des droits d'accès uniformes à chaque rôle. Il s'agira d'un processus au moyen duquel l'accès aux comptes peut facilement être accordé et révoqué si nécessaire.

Afin de gérer efficacement et avec précision les comptes et l'accès des utilisateurs à ceux-ci, le responsable des TI devra veiller à faire ce qui suit :

- Établir et tenir à jour un inventaire des comptes
- Utiliser des mots de passe uniques
- Désactiver les comptes inactifs
- Réserver les droits d'administrateur aux comptes administrateur
- Établir et tenir à jour un inventaire des comptes de service
- Centraliser la gestion des comptes
- Établir un processus d'octroi d'accès
- Établir un processus de révocation d'accès
- Établir et tenir à jour un inventaire des systèmes d'authentification et des systèmes autorisés
- Centraliser le contrôle d'accès
- Définir et maintenir l'accès fondé sur les rôles

vi. Sécurité Web

Afin de bien protéger l'environnement numérique de la vente au détail contre la cybercriminalité, les responsables des TI et leurs équipes devront s'assurer de sécuriser tout ce qui touche l'Internet. Compte tenu du grand volume d'activités en ligne menées par les employés des commerces de détail, il leur faut adopter l'approche la plus holistique possible.

Deux des principaux domaines les plus vulnérables à la cybercriminalité sont les communications par courrier électronique et la navigation sur le Web. Par conséquent, le responsable des TI doit axer une grande partie de ses efforts sur la mise en place de mesures de protection de premier ordre et la détection des diverses cybermenaces.

Navigateur Web

Les responsables des TI et leurs équipes doivent impérativement installer les fonctionnalités de sécurité et les correctifs de navigateur les plus récents pour garantir une navigation sécurisée au sein de leur organisation. Grâce à la configuration d'un navigateur Web unique, les détaillants peuvent empêcher leurs employés d'installer intentionnellement ou involontairement des logiciels malveillants à partir d'Internet en limitant leur capacité à installer des modules complémentaires, des plugiciels, des extensions ou toute autre chose du genre et en empêchant l'exécution automatique du contenu nuisible sur les appareils.

Hébergement Web et sécurité Web de l'entreprise

Il se peut que le site Web soit également un domaine de l'écosystème numérique vulnérable aux attaques. S'il n'est pas correctement sécurisé, il pourrait être une cible facile pour les cybercriminels.

Les entreprises hébergent leurs sites Web de différentes manières. Certaines recommandations s'imposent selon l'hébergement privilégié par votre organisation.

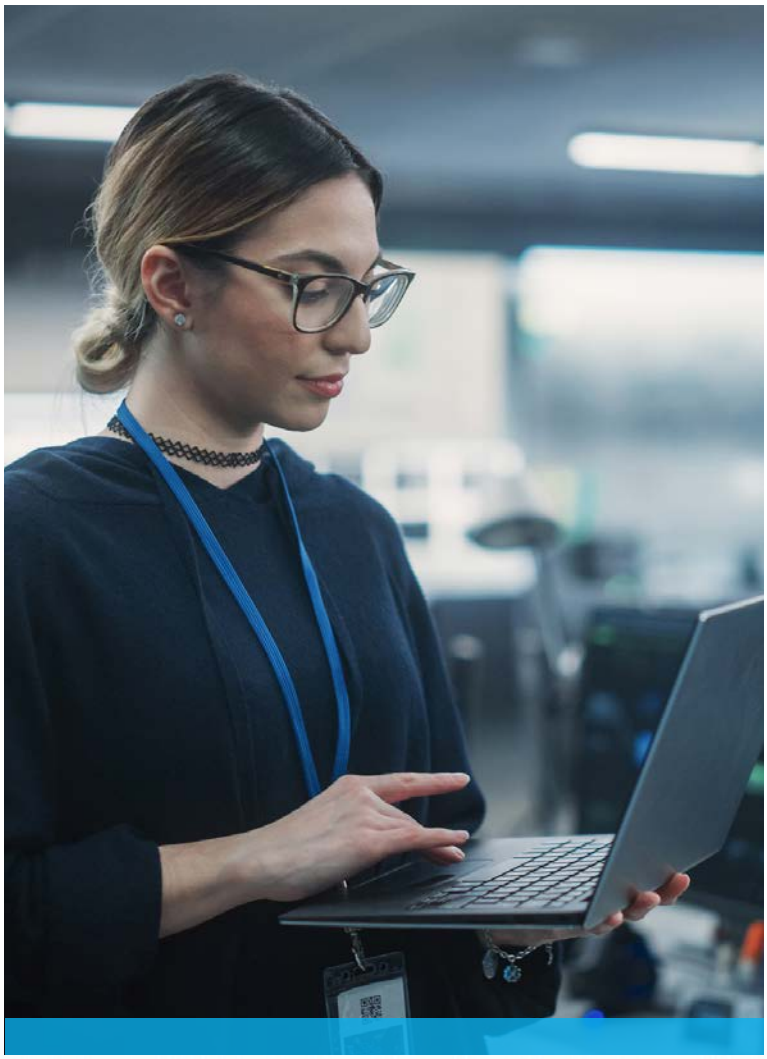
Hébergement sur des serveurs internes :

Restreindre l'accès – Permettez seulement aux employés autorisés d'y accéder.

Procéder aux mises à niveau – Les professionnels des TI doivent s'assurer que toutes les mises à niveau proposées ont été appliquées aux systèmes d'exploitation afin d'éviter tout problème et d'éliminer toute vulnérabilité.

Effectuer régulièrement des sauvegardes – Les professionnels des TI doivent s'assurer que les systèmes d'entreprise font régulièrement l'objet de sauvegardes, de préférence sur un serveur situé dans un endroit distinct. Ils doivent définir un processus à cet effet.

Veiller à la consignation des activités du serveur – Désignez une personne responsable des serveurs et veillez à ce qu'elle examine régulièrement les journaux de ces derniers aux fins de détection de toute activité suspecte.



Hébergement par l'intermédiaire åd'un service tiers :

S'assurer qu'un plan est en place – Le responsable des TI doit veiller à ce que le fournisseur de services dispose de son propre plan de sécurité et à ce que certaines pratiques exemplaires soient appliquées, parmi lesquelles l'analyse de ses serveurs Web et de votre site Web pour cerner tout problème potentiel et le régler dès sa détection, la surveillance du site Web et des systèmes de votre organisation pour détecter toute activité suspecte, la protection du site Web de votre organisation et la résolution des perturbations ou des défaillances causées par un acte cybercriminel.

Il est également important que le responsable des TI soit prêt à remédier à toute compromission du système à la suite d'une cyberattaque, en sachant qu'il pourrait notamment être amené à réduire le service, à passer à un serveur de sauvegarde, à utiliser un autre fournisseur de services, ou, dans le pire des cas, à fermer temporairement le site Web. En conséquence, il devra établir un plan et des tactiques permettant de remédier à des scénarios de défaillance de serveur qu'il a lui-même imaginés.

Communication électronique

La plupart, sinon la totalité, des communications entre collègues, associés et partenaires commerciaux se font aujourd'hui par courriel. Toutefois, comme nous l'avons mentionné, les cybercriminels ciblent souvent les courriels pour infiltrer les ordinateurs, appareils et systèmes des détaillants afin de s'emparer de données personnelles et professionnelles de nature délicate.

Afin d'empêcher les cybercriminels d'accéder facilement au réseau et aux systèmes internes des commerces de détail, le responsable des TI peut prendre les précautions suivantes pour sécuriser les communications électroniques :

Filtrage des communications – En mettant en œuvre un filtre antipourriel, les détaillants s'assurent d'exclure de leur boîte de réception la plupart des courriels potentiellement dangereux envoyés par les cybercriminels.

Chiffrement des données – Empêchez les cybercriminels de lire et de comprendre les données en chiffrant les courriels à l'aide du protocole HTTPS.

Utilisation de mots de passe complexes – Prônez l'usage de mots de passe complexes pour tous les comptes de messagerie utilisés au sein de l'entreprise, aussi bien à des fins professionnelles que personnelles.

Courriels génériques – Dans la mesure du possible, le responsable des TI doit prôner l'utilisation de courriels génériques afin d'éviter d'utiliser le nom des employés.

Défense contre les maliciels (logiciels malveillants)

Étant donné que l'ensemble du paysage et de l'écosystème numériques de la vente au détail repose sur une série quasi infinie de logiciels, de systèmes, de programmes et d'applications auxquels il est connecté, les menaces posées par les maliciels sont innombrables et, le plus souvent, très perturbatrices et destructrices. Certains types de maliciels, comme les vers, les chevaux de Troie, les rançongiciels, les logiciels espions ou encore les logiciels publicitaires, sont capables d'infecter les systèmes d'exploitation pour ensuite faire une copie d'eux-mêmes et infiltrer d'autres appareils.

Que peut faire le responsable des TI?

Bien que les maliciels soient souvent redoutablement efficaces, le responsable des TI peut protéger les systèmes commerciaux et les données numériques de son entreprise en prenant les mesures suivantes :

Logiciels antimaliciels – En raison de la prolifération de différents types de maliciels, il existe aujourd'hui une gamme de logiciels antimaliciels qui permettent aux utilisateurs d'analyser tous les fichiers entrant dans l'organisation et de bloquer tout ce qu'ils jugent suspect ou qui contient des maliciels.

Pare-feux – Les détaillants peuvent aussi installer des pare-feux informatiques afin d'empêcher la connexion à des sites Web malveillants et néfastes. De plus, de nombreux pare-feux sont capables d'empêcher l'intrusion de différents types de maliciels dans le système.

Mise en place de pratiques d'authentification appropriées

Lorsque l'on traite des volumes importants de données et de renseignements de nature délicate, il est extrêmement important que les pratiques d'authentification mises en place par les détaillants soient respectées par tous les employés.

Mots de passe

Couramment utilisés pour protéger différents comptes et systèmes contenant une pléthore de données et d'outils professionnels, les mots de passe constituent une couche de protection nécessaire dans l'écosystème numérique de la vente au détail. Cependant, s'ils ne sont pas utilisés correctement, les mots de passe peuvent constituer une vulnérabilité au sein des entreprises et les exposer davantage aux menaces des cybercriminels.

Maintenir le contrôle et la confidentialité – Veillez à ce que les employés aient conscience de l'importance de protéger leurs mots de passe et de ne pas les révéler à leur entourage.

Éviter d'utiliser des mots de passe faibles – Les employés doivent éviter d'utiliser des mots de passe faciles à deviner qui peuvent permettre à d'autres personnes d'accéder à leurs fichiers et à leurs données.

Éviter d'utiliser toujours le même mot de passe – Il convient de préciser à tous les employés qu'ils doivent non seulement éviter d'utiliser des mots de passe faciles à deviner, mais aussi éviter de toujours utiliser le même mot de passe pour leurs comptes et sur les différents appareils dont ils se servent.

Modifier fréquemment le mot de passe – Tous les employés doivent fréquemment modifier leurs mots de passe afin de ne pas céder à la complaisance et de les rendre moins prévisibles.

Établir une politique – Il peut être judicieux pour le responsable des TI d'élaborer une politique en matière de mots de passe avec l'aide de la direction afin d'établir des règles simples à suivre lors de la création d'un mot de passe.

Éviter les mots de passe courants et simples – Lors de la création de leurs mots de passe, les employés doivent éviter d'utiliser des expressions courantes telles que « mot de passe » ou « saisir », des séquences de chiffres simples telles que « 1234 », et des noms personnels faciles à deviner tels que le prénom d'un enfant.

Privilégier les longs mots de passe – Plus le mot de passe comporte de caractères, plus il est efficace. Veillez donc à encourager les employés à créer des mots de passe d'au moins huit caractères.

Recourir à des combinaisons – Les mots de passe sont également plus forts lorsque plusieurs types de caractères (lettres majuscules, lettres minuscules, chiffres et caractères spéciaux) sont utilisés.

Phrases de passe

Pour les détaillants qui souhaitent renforcer leur sécurité, l'utilisation de phrases de passe au lieu de mots de passe peut être une solution judicieuse.

Par exemple, au lieu d'utiliser le mot de passe « G0bLUe! », une phrase de passe telle que « Ceuxqui-resterontserontchampions! » devient beaucoup plus difficile à deviner. De plus, des sigles peuvent être utilisés à la place de longues phrases (par exemple, « bravoauxchampionsquiresterontpourtoujours! » devient « brvxchmpnsqlrstrntprtjrs! »), ce qui réduit le nombre de caractères à taper, mais maintient l'efficacité de la protection et de la sécurité.

Les cybercriminels créent constamment des logiciels destinés à pirater les systèmes et deviner les mots de passe. Dans ce contexte, les professionnels des TI doivent recommander aux utilisateurs de se servir d'outils démontrant la force ou la faiblesse relative d'un mot de passe ou d'une phrase de passe.

Authentification à deux facteurs

Bien plus difficile à deviner que les mots de passe ou les phrases de passe, l'authentification à deux facteurs permet d'ajouter une couche de complexité et de sécurité aux systèmes des détaillants.

Comme son nom l'indique, l'authentification à deux facteurs exige que la personne ou le système demandant une autorisation d'accès fournisse deux éléments d'authentification. Le premier facteur est connu par la personne ou le système (comme un mot de passe), et le second facteur est un élément, permanent ou temporaire, qui peut être utilisé pour valider l'identité de la personne ou du système (comme une empreinte digitale ou un mot de passe temporaire).

Alors que les technologies deviennent de plus en plus puissantes et intuitives, et que les capacités de l'intelligence artificielle et de l'apprentissage automatique augmentent sans cesse, l'authentification à deux facteurs devient indispensable au renforcement de la protection et de la sécurité des actifs, des données et des systèmes des détaillants.

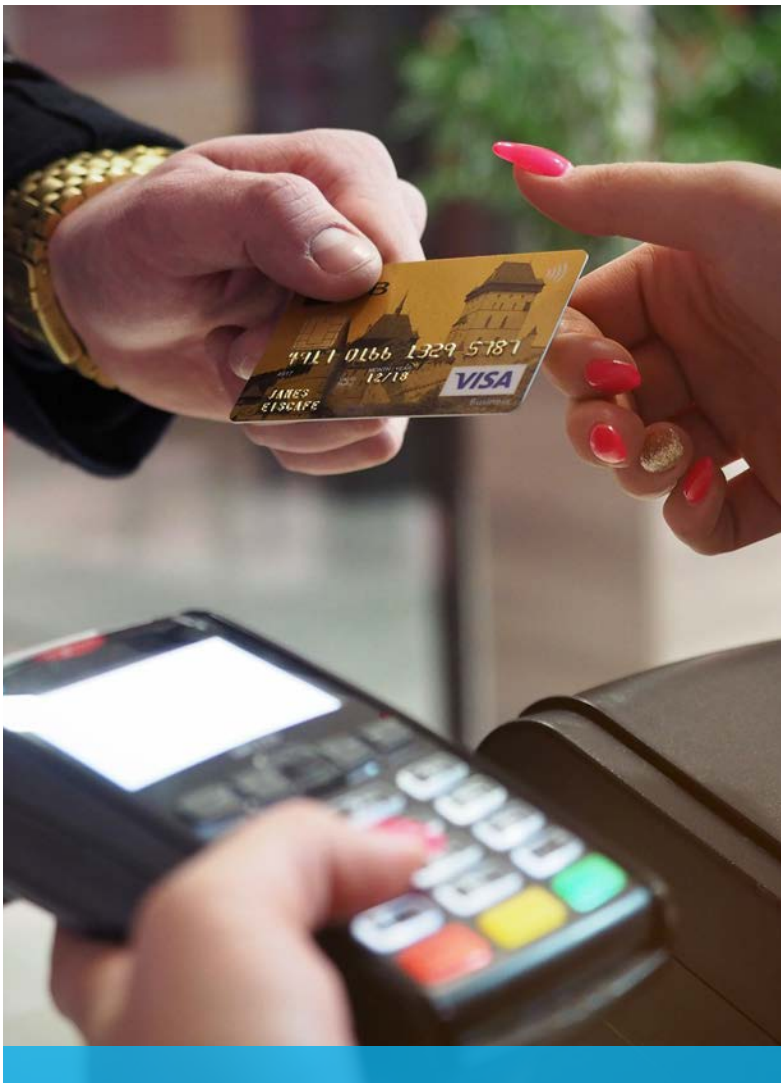
Signalement des attaques

Si un acte de cybercriminalité semble avoir compromis son entreprise d'une manière ou d'une autre, le détaillant doit faire ce qui suit :

- ***Signalement de l'attaque aux forces de l'ordre***
- ***Signalez l'attaque au système de signalement des incidents de cybercriminalité et de fraude. Ce signalement sera automatiquement transmis à la Gendarmerie royale du Canada (GRC), au Centre national de coordination en cybercriminalité (CNC3) et au Centre antifraude du Canada (CAFC) afin de protéger directement l'organisation et de l'aider à se prémunir contre des menaces similaires.***

vii. Sécurisation d'un système de point de vente

Au vu de l'envergure de l'écosystème numérique actuel, il est plus que probable que votre organisation utilise un système de point de vente électronique pour exécuter et traiter les transactions financières en magasin. Cette forme de technologie est omniprésente dans le monde des affaires d'aujourd'hui, permettant ainsi aux commerçants d'accepter les paiements par carte de crédit et de débit. Cependant, comme dans le cas de tout ce qui a trait au numérique, les systèmes de point de vente présentent également des vulnérabilités, ce qui oblige les responsables des TI et leurs équipes à faire tout ce qui est en leur pouvoir pour garantir la sécurité des paiements.



Le responsable des TI peut améliorer la sécurité des systèmes de point de vente en prenant les mesures suivantes :

S'assurer qu'un pare-feu est en place – Il est essentiel de placer votre système de point de vente derrière un pare-feu de sécurité. Il s'agit de l'unique moyen de limiter le trafic entrant et sortant du réseau. Le fournisseur d'accès à Internet de votre organisation/magasin a sans doute installé un pare-feu sur votre routeur, mais il est préférable de vérifier si tel est le cas et de s'assurer de sa fiabilité.

Mettre en place une technique de chiffrement renforcée – Il est extrêmement important de renforcer le chiffrement de toutes les données transactionnelles contenant des renseignements sur les titulaires de carte avant de les transmettre au fournisseur de services du système de point de vente.

Veiller à créer des noms d'utilisateur et des mots de passe uniques – Il vous est fortement recommandé d'éviter d'utiliser le nom d'utilisateur et le mot de passe par défaut fournis avec votre système de point de vente. Ceux-ci vous exposent directement aux cybercriminels, qui cherchent le moyen le plus simple d'accéder à votre écosystème numérique et à votre entreprise.

Limiter l'accès – Votre organisation doit limiter l'accès aux données clients aux personnes qui en ont besoin et qui sont autorisées à les consulter.

Effectuer les mises à jour nécessaires – Il est toujours bon de conserver une longueur d'avance sur les logiciels antimaliciels, en mettant à jour tous les systèmes numériques aussi fréquemment et uniformément que possible.

viii. Sécurité des données

Avec l'évolution de la numérisation, les détaillants sont en possession d'une énorme quantité de données qu'ils traitent en permanence. Compte tenu de l'importance des données qu'ils collectent chaque jour pour la croissance de leurs entreprises et l'optimisation de leurs opérations, il est logique qu'elles soient sécurisées et protégées aussi rigoureusement que n'importe quel autre actif.

Pourquoi sauvegarder les données?

La sauvegarde des fichiers numériques et physiques est une pratique qui permet de conserver les données importantes et de restaurer les fichiers perdus ou endommagés. De plus, et c'est peut-être le plus important, les plans de sauvegarde bien exécutés à intervalles réguliers permettent aux détaillants de se rétablir rapidement en cas de panne du système, de corruption des données ou d'autres problèmes.

Sauvegarde des données

Le moyen le plus efficace pour les détaillants de garantir la bonne conservation des données est d'élaborer un plan de sauvegarde. Il s'agit d'un plan auquel tous les employés de l'entreprise se conformeront, en respectant un ensemble strict de pratiques de sauvegarde.

Sauvegardes fréquentes – Les employés doivent sauvegarder régulièrement les données conformément au plan de sauvegarde, que ce soit toutes les heures ou tous les jours.

Stockage physique – En plus d'être régulièrement sauvegardées, les données doivent être sauvegardées de différentes manières, notamment sur des disques durs physiques, afin d'ajouter une couche de sécurité.

Destruction des données – Les données qui n'ont pas été sauvegardées et qui seront éliminées par l'entreprise doivent être détruites adéquatement. Il vous faut donc supprimer tous les fichiers numériques et déchiqueter tous les documents physiques afin d'éviter qu'ils ne soient utilisés contre l'entreprise.

Options de sauvegarde

Les entreprises de vente au détail peuvent sauvegarder leurs données de plusieurs manières, afin de garantir leur sécurité à court et à long terme.

Disque dur externe – Selon la taille de l'entreprise, les disques durs externes portables ou fixes peuvent constituer une option de sauvegarde appropriée.

Serveur – L'idéal serait que les données soient stockées sur le réseau local (LAN) de l'entreprise et sauvegardées automatiquement à partir de là.

En ligne – Les détaillants peuvent également choisir de sauvegarder leurs données sur Internet, ce qui permet à des fournisseurs de services tiers de se charger de leur sauvegarde et de leur restauration.

Traitement des données de nature délicate

Compte tenu de la quantité de données traitées par les détaillants, au moins une partie d'entre elles peuvent être de nature délicate, comme les renseignements personnels des employés, ainsi que les données relatives aux clients et aux finances. Tout traitement inapproprié de ces données pourrait donc entraîner un accès non autorisé à celles-ci, leur perte, leur instrumentalisation ou leur modification, ainsi qu'une série de préjudices pour les entreprises et leurs clients. Compte tenu de ce qui précède, tous les employés doivent connaître les pratiques exemplaires liées au traitement des données de nature délicate.

Accès restreint – Lorsque les données ne sont pas utilisées, qu'il s'agisse de fichiers numériques ou physiques, elles doivent être mises sous clé, avec un accès limité à un petit nombre d'employés, et sécurisées par une combinaison de mesures de protection électroniques et physiques.

Attribution de la bonne désignation – Afin de garantir la bonne conservation des données de nature délicate, les dossiers et les documents doivent être correctement nommés et stockés en conséquence.

Destruction totale – Tout document contenant des données de nature délicate doit être détruit à l'aide d'une déchiqueteuse à papier de haute qualité qui coupe les feuilles en tout petits morceaux. Les dossiers papier et les données stockées sur des disques doivent être détruits de la même manière. En ce qui concerne la destruction des données stockées sur les lecteurs ou les ordinateurs, les outils commerciaux d'effacement ou de suppression feront l'affaire.

Classification et désignation des données de nature délicate

Pour être à même de repérer les données de nature délicate, les responsables des TI et leurs équipes doivent d'abord bien connaître leurs caractéristiques distinctives.

Pour ce faire, ils doivent tenir compte de ce qui suit :

Lieu de stockage – Il est important que le responsable des TI détermine si les données se trouvent au sein de l'organisation, que ce soit sur un serveur, dans l'infonuagique ou ailleurs.

Répercussions potentielles – Pour savoir si elles sont de nature délicate, les données doivent être évaluées en fonction de la gravité des répercussions potentielles de leur perte ou de leur endommagement. Classez-les simplement sur une échelle allant de 1 à 5 – 1 correspondant aux répercussions les plus faibles, et 5 correspondant aux répercussions les plus graves.

Traitement prudent – Les données situées au haut de l'échelle (les données les plus délicates ne seront pas les mêmes d'une organisation à une autre) doivent se voir attribuer la désignation de « données de nature délicate » et être traitées avec prudence.

Une fois l'évaluation terminée, le responsable des TI doit chercher à renforcer les mesures de sécurité et de contrôle associées à la désignation et au traitement des données de nature délicate en classant ces dernières avec l'aide de chaque service de l'organisation.

Donnée publique – Ce type de donnée n'est aucunement de nature délicate et peut être consulté par tout un chacun, que ce soit à l'intérieur ou à l'extérieur de l'entreprise. Il ne nécessite ni désignation ni traitement spécial.

Donnée à accès restreint – Ce type de donnée est de nature plus délicate et doit être désigné en tant que « donnée à accès restreint ». Seul un groupe restreint de personnes ont accès à ces données qui font l'objet d'un certain nombre de mesures de protection différentes.

Donnée confidentielle – Ce type de donnée ne peut être consulté que par un groupe extrêmement limité d'employés autorisés. Il doit être désigné en tant que « donnée confidentielle » et ne devrait jamais être autorisé à sortir des systèmes de l'organisation, pour quelque raison que ce soit.

Sécurité de l'infonuagique

L'infonuagique est l'une des dernières innovations les plus saluées de l'ère numérique. Étant donné qu'elle permet l'utilisation de ressources accessibles sur le Web, en dehors d'une organisation, cette solution informatique puissante est généralement utilisée en conjonction avec des solutions de transaction et de traitement des paiements, de gestion des documents et des comptes, et bien plus encore. Pilotée par un logiciel puissant, l'infonuagique permet souvent aux utilisateurs de personnaliser les services dont ils se servent, de sorte à répondre aux besoins et respecter le budget de leur organisation. Cependant, compte tenu du volume de données en jeu, dont une grande partie est de nature délicate, les responsables des TI devront faire preuve de diligence raisonnable dans le cadre de la recherche d'options infonuagiques pour leur entreprise.

Voici les éléments dont les responsables des TI doivent tenir compte lorsqu'ils étudient les différentes options de logiciel infonuagique s'offrant à leur organisation :

Lire les avis – Il est important que les responsables des TI lisent le plus grand nombre possible d'avis et cherchent à obtenir des recommandations au sujet des différents fournisseurs de services infonuagiques envisagés.

Poser des questions sur la fiabilité de la solution – Lorsque vous parlez à un fournisseur de services infonuagiques, interrogez-le d'emblée sur la fiabilité de ses services et sur son rendement passé.

Gérer l'accès – Comme dans le cas de tous les autres comptes de l'organisation, l'accès aux services infonuagiques doit être limité et déterminé à l'avance.

Prendre son temps – Le choix d'un fournisseur de services infonuagiques constitue une décision importante qui peut avoir de graves conséquences. Les responsables des TI ne doivent pas prendre de décision tant qu'ils n'ont pas parfaitement connaissance de toutes leurs options.

ix. Accès à distance

Beaucoup de choses ont changé dans l'environnement des entreprises nord-américaines au cours des dernières années, notamment en raison de la popularité croissante du travail à distance et l'adoption de ces nouvelles modalités de travail par les entreprises partout dans le monde. Le télétravail s'est avéré un véritable atout pour les entreprises, leur permettant de gagner du temps et d'économiser de l'argent tout en stimulant la productivité des employés. Toutefois, cette évolution des conditions et de l'environnement de travail s'accompagne d'une hausse des risques d'exposition aux cybercriminels et à leurs stratagèmes numériques. En mettant en place les bons contrôles et en garantissant l'adoption de pratiques exemplaires, il est possible d'atténuer une grande partie de la menace posée par les cybercriminels.

Notions de base de la téléinformatique

Pour les commerces de détail qui ont décidé d'accorder à leurs employés les avantages du télétravail, l'accès à leurs réseaux se fera probablement par Internet. Il s'agit d'un moyen facile et efficace de connecter les employés à leur travail, quel que soit l'endroit où ils se trouvent, mais la connexion par Internet n'est pas considérée comme un moyen sûr d'échanger des informations, car elle offre aux cybercriminels plus de possibilités que jamais d'exploiter les faiblesses des politiques et des pratiques numériques.

Il est donc judicieux que les responsables des TI proposent aux employés un réseau privé virtuel (VPN) sécurisé pour la connexion aux réseaux de l'entreprise, car un VPN permet de chiffrer la connexion, ce qui rend les communications et les données transférées inutilisables pour toute personne autre que celle à qui le message a été envoyé.

Les services des TI doivent combiner leur VPN à d'autres mesures et couches de protection mentionnées dans ce guide, et s'associer à leur direction pour faire en sorte que les employés suivent un ensemble de pratiques exemplaires garantissant la sécurité de l'accès à distance.

Afin d'assurer la sécurité du travail à distance, les services des TI doivent :

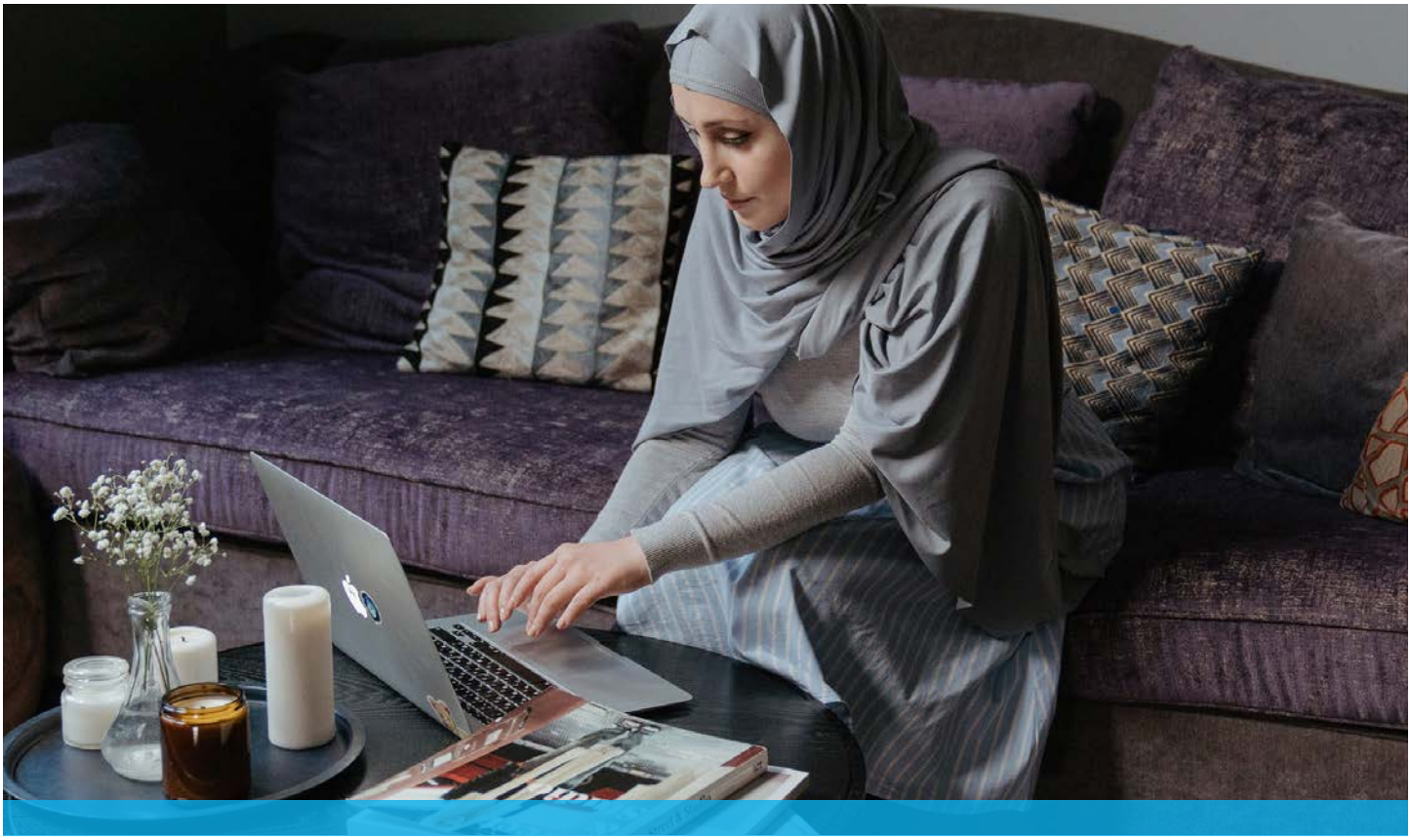
Limiter l'accès – L'accès à distance doit être réservé aux employés autorisés ayant un besoin professionnel clair. Par ailleurs, il doit seulement concerner les applications, renseignements et services nécessaires à l'exécution du travail.

Accorder l'accès à distance – Le service des TI et la direction doivent obliger tous les employés jouissant d'un accès à distance à signer un accord d'accès à distance qui décrit et souligne les règles, les responsabilités et les pratiques exemplaires en la matière.

Ajuster l'accès – Le service des TI doit permettre l'ajustement des droits d'accès à distance en cas de modification des responsabilités des employés de l'entreprise.

Attribuer des ordinateurs – Afin de renforcer la sécurité du télétravail, le responsable des TI doit faire en sorte que les employés reçoivent des ordinateurs professionnels qui ont été configurés et activés avec les logiciels et les mesures de protection choisies par l'entreprise pour améliorer la sécurité et le contrôle.

Étiqueter et consigner les renseignements relatifs aux appareils – Comme pour tous les autres appareils mobiles numériques, le service des TI doit marquer tous les ordinateurs attribués aux employés travaillant à distance d'un numéro de série qu'il consignera dans ses dossiers afin de faciliter le suivi de leur configuration ou leur récupération en cas de perte ou de vol.



Télétravail à domicile et en déplacement

Le mode d'accès à distance le plus couramment fourni par les détaillants est le télétravail à domicile et en déplacement. Il offre aux employés un moyen de communication simple et pratique avec leur employeur lorsqu'ils ne sont pas présents sur le lieu de travail. Toutefois, en utilisant un ordinateur personnel ou portable, l'employé expose l'entreprise à des risques supplémentaires.

Pour réduire ces risques, le responsable des TI doit prendre les mesures suivantes :

Restreindre l'accès sans fil – Le responsable des TI doit veiller à ce que tous les employés travaillant à domicile sur un ordinateur personnel connectent leur ordinateur directement à un routeur à l'aide d'un câble Ethernet, et connectent le câble Ethernet au modem, afin d'empêcher toute personne extérieure au réseau d'écouter ou d'intercepter les communications.

Sécuriser le réseau Wi-Fi – Le responsable des TI doit veiller à ce que les employés utilisent une connexion Wi-Fi sécurisée afin d'empêcher les cybercriminels d'accéder à des données professionnelles de nature délicate.

Modifier le nom du réseau par défaut – Le responsable des TI doit aider les employés travaillant à domicile ou en déplacement à modifier le nom du réseau Wi-Fi par défaut et le mot de passe d'accès au routeur du réseau pour améliorer la sécurité de la connexion.

Chiffrer le réseau – Le responsable des TI doit s'assurer d'activer le chiffrement du réseau pour empêcher les cybercriminels d'utiliser toute communication et toute donnée de nature délicate interceptée.

x. Appareils numériques

Parmi les outils les plus significatifs et les plus importants au sein de l'écosystème numérique de la vente au détail en pleine évolution, on trouve les différents appareils utilisés pour communiquer, transmettre des informations et collaborer au travail. Cependant, étant donné que chaque appareil représente une porte d'entrée dans un réseau ou un système, les cybercriminels les ciblent de plus en plus. C'est pourquoi il devient extrêmement important pour le responsable des TI de mettre en œuvre des mesures de protection et d'adopter des comportements permettant d'assurer la sécurité de ces appareils mobiles fréquemment utilisés.

Les tablettes, les téléphones intelligents et les appareils de stockage de données portables comptent parmi les appareils les plus couramment utilisés par les commerces de détail et leurs employés. La disparition d'un tel appareil peut avoir un certain nombre de conséquences négatives, allant des dommages et de la perte de données à l'exposition à des maliciels. Pire encore, les données de nature délicate et les outils de réseau sont susceptibles d'être détournés.

Afin d'éviter le pire, ou d'atténuer les répercussions de toute perte liée à des appareils volés ou endommagés, le responsable des TI peut prendre les mesures suivantes :

Consignation des numéros de série – Il est judicieux de consigner le numéro de série de tous les appareils mobiles et dispositifs de stockage portables utilisés par les employés de l'organisation au cas où ils viendraient à les perdre ou à se les faire voler.

Sauvegarde régulière – Le responsable des TI doit régulièrement effectuer une sauvegarde du contenu des appareils des employés.

Utilisation d'applications de sécurité – Le responsable des TI doit s'assurer que toutes les applications de sécurité appropriées sont installées, notamment pour ce qui est du chiffrement, des localisateurs d'appareils perdus et des logiciels antimaliciels.

Utilisation des mesures de protection existantes – La plupart des appareils mobiles sont aujourd'hui équipés de fonctions de sécurité, notamment de logiciels antimaliciels, qui doivent être activées sur chaque appareil fourni par l'entreprise.

Chiffrement – Tous les dispositifs de stockage de données portables doivent être chiffrés pour garantir la protection des données qui y sont renfermées.

Étiquetage des appareils – Il est judicieux d'indiquer le nom et les coordonnées de l'entreprise sur tous les appareils portables.

xi. Gestion des interventions en cas d'attaque

En plus du plan complet de cybersécurité, le responsable des TI doit veiller à l'élaboration d'un plan d'intervention contenant les politiques, les procédures et les pratiques exemplaires à suivre en cas de cyberattaque.

Élaboration d'un plan

En conjonction avec le plan global de cybersécurité, les plans d'intervention en cas d'attaque permettent aux détaillants de se préparer aux cyberattaques, de les détecter et de les contrer rapidement. Ils sont essentiels à la protection de l'écosystème numérique et de l'ensemble des activités de tout détaillant, et jouent un rôle clé dans la définition des étapes à suivre, des mesures à prendre et des responsabilités des employés chargés de les appliquer.

Fondamentalement, un solide plan d'intervention en cas d'attaque doit traiter des points suivants :

Mesures de protection et de détection – Définition claire des mesures de protection et de détection que l'organisation a actuellement en place.

Politiques et procédures – Liste claire et complète des règles, des politiques et des procédures d'intervention que les employés de l'organisation doivent respecter en cas d'attaque.

Ressources et aide – Liste de toutes les ressources et de l'aide mises à disposition des employés, selon la nature de l'incident.

Rôles et responsabilités – Définition claire des rôles et des responsabilités des personnes de l'organisation répondant aux attaques.

Signalement des attaques – Directives indiquant à quel moment et de quelle manière les employés doivent signaler une cyberattaque qui, selon eux, compromet l'organisation de quelque façon que ce soit.

Processus d'intervention – Liste exhaustive des types de cyberattaques et d'incidents, et des mesures à prendre pour y remédier.

Mécanismes de communication – Processus détaillé en vertu duquel les collègues et partenaires internes ainsi que les intervenants externes doivent être informés d'une cyberattaque.

Processus postérieur à l'attaque – Définition claire des directives de reprise après l'attaque, ainsi que des mesures à prendre pour bien cerner la cause de l'incident, les façons dont il aurait pu être évité et les moyens d'atténuation de son incidence.

Tests d'intrusion

Les tests d'intrusion réguliers contribuent grandement à l'actualisation et au maintien de la fiabilité de tout programme de cybersécurité, et font partie intégrante du plan d'intervention en cas d'attaque d'une organisation de vente au détail. Destinés à évaluer l'efficacité et la résilience des actifs, des appareils, du réseau et des systèmes de l'entreprise, ces tests permettent justement de détecter leurs points faibles en matière de protection et de défense en démontrant leurs vulnérabilités aux attaques.

En simulant une cyberattaque guidée par des objectifs simulés, les tests d'intrusion visent à atteindre les objectifs suivants :

Démasquer les technologies obsolètes – Il s'agit de démasquer les technologies obsolètes et vulnérables aux tactiques de plus en plus sophistiquées des cybercriminels pour aider le responsable des TI à maintenir la fiabilité du réseau et des systèmes de l'organisation.

Cerner l'ampleur potentielle des attaques – Il est essentiel de cerner la mesure dans laquelle une cyberattaque peut porter atteinte aux données de nature délicate de l'entreprise pour évaluer la rigueur de ses mesures de protection et de contrôle.

Repérer les données à risque – En plus de cerner l'ampleur potentielle des cyberattaques, il est important que le responsable des TI et la direction s'emploient à repérer les données les plus à risque et celles constituant la plus grande menace pour l'entreprise en cas d'atteinte aux systèmes.

Cerner les lacunes – Les travaux de détection des faiblesses et des lacunes des mesures de protection existantes de l'organisation permettent au responsable des TI de déterminer les mesures de protection nécessaires au renforcement de la sécurité.

Remarque : *Les tests d'intrusion doivent être effectués par un professionnel expérimenté qui connaît les risques inhérents à l'exécution de tels tests.*

Surveillance et défense du réseau

En plus de procéder régulièrement à l'exécution de tests d'intrusion, le responsable des TI devra constamment garder un œil sur le réseau et les systèmes de son organisation. Même si le plan de cybersécurité s'avère efficace et même si l'organisation est en mesure de réagir aux attaques le plus rapidement et le plus efficacement possible, il est essentiel d'assurer une surveillance diligente des menaces et des défenses associées à l'entreprise.

La surveillance rigoureuse et systématique du réseau et des systèmes organisationnels constitue à bien des égards la première et dernière ligne de défense de tout commerce de détail et peut procurer certains des avantages suivants :

Perception améliorée – Grâce à la surveillance systématique des menaces à la sécurité du réseau et des systèmes du détaillant (notamment les systèmes et les logiciels axés sur la technologie, ainsi que les interventions humaines), le responsable des TI se fait une idée claire de l'écosystème soutenant ses activités numériques, ce qui lui permet de mieux connaître les besoins et les capacités de l'entreprise en matière d'infrastructure.

Lutte contre la propagation des menaces – En surveillant les menaces, il est souvent possible de prévenir les cyberattaques, ou du moins de réussir à atténuer la plupart des dommages qu'elles peuvent causer.

Réalisation d'une veille stratégique – La surveillance du réseau et des systèmes de l'organisation donne également lieu à la production d'une quantité considérable de rapports d'activité et de mesures qui peuvent contribuer à améliorer les politiques de sécurité et soutenir la conformité réglementaire.

Adoption d'une approche proactive – En plus de prévenir les cyberattaques, la surveillance facilite l'adoption d'une approche proactive en matière de sécurité, en éclairant le choix des mesures de protection, des outils et des pratiques exemplaires à mettre en œuvre à l'avenir.

xii. Sensibilisation et formation à la cybersécurité

Afin de veiller à l'application du plan et de toutes les politiques et procédures connexes au sein de l'organisation, il est essentiel d'organiser des séances de sensibilisation et de formation sur l'importance de la cybersécurité. Par ailleurs, il est tout aussi important que le responsable des TI anime ces séances pour assurer un bon transfert de l'information et des connaissances.

Dans le cadre du programme de sensibilisation à la cybersécurité, le responsable des TI et la direction de l'organisation de vente au détail devront s'employer à proposer des ressources et des documents de formation et d'information consacrés aux cybermenaces et aux risques connexes, ainsi qu'au plan de cybersécurité de l'entreprise.

Tous les employés de l'organisation de vente au détail, tous échelons confondus, doivent participer au programme de sensibilisation à la cybersécurité. Les séances de formation et d'information doivent se faire en groupe pour permettre le renforcement de l'esprit d'équipe et de collaboration des employés et le renforcement approprié et efficace des politiques et des procédures normalisées.

Les activités de formation et de sensibilisation peuvent s'accompagner de jeux-questionnaires, de concours et de récompenses. Ces précieuses ressources permettront à la direction de relayer les principes de la sécurité et de la sûreté, et aux employés de les assimiler plus facilement.

De plus, toute ressource de formation ou de sensibilisation à la sécurité doit être régulièrement examinée et mise à jour afin d'en garantir la pertinence. Il est suggéré d'y inclure du contenu portant sur les éléments suivants :

- Piratage psychologique
- Hameçonnage
- Comportements à adopter sur les médias sociaux
- Habitudes de navigation en ligne
- Pratiques d'authentification
- Traitement des données
- Détection et signalement des attaques
- Appareils mobiles
- Télétravail

xiii. Assistance

Il n'est pas facile d'élaborer et de superviser un programme de cybersécurité complet qui permette de protéger efficacement une organisation contre la multitude de menaces posées par les cybercriminels. Cela est particulièrement vrai pour les petites et moyennes entreprises de vente au détail, qui ne possèdent peut-être pas l'expertise nécessaire pour le faire, ou les équipes nécessaires pour mettre en œuvre toutes les initiatives et s'assurer que le personnel respecte les pratiques exemplaires. Par conséquent, il est important de savoir quand et où demander de l'aide pour protéger l'entreprise.

Quand demander de l'aide?

Au vu de la multitude d'aspects à traiter, comme la sélection et la mise en œuvre d'un éventail de solutions de sécurité, le traitement et la gestion sûrs de montagnes de données, l'administration de séances de sensibilisation et de formation continue au personnel, en plus d'une multitude d'autres couches critiques, certaines personnes peuvent avoir du mal à gérer la mise en œuvre du plan de cybersécurité. Si le niveau de cybersécurité de votre organisation vous préoccupe et que vous ne croyez pas pouvoir répondre à tous les besoins connexes de l'entreprise, il est certainement temps de demander de l'aide à des fournisseurs de services tiers possédant les connaissances recherchées. Selon vos besoins en matière de cybersécurité, un certain nombre d'entreprises offrent une gamme de services, comme des conseils et un service à la clientèle, qui peuvent grandement profiter à votre organisation.

Protection de votre entreprise

Si votre organisation ne dispose pas des ressources nécessaires pour commencer à élaborer un programme de cybersécurité complet et efficace, ou si vous avez un budget serré, vous pouvez recourir à des outils gratuits offerts en ligne. Cependant, les détaillants devront faire preuve de prudence lors de la recherche de ces types d'outils, en confirmant notamment la légitimité des outils par la vérification de leurs sources et l'examen des avis des utilisateurs. Il est important de comprendre que l'élaboration d'un programme et d'une infrastructure de cybersécurité solides nécessite au moins un investissement initial, en plus des paiements associés aux services continus. Cela peut sembler onéreux pour certaines organisations. Toutefois, de nombreux fournisseurs de logiciels de cybersécurité offrent également un service à la clientèle, des garanties sur les produits, une assistance technique pour l'installation et la configuration des produits, ainsi que toutes les mises à jour qui peuvent être nécessaires en cours de route.

Quand communiquer avec les autorités?

Bien que les organisations aient de nombreux outils et une assistance technique à leur disposition, il leur est parfois nécessaire de communiquer avec les forces de l'ordre. En cas de cyberattaque grave, qui pourrait prendre la forme de menaces contre les employés ou de dommages aux actifs de l'entreprise, les détaillants doivent effectuer un signalement.

- ***Signalement d'une attaque aux forces de l'ordre***
- ***Signalez l'attaque au système de signalement des incidents de cybercriminalité et de fraude. Ce signalement sera automatiquement transmis à la Gendarmerie royale du Canada (GRC), au Centre national de coordination en cybercriminalité (CNC3) et au Centre antifraude du Canada (CAFC) afin de protéger directement l'organisation et de l'aider à se prémunir contre des menaces similaires.***

xiv. Autoévaluation de la cybersécurité

Cette autoévaluation de la cybersécurité vous aidera à améliorer vos efforts de cybersécurité. Le fait de passer en revue cette courte liste de questions et d'y répondre avant de lire ce guide dans son intégralité aidera les services des TI et leurs équipes à mieux connaître l'état de leurs capacités en matière de cybersécurité et, par conséquent, à repérer les parties ou le contenu du guide qui méritent d'être mis en évidence et sur lesquels il convient de se concentrer.

Avant de répondre, veuillez noter que ces questions ont été formulées en supposant que votre entreprise, quel que soit sa taille ou son format :

1. utilise des ordinateurs d'entreprise;
2. utilise des ordinateurs et des appareils de communication portables d'entreprise;
3. connecte au moins une partie de ces appareils à Internet au moins une partie du temps;
4. possède et utilise un intranet afin de diffuser en interne des logiciels d'applications, des documents et d'autres données, de nature délicate ou non.

Pour remplir correctement et avec précision l'autoévaluation, encerclez une réponse pour chaque question posée. Si vous ne connaissez pas la réponse à la question posée, encerclez « Je ne sais pas ».

Questions de l'autoévaluation de la cybersécurité

1. La cybersécurité est-elle actuellement une priorité au sein de votre organisation de vente au détail ?

0. Je ne sais pas 1. Non 2. Oui

2. Est-ce qu'un employé de votre organisation de vente au détail est responsable des activités, de la stratégie et du rendement associés à la cybersécurité ?

0. Je ne sais pas 1. Non 2. Oui

3. Si vous avez répondu « Oui », cette personne occupe-t-elle un poste permanent soutenu par la direction ? (Encerclez cette réponse si vous avez répondu « Oui » à cette question.)

3. Votre organisation de vente au détail a-t-elle déjà effectué une évaluation des risques ou une analyse des menaces, ou tout autre type d'examen semblable ?

0. Je ne sais pas 1. Non 2. Oui

3. Si vous avez répondu « Oui », les risques et les menaces connexes ont-ils été classés par ordre de priorité et surveillés dans le cadre des efforts visant à les limiter ou à les éliminer ? (Encerclez cette réponse si vous avez répondu « Oui » à cette question.)

4. Y a-t-il un plan ou une stratégie de cybersécurité en place au sein de votre organisation de vente au détail ?

0. Je ne sais pas 1. Non 2. Oui

3. Si vous avez répondu « Oui », les gestionnaires de l'organisation respectent-ils le plan ou la stratégie ? (Encerclez cette réponse si vous avez répondu « Oui » à cette question.)

5. Des politiques de cybersécurité sont-elles en place au sein de votre organisation de vente au détail ?

0. Je ne sais pas 1. Non 2. Oui

3. Si vous avez répondu « Oui », les politiques sont-elles appuyées par des séances de sensibilisation et de formation continue des employés ? (Encerclez cette réponse si vous avez répondu « Oui » à cette question.)

6. Y a-t-il un plan d'intervention d'urgence en place au sein de votre organisation de vente au détail ?

0. Je ne sais pas 1. Non 2. Oui

3. Si vous avez répondu « Oui », ce plan est-il tenu à jour et révisé régulièrement ? (Encerclez cette réponse si vous avez répondu « Oui » à cette question.)

7. Votre organisation de vente au détail offre-t-elle à ses employés des séances de sensibilisation et de formation sur le traitement et la désignation sécuritaires des renseignements personnels et/ou commerciaux de nature délicate?

0. Je ne sais pas 1. Non 2. Oui

3. Si vous avez répondu « Oui », ces séances de sensibilisation et de formation sont-elles les mêmes pour tous les employés et sont-elles appuyées par des politiques ? (Encerclez cette réponse si vous avez répondu « Oui » à cette question.)

8. Votre organisation de vente au détail offre-t-elle à ses employés des séances de sensibilisation et de formation sur l'utilisation sécuritaire des appareils mobiles ou des ordinateurs ?

0. Je ne sais pas 1. Non 2. Oui

3. Si vous avez répondu « Oui », cette formation est-elle appuyée par des outils de gestion des appareils mobiles ? (Encerclez cette réponse si vous avez répondu « Oui » à cette question.)

9. Votre organisation de vente au détail a-t-elle installé un pare-feu entre les ordinateurs d'entreprise (y compris les systèmes de point de vente) et Internet ?

0. Je ne suis pas sûr(e) 1. Non 2. Oui

3. Dans l'affirmative, la maintenance est-elle régulièrement effectuée par une personne disposant de la bonne expérience et de la bonne formation ? (Encerclez cette réponse si vous avez répondu « Oui » à cette question.)

10. Votre organisation de vente au détail utilise-t-elle un outil de chiffrement pour sécuriser ses communications numériques avant de les envoyer à l'extérieur de l'entreprise ?

0. Je ne suis pas sûr(e) 1. Non 2. Oui

3. Dans l'affirmative, les employés ont-ils reçu une formation sur l'utilisation de ces outils, et leur utilisation est-elle surveillée par le service des TI ? (Encerclez cette réponse si vous avez répondu « Oui » à cette question.)

11. Votre organisation de vente au détail utilise-t-elle des filtres antipourriel pour sécuriser ses boîtes de réception ?

0. Je ne suis pas sûr(e) 1. Non 2. Oui

3. Si oui, les employés ont-ils reçu une formation sur le signalement des pourriels et des attaques par hameçonnage ? (Encerclez cette réponse si vous avez répondu « Oui » à cette question.)

12. Votre organisation de vente au détail utilise-t-elle des logiciels antimaliciel ?

0. Je ne suis pas sûr(e) 1. Non 2. Oui

3. Si oui, est-ce que tous les ordinateurs de l'organisation en sont équipés, et sont-ils mis à jour régulièrement ? (Encerclez cette réponse si vous avez répondu « Oui » à cette question.)

13. Votre organisation de vente au détail encourage-t-elle l'utilisation de mots de passe et de phrases de passe complexes ?

0. Je ne suis pas sûr(e) 1. Non 2. Oui

3. Si oui, les règles et politiques relatives aux mots de passe sont-elles appliquées ? (Encerclez cette réponse si vous avez répondu « Oui » à cette question.)

14. Votre organisation de vente au détail sauvegarde-t-elle régulièrement les données et les applications utilisées au sein de l'entreprise ?

0. Je ne suis pas sûr(e) 1. Non 2. Oui

3. Si oui, les sauvegardes sont-elles régulièrement testées et conservées hors site dans l'éventualité d'un dommage ? (Encerclez cette réponse si vous avez répondu « Oui » à cette question.)

15. Votre organisation de vente au détail a-t-elle des politiques en place sur le télétravail sécuritaire ?

0. Je ne suis pas sûr(e) 1. Non 2. Oui

3. Si oui, l'organisation a-t-elle recours à un réseau privé virtuel (VPN) dans le cadre du télétravail ? (Encerclez cette réponse si vous avez répondu « Oui » à cette question.)

Quelle note avez-vous obtenue?

Une fois que vous avez rempli le questionnaire, additionnez tous les chiffres situés à gauche des réponses encerclées (0, 1, 2 et 3). Votre note totale vous aidera à évaluer le niveau de cybersécurité au sein de votre organisation et le travail qui pourrait devoir être fait pour améliorer la sécurité de votre entreprise.

Note comprise entre 0 et 15 : Si vous avez obtenu une note dans cette fourchette, nous vous conseillons de bien lire ce guide afin de mieux saisir l'importance d'un plan de cybersécurité solide et complet pour votre organisation. Une fois que vous aurez lu le guide et formulé vos propres recommandations, rencontrez vos collègues et vos supérieurs pour commencer à élaborer et à mettre en œuvre une stratégie de cybersécurité et des outils et procédures connexes.

Note comprise entre 16 et 30 : Si vous vous situez dans cette fourchette, on peut penser que votre organisation a connaissance des risques associés à la cybercriminalité, mais qu'il y a encore du travail et de la recherche à faire. Compte tenu de ce qui précède, il vous est conseillé de lire attentivement l'ensemble de ce guide, en prenant note des domaines dans lesquels des améliorations peuvent être apportées au plan et à la stratégie de votre organisation.

Note supérieure à 30 : Si vous vous situez dans cette fourchette, félicitations! Votre organisation semble arriver à maintenir un environnement numérique sécuritaire pour sa marque de détail, ses employés et ses clients. Cependant, compte tenu de la vitesse à laquelle le paysage numérique de la vente au détail évolue, il est toujours bon de continuer à examiner les pratiques exemplaires pour rester au courant des dernières avancées en matière de cybersécurité.

xv. Ressources pour les détaillants

Pour aider les entreprises de vente au détail à mieux se protéger contre la cybercriminalité, voici une liste de ressources en cas de besoin :

Programme Cybersécurité au détail du CCCD :
https://www.commercedetail.org/programme-cybersecurite-au-detail-du-cccd/

Centre canadien pour la cybersécurité :
https://www.cyber.gc.ca/fr

Centre canadien pour la cybersécurité – Alertes et avis :
https://www.cyber.gc.ca/fr/alertes-avis

Centre antifraude du Canada :
https://antifraudcentre-centreantifraude.ca/protect-protegez-fra.htm

Gouvernement du Canada – Cybersécurité :
https://www.canada.ca/fr/services/defense/cybersecurite.html