Renforcer la Cybersécurité des PME au Québec : Guide Pratique

Table des matières

Introduction

La numérisation croissante des activités commerciales des petites et moyennes entreprises (PME) au Québec a ouvert de nouvelles opportunités, mais elle a également accru leur exposition aux menaces cybernétiques. Les cyberattaques, telles que les rançongiciels, les piratages de données et les attaques par hameçonnage, représentent désormais une menace constante pour la sécurité des données sensibles des PME. Ces attaques peuvent avoir des conséquences dévastatrices, allant de la perte de données à la perturbation des opérations commerciales et à la perte de confiance des clients.

> ***La cybercriminalité au Canada[1]***
> *En 2020, 78 % des entreprises canadiennes ont été victimes d'une attaque réussie.*
>
> *Au cours de la première moitié de 2023, le Canada a été la cible de plus de 17,8 milliards de tentatives de cyberattaques.*

Depuis juin 2018, le gouvernement du Canada a mis en place un centre consolidé des opérations de cybersécurité, soit le Centre canadien pour la cybersécurité. Les technologies numériques et l'Internet jouent un rôle de plus en plus important dans l'innovation et la croissance économique, et il est essentiel d'adopter des mesures de cybersécurité rigoureuses pour assurer la capacité concurrentielle, la stabilité économique et la prospérité à long terme du Canada. Dans ce contexte, le Centre canadien pour la cybersécurité propose le guide Pensez cybersécurité pour les petites entreprises. des conseils pratiques pour protéger les petites entreprises contre la cybercriminalité.
référence : https://www.pensezcybersecurite.gc.ca/fr/ressources/guide-pensez-cybersecurite-petites-entreprises

[1] https://www.comparitech.com/fr/blog/securite-information/statistiques-cybercriminalite-au-canada/#:~:text=Le%20rapport%20CyberEdge%2C%20qui%20se,Mexique%20(72%2C7%20%25).

Face à ces défis, la cybersécurité est devenue une priorité absolue pour les dirigeants de PME. Protéger les données sensibles, garantir la confidentialité des informations clients et maintenir la continuité des activités sont autant d'objectifs essentiels pour assurer la pérennité et la croissance des PME. Cependant, de nombreuses PME peuvent se sentir dépassées par la complexité de la cybersécurité et avoir du mal à mettre en œuvre des mesures efficaces pour se protéger contre les menaces en ligne.

C'est dans ce contexte que ce guide intervient. En fournissant des conseils pratiques et des solutions spécifiquement adaptées aux besoins des PME, il vise à aider les dirigeants à renforcer leur posture en matière de cybersécurité. Des stratégies de protection des données aux technologies de sécurité informatique, en passant par la sensibilisation des employés et la conformité aux réglementations en vigueur, il couvre un large éventail de sujets essentiels pour aider les PME à se prémunir contre les cybermenaces.

En fin de compte, en investissant dans la cybersécurité et en adoptant une approche proactive pour protéger leurs activités en ligne, les PME peuvent non seulement prévenir les attaques potentielles, mais aussi renforcer la confiance de leurs clients et assurer leur croissance à long terme dans un environnement numérique en constante évolution.

Chapitre 1 : Les menaces actuelles

Dans ce chapitre dédié aux menaces actuelles, nous plongeons au cœur des défis rencontrés par les PME en matière de cybersécurité.

Parmi les menaces les plus courantes, nous identifions les attaques d’hameçonnage, un stratagème sophistiqué où les cybercriminels se font passer pour des entités légitimes afin d'induire les utilisateurs à divulguer des informations confidentielles telles que des identifiants de connexion ou des données bancaires.

Les rançongiciels, une autre menace redoutable, sont des logiciels malveillants conçus pour chiffrer les fichiers des entreprises et exiger une rançon en échange de leur déchiffrement. Ces attaques peuvent paralyser les activités commerciales et entraîner des pertes financières importantes.

> *Les courriels d'hameçonnage, le manque de formation et les mots de passe faibles sont quelques-unes des principales causes des attaques de rançongiciels.*

Les logiciels malveillants, incluant virus, vers et chevaux de Troie, représentent également une menace constante pour les PME. Ces programmes nocifs peuvent infecter les systèmes informatiques et causer des dommages allant de la perte de données à la prise de contrôle de l'ordinateur.

- *Les attaques de cryptojacking ont fait leur retour en 2023 après avoir connu d'énormes baisses au cours du second semestre 2019. Au total, il y a eu une augmentation d'environ 40 millions par an. (Rapport 2023 sur les cybermenaces SonicWall)*
- *Les cybercriminels diffusent désormais des logiciels malveillants qui infectent les ordinateurs des victimes et utilisent illégalement leur puissance de traitement pour exploiter des cryptomonnaies, telles que Bitcoin ou Monero.*
- *Si l'un de vos sites web favoris est infecté, votre ordinateur risque également de l'être lorsque vous le visitez.*

Enfin, les attaques par déni de service distribué (DDoS) sont une forme d'attaque où les serveurs sont submergés par un trafic web excessif, les rendant indisponibles pour les utilisateurs légitimes. Ces attaques peuvent entraîner une interruption totale des services en ligne et nuire à la réputation de l'entreprise.

> *Au troisième trimestre 2022, le nombre d'attaques DDoS a été **multiplié par plus de 4,5** par rapport à la même période en 2021. (Kaspersky Labs)*

De plus, dès que l'on se connecte à Internet, des tentatives de validation d'IP et des scans pour détecter les ports ouverts (port sniffer) sont effectués. Cela signifie que la menace est toujours présente, même si elle n'est pas immédiatement visible.

En comprenant les motivations des cybercriminels, qui peuvent inclure le vol d'argent, l'espionnage industriel ou simplement le désir de perturber les opérations commerciales, les PME peuvent mieux se préparer à faire face à ces menaces. De plus, en prenant conscience des conséquences potentielles des cyberattaques, telles que la perte de données, les dommages à la réputation et les pertes financières, les dirigeants sont incités à investir dans des mesures de sécurité appropriées pour protéger leur entreprise.

Chapitre 2 : Évaluation des Risques

Dans ce chapitre dédié à l'évaluation des risques, nous plongeons dans l'importance cruciale de comprendre les menaces potentielles auxquelles les PME sont exposées. Une évaluation approfondie des risques de sécurité informatique est essentielle pour identifier les vulnérabilités et les faiblesses de l'infrastructure informatique de l'entreprise, permettant ainsi de prendre des mesures proactives pour les atténuer.

Cette évaluation est une étape fondamentale dans la protection des données sensibles et des activités commerciales. Identifier les menaces potentielles, les actifs critiques et les points de vulnérabilité est essentiel pour élaborer une stratégie de cybersécurité efficace.

Une approche holistique est recommandée, qui examine tous les aspects de l'infrastructure informatique, y compris les réseaux, les applications, les données et les utilisateurs. Il est important d'impliquer toutes les parties prenantes, y compris les dirigeants, les responsables informatiques et les employés, dans ce processus d'évaluation.

Les mesures de sécurité peuvent alors être hiérarchisées en fonction de leur impact potentiel sur l'entreprise. Toutes les menaces ne sont pas égales, et il est essentiel de concentrer les ressources là où elles seront le plus efficaces. Il est important de tenir compte à la fois de la probabilité et de l'impact des risques potentiels lors de la priorisation des mesures de sécurité.

En fin de compte, une évaluation rigoureuse des risques de sécurité informatique permet aux PME de mieux comprendre les défis auxquels elles sont confrontées et de prendre des mesures concrètes pour renforcer leur posture en matière de cybersécurité.

Chapitre 3 : Stratégies de Cybersécurité

Dans ce chapitre consacré aux stratégies de cybersécurité, nous explorons des mesures concrètes pour renforcer la résilience des PME face aux menaces cybernétiques croissantes. Nous fournissons des conseils pratiques sur divers aspects de la sécurité informatique, visant à protéger les données sensibles, à prévenir les cyberattaques et à promouvoir une culture de sécurité au sein de l'entreprise.

Selon une étude réalisée en 2012, 83 % des PME ne disposent pas d'un plan de cybersécurité.[2]

L'essence même d'une stratégie de cybersécurité réussie réside dans une compréhension approfondie de votre infrastructure informatique. Après tout, comment pouvons-nous protéger ce que nous ne connaissons pas ? Cette phase initiale revêt une importance capitale pour élaborer une stratégie de sécurité informatique adéquate.

Cet inventaire implique non seulement de répertorier les équipements informatiques tels que les ordinateurs, les serveurs, les imprimantes, les clés USB, et autres, mais aussi de dresser la liste des logiciels utilisés, incluant leurs versions et licences associées.

Cette démarche vous permettra d'avoir une vision précise de ce qui doit être protégé, tout en identifiant les éléments critiques pour le bon déroulement de vos activités. En somme, un inventaire exhaustif constitue le socle sur lequel s'appuie toute stratégie de sécurité informatique efficace.

Protection des données

La protection des données est d'une importance cruciale. Cela inclut la mise en place de politiques de confidentialité robustes, le chiffrement des données sensibles et la sauvegarde régulière des informations critiques. En cas de cyberattaque, de panne matérielle ou d'erreur humaine, les sauvegardes régulières deviennent votre bouée de sauvetage numérique. Elles représentent le rempart ultime contre la perte totale ou partielle de précieuses informations.

[2]https://www.pensezcybersecurite.gc.ca/fr/ressources/guide-pensez-cybersecurite-pour-les-petites-et-moyennes-entreprises#s1

Une stratégie de sauvegarde bien pensée est bien plus qu'une simple précaution ; elle assure la pérennité de vos opérations même face aux pires scénarios.

Lors de la mise en place de cette stratégie, la première étape consiste à identifier avec précision les données cruciales à sauvegarder. Il s'agit non seulement des données opérationnelles, mais également des configurations système et des logiciels essentiels qui sont le moteur de votre activité. Cette démarche minutieuse garantit que chaque aspect vital de votre entreprise est protégé.

Une fois ces éléments identifiés, il est impératif de déterminer la fréquence de sauvegarde appropriée. Cette décision dépendra de la nature de vos données et de la cadence de leur création ou modification. Une fréquence de sauvegarde plus élevée peut être nécessaire pour les données en constante évolution, assurant ainsi une protection en temps quasi réel.

Enfin, la conformité aux lois et réglementations en matière de protection des données, telles que la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) au Canada est incontournable. La loi 25 au Québec stipule que votre entreprise est responsable de protéger les renseignements personnels qu'il recueille, détient, utilise, communique et conserve. Il en est donc imputable. Il doit mettre en place des structures et des règles et adopter des pratiques pour les protéger de manière adéquate. Se conformer à ces normes non seulement garantit la protection des données des clients, mais peut également aider à éviter des amendes importantes en cas de violation de la sécurité des données.

De plus, il est primordial de limiter l'accès aux données sensibles uniquement aux employés autorisés, ainsi que de surveiller et d'auditer régulièrement les accès aux données.

Gestion des accès

La gestion des mots de passe est un élément essentiel de la sécurité informatique. Les PME sont encouragées à mettre en œuvre des politiques de mots de passe solides, à promouvoir l'utilisation de mots de passe complexes et uniques pour chaque compte, et à envisager l'utilisation de solutions de gestion des mots de passe pour renforcer la sécurité. Une gestion efficace des mots de passe est cruciale pour la sécurité des systèmes d'information de toute entreprise.

Voici quelques bonnes pratiques :

- **Complexité et longueur** : Optez pour des mots de passe longs et variés pour éviter les prévisibilités.
- **Unicité** : Chaque compte doit avoir un mot de passe unique
- **Renouvellement régulier** : Encouragez le changement périodique des mots de passe, surtout pour les comptes critiques.

En complément des mots de passe solides, l'authentification multi facteurs (MFA) offre une sécurité supplémentaire en exigeant plusieurs preuves d'identité pour accéder à un compte.

Sécurisation du réseau

La sécurisation des réseaux passe par la mise en place des pares-feux, des systèmes de détection d'intrusion et des protocoles de sécurité Wi-Fi robustes pour protéger les infrastructures réseau contre les cyberattaques. En tant que composant crucial de la sécurité des réseaux, le pare-feu agit comme un gardien, contrôlant le trafic entrant et sortant selon des règles de sécurité définies, et bloquant ainsi les accès non autorisés ou malveillants.

Parallèlement, la sensibilisation des employés en matière de cybersécurité est primordiale. Former les employés aux bonnes pratiques en matière de sécurité informatique, telles que l'identification des courriels d'hameçonnage et la protection des informations confidentielles, est crucial pour réduire les risques liés aux erreurs humaines.

En combinant ces stratégies et en adoptant une approche proactive en matière de cybersécurité, les PME peuvent renforcer leur posture de sécurité, protéger leurs données sensibles et assurer la confiance de leurs clients.

Budget de cybersécurité

Un plan de cybersécurité efficace coûte de l'argent et il faut en tenir compte lorsque vous établissez vos budgets annuels. Heureusement, il est possible d'obtenir des services, des outils et des conseils gratuits. Mais certains éléments clés, comme des mesures de protection, devront être achetés et pourront aussi comporter des frais d'abonnement annuel.

Afin d'éviter les surprises, mieux vaut prévoir :

- Le coût de départ des outils de sécurité ainsi que les frais de mise à niveau et de mise à jour;
- Les frais rattachés au soutien, aux conseils ou à la formation.

Chapitre 4 : Solutions Technologiques

Dans ce chapitre dédié aux solutions technologiques, nous explorons les différentes options disponibles pour renforcer la cybersécurité des PME. Une gamme d'outils et de technologies sont conçus pour protéger les infrastructures informatiques, détecter les menaces et garantir la résilience des entreprises face aux cyberattaques.

> Microsoft propose diverses solutions et services en matière de cybersécurité pour aider les organisations à se protéger contre les menaces en ligne. Microsoft continue également de développer et d'améliorer ses solutions de sécurité grâce à l'intelligence artificielle et à l'apprentissage automatique, permettant une détection plus rapide et plus précise des menaces, ainsi qu'une réponse plus efficace.

Les logiciels de sécurité, qui constituent la première ligne de défense contre les menaces cybernétiques. Ces logiciels incluent les antivirus, les anti-malwares et les anti-logiciels espions, qui sont essentiels pour détecter et neutraliser les programmes malveillants susceptibles de compromettre la sécurité des systèmes.

Ces logiciels spécialisés ne se contentent pas de détecter les virus ; ils surveillent également en permanence les activités suspectes, analysent les fichiers et les applications en temps réel, et fournissent une protection proactive contre les nouvelles menaces émergentes qui peuvent surgir à tout moment.

Pour assurer une protection optimale, il est crucial de choisir un antivirus qui réponde spécifiquement aux besoins de votre entreprise. Optez pour un logiciel doté d'un taux de détection élevé, de mises à jour fréquentes pour rester en phase avec les dernières menaces.

De plus, recherchez des fonctionnalités complémentaires telles que le pare-feu et la protection contre l'hameçonnage pour renforcer encore davantage votre sécurité.

Une fois que l'antivirus est installé, il est impératif de le maintenir régulièrement à jour afin de garantir son efficacité maximale. En investissant dans une protection antivirus robuste et en restant vigilants, vous protégez efficacement votre entreprise des menaces numériques qui guettent.

Les pare-feux sont des dispositifs de sécurité qui surveillent et contrôlent le trafic entrant et sortant des réseaux informatiques. Les pare-feux aident à bloquer les attaques externes et à prévenir les fuites de données en limitant l'accès non autorisé aux réseaux et aux systèmes.

Les outils de détection des menaces, tels que les systèmes de détection d'intrusion (IDS) et les systèmes de prévention des intrusions (IPS), surveillent en permanence les réseaux et les systèmes à la recherche d'activités suspectes ou de comportements anormaux pouvant indiquer une cyberattaque en cours.

La sauvegarde et la récupération des données, il est primordial de disposer de solutions robustes pour protéger les informations critiques contre la perte ou la corruption. Les solutions de sauvegarde automatique et de récupération des données permettent aux entreprises de restaurer rapidement leurs systèmes en cas de sinistre ou de cyberattaque, minimisant ainsi les temps d'arrêt et les pertes de données.

- Effectuez fréquemment une sauvegarde de vos données vers un disque dur externe, un serveur ou un service en ligne – il est essentiel d'avoir plusieurs copies de sauvegarde en cas de défaillance de l'une d'elles;
- Téléchargez ou achetez des logiciels de sauvegarde automatique pour assurer la sauvegarde de vos systèmes en temps opportun;
- Conservez des copies de sauvegarde physiques (p. ex. disque dur externe) dans un endroit sécuritaire à l'extérieur des installations de l'entreprise;
- Faire un test de restauration périodiquement, soit aux 4 mois à partir d'un autre poste;

Les services de gestion de la sécurité informatique offrent aux entreprises une expertise spécialisée pour surveiller, gérer et répondre aux menaces de manière proactive. Ces services comprennent la surveillance continue des réseaux, l'analyse des journaux d'activité, la gestion des incidents de sécurité et la formation des employés en matière de cybersécurité.

En conclusion, l'utilisation judicieuse de solutions technologiques adaptées peut aider les PME à renforcer leur posture de sécurité informatique et à se protéger contre les menaces cybernétiques. En combinant ces outils avec des pratiques de sécurité solides, les entreprises peuvent réduire leur exposition aux risques.

Chapitre 5 : Éducation et Sensibilisation

Dans ce chapitre crucial consacré à l'éducation et à la sensibilisation, nous mettons en lumière l'importance vitale de former et de sensibiliser les employés aux enjeux de la cybersécurité. Des programmes de formation complets conçus pour armer les employés avec les connaissances et les compétences nécessaires pour reconnaître, prévenir et répondre aux menaces cybernétiques, sont nécessaires.

Cette formation passe par la sensibilisation des employés aux diverses formes de menaces cybernétiques, telles que l'hameçonnage, les attaques de rançongiciel, les logiciels malveillants et les fraudes en ligne. Il est important d'outiller les employés pour leur permettre d'identifier ces menaces potentielles et de prendre des mesures préventives pour les contrer.

- Accordez à vos employés uniquement l'accès dont ils ont besoin;
- Demandez à vos employés de verrouiller leur ordinateur et de ranger leurs documents de nature délicate avant de quitter leur poste;

Les comportements des employés doivent être sécures, tels que l'utilisation de mots de passe forts, la vérification des sources avant de cliquer sur des liens, et la protection des informations sensibles. La prudence et la vigilance dans toutes les interactions en ligne, que ce soit par courriel, sur les réseaux sociaux ou lors de la navigation sur le web, font partie des défenses de l'entreprise.

> *Les pourriels représentent environ 69 % de tous les courriels transmis dans Internet.*
> *Non seulement les pourriels contiennent-ils des liens qui peuvent faire du tort à votre entreprise si vous cliquez dessus, mais ils peuvent aussi ralentir vos réseaux, vos serveurs et vos ordinateurs, ainsi qu'accroître les coûts et réduire la productivité.*[3]

[3]https://www.pensezcybersecurite.gc.ca/fr/ressources/guide-pensez-cybersecurite-pour-les-petites-et-moyennes-entreprises#s1

Les employés doivent signaler tout incident de sécurité ou toute activité suspecte à l'équipe informatique de l'entreprise. La transparence et la collaboration pour détecter, enquêter et répondre rapidement aux incidents de sécurité sont cruciaux afin de minimiser leur impact sur l'entreprise.

Nous recommandons la participation à des séminaires, à des webinaires et à des programmes de formation continue sur les dernières tendances et les meilleures pratiques en matière de cybersécurité pour maintenir ses connaissances à jour et développer une culture de sécurité forte au sein de l'entreprise.

Enfin, les employés doivent être encouragés à partager leurs expériences, leurs préoccupations et leurs idées pour renforcer la posture de sécurité globale de l'entreprise et protéger ses actifs numériques.

En combinant l'éducation, la sensibilisation et la collaboration, les PME peuvent renforcer leur défense contre les menaces cybernétiques et créer une culture de sécurité proactive qui protège efficacement leurs activités.

Conclusion

En conclusion, il est impératif de renforcer la cybersécurité des PME au Québec afin de garantir la protection des données, d'assurer la pérennité des activités et de préserver la confiance des clients. Grâce aux bonnes stratégies, aux technologies adéquates et aux programmes de sensibilisation efficaces, les PME peuvent considérablement réduire les risques d'attaques cybernétiques et se prémunir contre les menaces en ligne.

Ce guide s'efforce de fournir aux dirigeants de PME les outils et les connaissances nécessaires pour renforcer leur posture en matière de cybersécurité et protéger efficacement leur entreprise. En adoptant une approche proactive et en intégrant les principes de la cybersécurité dans toutes les facettes de leurs opérations, les PME peuvent mieux se

préparer à faire face aux défis numériques actuels et à assurer la sécurité de leurs activités dans un environnement en constante évolution.

Ressources supplémentaires en cybersécurité

Centre canadien pour la cybersécurité
Guide Pensez cybersécurité pour les petites et moyennes entreprises
La cybersécurité pour les TPE/PME en 13 questions
Cybersécurité | Loi 25 : les PME se surestiment | La Presse