La trousse élan

Conseils d'experts pour favoriser l'accompagnement

Présenté par

ADRIQ

PROMOUVOIR • MOBILISER • ACCOMPAGNER

Avec la participation financière de

Québec

Rédigé par

EFICIO

Pierre Farley, Expert-conseil en innovation, ADRIQ &
Associé & CIO sur demande, Eficio

Propulsé par

Réseau accès pme

Éléments de base en cybersécurité

1. À QUI S'ADRESSE CE GUIDE

Ce guide est principalement destiné aux conseillers en développement économique qui interviennent auprès de dirigeants de petites entreprises. L'objectif est de renforcer le niveau de connaissance des conseillers sur les éléments fondamentaux de la cybersécurité et de leur permettre d'évaluer le niveau de maturité général en matière de cybersécurité des entreprises qu'ils accompagnent.

1.1 Objectifs du guide

- **Augmenter les connaissances en cybersécurité :** Fournir aux conseillers les informations nécessaires pour comprendre les aspects cruciaux de la cybersécurité, permettant ainsi d'identifier où se situe une entreprise sur l'échelle de maturité de la cybersécurité.
- **Développer des intervenants de première ligne :** Fournir des outils aux conseillers afin de sensibiliser les dirigeants à l'importance de la sécurité de l'information sans pour autant les transformer en experts de la cybersécurité.

Il est important de noter que les éléments de base présentés dans ce guide constituent le minimum requis pour les petites entreprises afin d'instaurer une culture de la sécurité informatique. Toutefois, ces fondamentaux ne doivent pas être vus comme limitatifs. Un programme de cybersécurité complet pour une petite entreprise peut nécessiter des mesures supplémentaires et plus détaillées, adaptées aux spécificités de chaque organisation, à son industrie, et aux réglementations en vigueur.

Ce guide vise donc à établir une base sur laquelle les entreprises peuvent construire et élargir leur approche de la cybersécurité selon leurs besoins et capacités spécifiques.

2. INTRODUCTION

Bienvenue dans ce guide essentiel sur la cybersécurité, destiné à équiper les dirigeants d'entreprise avec les connaissances nécessaires pour identifier et gérer les risques de cybersécurité. Ce guide est conçu pour vous offrir une compréhension complète des menaces courantes, des meilleures pratiques de prévention, et des stratégies de réponse adaptées, le tout présenté de manière accessible sans prérequis technique approfondi.

2.1 Le contexte de la cybersécurité dans les petites entreprises

Les petites et moyennes entreprises (PME) sont essentielles à l'économie, mais elles représentent également des cibles attrayantes pour les cybercriminels en raison de leurs ressources souvent limitées en matière de cybersécurité. Confrontées à des défis uniques, ces organisations doivent jongler entre la nécessité de protéger des données sensibles et le manque de fonds et de personnel spécialisé pour mettre en place des systèmes de sécurité complexes basés sur des normes telles que ISO27001 ou NIST.

2.2 Importance de la sensibilisation et des pratiques exemplaires

Les PME sont fréquemment ciblées par des attaques visant à obtenir des informations sur leurs clients, partenaires, et fournisseurs, des données financières, des renseignements sur leurs systèmes de paiement, et des informations exclusives. En dépit de ces menaces, les PME peuvent réaliser des avancées significatives en matière de sécurité par la sensibilisation et l'adoption de pratiques de sécurité exemplaires. Une application judicieuse de la règle des 80/20 peut permettre d'atteindre environ 80 % des bienfaits en cybersécurité avec seulement 20 % des efforts typiquement requis.

2.3 Adaptation à l'environnement spécifique de l'entreprise

L'adaptation des stratégies de cybersécurité doit tenir compte de plusieurs facteurs clés pour être efficace :

- **Type de données sensibles en possession :** La nature des données traitées détermine les niveaux de sécurité nécessaires. Les données financières, personnelles ou relatives à la propriété intellectuelle nécessitent des mesures de sécurité accrues.
- **Industrie d'opération :** Les normes de sécurité varient considérablement selon les secteurs, certains étant soumis à des réglementations plus strictes que d'autres.
- **Exigences législatives régionales :** Les lois locales peuvent imposer des directives spécifiques sur la manière de gérer et protéger les données (loi 25 au Québec par exemple).
- **Obligations contractuelles :** Les accords avec des tiers peuvent également stipuler des exigences de sécurité spécifiques qui doivent être respectées pour maintenir la confiance et les opérations commerciales.

2.4 Mise en œuvre des contrôles de base

Il est recommandé aux PME de mettre en place des contrôles de cybersécurité de base, conçus pour être accessibles et réalisables avec des ressources limitées. En adoptant ces mesures, les PME peuvent significativement améliorer leur résilience face aux cybermenaces, tout en protégeant leurs actifs les plus critiques.

De nombreuses ressources sont disponibles en ligne[1] pour guider les PME dans l'élaboration et l'implémentation de leurs stratégies de cybersécurité. Il est aussi conseillé de ne pas hésiter à se faire accompagner par des professionnels de la sécurité pour une mise en œuvre adaptée et efficace des pratiques de sécurité.

[1] Voir en annexe.

3. INSTRUCTION D’UTILISATION

Ce guide de cybersécurité a été créé aider les conseillers en développement économique dans l’accompagnement de petites et moyennes entreprises. Il est conçu pour être utilisé conjointement avec une liste de contrôle détaillée. Cette liste se compose de questions stratégiquement élaborées pour sensibiliser les dirigeants aux enjeux de la cybersécurité et évaluer si les éléments essentiels de sécurité sont en place ou ont été planifiés.

Utilisation du guide et de la liste

1. Lecture du guide : Commencez par lire attentivement ce guide pour comprendre les principes de base de la cybersécurité, les risques spécifiques auxquels l’entreprise que vous accompagnée pourrait être exposée, et les meilleures pratiques pour y faire face.

2. Répondre à la liste de contrôle : Passez ensuite à la liste de contrôle avec l’entreprise. Chaque question doit être abordée avec soin. Notez les réponses et réfléchissez à la manière dont elles reflètent l'état actuel de la cybersécurité au sein de l’organisation accompagnée.

3. Analyse des réponses : Examinez les réponses où vous avez identifié des faiblesses ou des absences de mesures de sécurité. Ce sera un indicatif clair des domaines nécessitant une attention immédiate.

4. Planification des actions : Sur la base de cette analyse, élaborez un plan d'actions pour aborder les points faibles. Priorisez les mesures qui peuvent être mises en œuvre rapidement et qui ont un impact significatif sur la sécurité globale.

Résultats attendus

L'utilisation de ce guide et de la liste de contrôle devrait vous aider à dresser le portrait de l’entrperise et conduire à une prise de conscience accrue parmi les dirigeants. Le niveau de réponse aux questions de la liste peut servir de signal d'alarme si les scores sont particulièrement bas, indiquant un besoin urgent d'amélioration. Le but final est de s'assurer que les éléments de base de la cybersécurité ne sont pas seulement envisagés, mais effectivement intégrés dans la stratégie de sécurité de l'entreprise.

Suivi et amélioration continue

La cybersécurité n'est pas un exercice ponctuel mais un processus continu. Il est recommandé de réviser régulièrement le guide et de répondre à nouveau à la liste de contrôle pour suivre les progrès et identifier de nouveaux domaines qui pourraient nécessiter des améliorations à mesure que l'entreprise grandit et que le paysage des menaces évolue.

4. PRÉSENTATION DES RISQUES

1. Cybersécurité : Définition et enjeux

- **Définition :** La cybersécurité englobe les technologies, processus et les employés, pour protéger les systèmes, réseaux, programmes, dispositifs et données contre les attaques cybernétiques.
- **Enjeux :** Protéger l'intégrité, la confidentialité et la disponibilité des informations.

2. Types de menaces

- **Malware :** Comprend des logiciels comme les virus et les chevaux de Troie, qui peuvent endommager les données, voler des informations ou déstabiliser les opérations.
- **Phishing :** Désigne les courriels et messages conçus pour tromper les utilisateurs afin qu'ils révèlent des informations personnelles ou financières.
- **Ransomware :** Malware qui chiffre les fichiers de l'utilisateur, exigeant un paiement pour leur déchiffrement.
- **Attaques par déni de service (DDoS) :** Tentatives de rendre un service en ligne indisponible en le submergeant de trafic excessif.

3. Comprendre les fondamentaux

- **Politiques de sécurité :** Il est vital d'établir des politiques claires qui définissent les attentes en matière de sécurité, les procédures à suivre et les responsabilités de chaque employé.

- **Formation et sensibilisation :** Programmes réguliers de formation sur la sécurité pour tous les employés pour les éduquer sur les risques et les protocoles de sécurité, ainsi que les mises à jour régulières face aux nouvelles menaces.

4. Mesures de protection essentielles

- **Mots de passe forts et authentification à deux facteurs :** Encouragez l'utilisation de mots de passe complexes, changés régulièrement, et l'utilisation de l'authentification à deux facteurs pour une sécurité optimale.

- **Mises à jour des systèmes :** Garantir que tous les systèmes opérationnels et les logiciels sont maintenus à jour pour se protéger contre les vulnérabilités exploitées par les nouveaux virus et malwares.

5. Plan de réponse aux incidents

- **Développement d'un plan de réponse :** Établir un protocole clair d'intervention rapide en cas de violation de sécurité pour minimiser les impacts.

- **Stratégies de communication en cas de crise :** Prévoir des communications internes et externes pour informer et rassurer les parties prenantes sans compromettre la sécurité.

6. Audits et surveillance

- **Audits de sécurité réguliers :** Conduire des audits de sécurité pour évaluer l'efficacité des mesures de sécurité et identifier les faiblesses avant qu'elles ne soient exploitées.

- **Surveillance continue :** Mettre en place des systèmes de surveillance qui détectent et alertent en temps réel les activités suspectes ou malveillantes.

5. CONCLUSION

Nous espérons que ce guide vous donnera les outils nécessaires pour comprendre et guider les entreprises dans l'amélioration de la cybersécurité en entreprise. La protection contre les menaces cybernétiques nécessite une vigilance continue et une adaptation aux nouvelles technologies et menaces.

Pour en connaitre davantage sur la cybersécurité

BALADO ÉLAN : Le balado vous aidera à comprendre pourquoi la cybersécurité est cruciale, même pour les petites entreprises. Vous découvrirez les types de menaces les plus courantes pour les PME et les mesures de base à adopter pour se protéger.

6. ANNEXE

SOURCES

- Pensez cybersécurité : https://www.pensezcybersecurite.gc.ca/fr
- Centre canadien pour la cybersécurité : https://www.cyber.gc.ca/fr
- Securité 101 | Sécurité - Microsoft : https://www.microsoft.com/frca/security/business/security-101
- National Cybersecurity Alliance : https://www.staysafeonline.org/fr/
- CIS Center for Internet Security : https://www.cisecurity.org/

ADRIQ

2025

La trousse élan

Conseils d'experts pour favoriser l'accompagnement