Renforcez vos défenses numériques

Notions de base sur la cybersécurité

En 2023, le coût d'une violation de données s'élève à 6,5 M$ pour une PME[1]. Toute entreprise, peu importe sa taille et son secteur d'activité, est une cible potentielle. En investissant dans des technologies efficaces et en adoptant les meilleures pratiques de cybersécurité, vous pouvez protéger votre entreprise contre les cyberattaques.

Prenez les mesures suivantes pour protéger pour votre entreprise.

Investissez dans la sécurité de votre réseau

80 % des PME nord-américaines risquent de subir des cybermenaces[2].

Pare-feu

Les pare-feu surveillent le trafic réseau (entrant et sortant) et vous avertissent lorsqu'ils détectent une source suspecte ou un maliciel dans l'une de vos applications.

Logiciels de sécurité

Les logiciels antivirus et anti-maliciel défendent vos systèmes contre les virus, les rançongiciels, les logiciels espions et d'autres types de logiciels malveillants.

Outils de surveillance continue

Les logiciels de protection évolutive des points de terminaison surveillent vos systèmes et vos points d'accès. Ils détectent automatiquement toute anomalie et vous avisent afin de prévenir les cyberattaques.

Assurez la sécurité de vos points terminaux

97 % des PME canadiennes affirment avoir été ciblées par une attaque d'hameçonnage[3].

Correctifs et mises à jour

Mettre à jour vos micrologiciels (logiciels qui contrôlent des fonctions essentielles de votre matériel informatique) et installer les correctifs applicables au logiciel de votre système d'exploitation et à vos applications vous permet d'assurer que vos appareils sont munis des protections les plus à jour contre les cyberattaques, qui évoluent constamment

Copies de sauvegarde

Effectuer régulièrement des copies de sauvegarde de vos systèmes et données critiques hors ligne peut vous aider à minimiser vos pertes en cas de cyberattaque.

Chiffrement

Les ordinateurs personnels qui sont optimisés par Intel vPro® utilisent le chiffrement pour protéger la mémoire, les micrologiciels et les systèmes d'exploitation contre toute modification non autorisée. En protégeant les données, le chiffrement vous protège contre l'accès des cybercriminels aux appareils perdus ou volés.

Sécurité du cloud (infonuagique)

Au Canada, 1 PME sur 2 n'est pas en mesure de se protéger contre une brèche de sécurité infonuagique[4].

Broker de sécurité d'accès au cloud (CASB)

Les logiciels CASB renforcent la sécurité des applications infonuagiques, vous permettent de voir l'utilisation de vos employés, et vous offrent un meilleur contrôle sur la sécurité de vos données infonuagiques.

Authentification multifacteur (AMF)

L'authentification multifacteur vous permet de vous assurer que seules les personnes autorisées ont accès à vos appareils et vos systèmes. L'AMF comprend un mot de passe ainsi qu'un deuxième facteur d'identification.

Impliquez vos employés

En tout, 75 % des employés de PME ont indiqué avoir eu au moins un comportement qui pourrait compromettre la cybersécurité ou les données de leur employeur[5].

Établissez vos attentes

Sensibilisez vos employés au fait qu'ils ont un rôle de première ligne de défense contre les cyberattaques. Vous favoriserez ainsi une culture de la sécurité qui contribuera à la protection de votre entreprise.

Formation

Formez vos employés pour qu'ils soient en mesure de protéger leurs renseignements personnels sur les médias sociaux et de reconnaître les courriels, appels et sites Web suspects.

Politiques internes

Créez des politiques applicables à l'ensemble de l'entreprise (p. ex., utilisation des technologies, contrôle d'accès, bureau propre, etc.) pour protéger vos données et vos systèmes en établissant des exigences et des attentes claires envers vos employés.

Découvrez comment Intel vPro® peut vous aider à assurer la cybersécurité de votre entreprise. Visitez la page sur les fonctions de sécurité offertes par la plateforme Intel vPro® pour en savoir plus.

1 — IBM, Cost of Data Breach Report, 2023
2 — CyberCatch, Small and Medium-sized Businesses Vulnerabilities Report, 2022t
3 — CyberSavvy, Insurance Bureau of Canada Cyber Security Survey, 2023
4 — IDC, The State of Cloud Security in Canada, 2022
5 — CyberSavvy, Report Card, 2023

Renforcez vos défenses numériques

Liste de vérification

La plupart des cyberattaques peuvent être évitées en utilisant des appareils modernes et en appliquant quelques pratiques exemplaires de base en matière de cybersécurité[1].

Connaissez votre environnement

Faites l'inventaire du matériel informatique, des logiciels et des applications infonuagiques de votre entreprise afin de comprendre vos vulnérabilités.

Mettez en œuvre une politique sur l'utilisation des technologies

Créez une politique qui explique comment utiliser les technologies de façon adéquate et sécuritaire. Cette politique devrait comprendre des lignes directrices concernant les mots de passe et devrait aborder l'utilisation de technologies hors site ou à distance ainsi que la confidentialité des données.

Adoptez l'authentification multifacteur (AMF)

L'AMF vous permet de vous assurer que seules les personnes autorisées accèdent à vos systèmes.

Choisissez une technologie efficace

Les ordinateurs professionnels, optimisés par Intel vPro®, sont conçus pour protéger vos systèmes contre les cybermenaces courantes. Optez pour des appareils auxquels sont intégrées des fonctions de sécurité, qui sont en mesure de détecter et de prévenir les cyberattaques et de limiter les inefficacités qui prolongent la durée d'arrêt en cas de problème.

Tirez parti des fonctions intégrées

Activez les fonctions de sécurité (pare-feu, chiffrement, etc.) qui sont intégrées aux systèmes d'exploitation et aux appareils, notamment ceux qui sont optimisés par Intel vPro®.

Investissez dans des logiciels de sécurité

Installez des logiciels de sécurité modernes (anti-maliciel, antivirus, etc.) pour protéger vos systèmes contre les maliciels, virus, rançongiciels et logiciels espions. Configurez ces logiciels pour qu'ils vous envoient une alerte lorsqu'ils détectent une menace.

Remplacez vos appareils plus anciens

Les appareils plus anciens sont plus vulnérables aux cybermenaces, ce qui expose votre entreprise à des risques plus importants. Prévoyez dans vos plans et votre budget de remplacer vos anciens appareils par des plus récents auxquels sont intégrées des fonctions de sécurité.

Activez les mises à jour automatiques

Établissez un calendrier pour l'installation régulière des mises à jour de vos micrologiciels, de votre système d'exploitation et de vos logiciels. Ces correctifs comprennent souvent des mises à jour critiques sur le plan de la sécurité qui protégeront votre entreprise.

Accordez la priorité à la sécurité

La cybersécurité ne relève plus seulement des TI. Tout le monde a son rôle à jouer. Offrez une formation adaptée à vos employés afin qu'ils comprennent leur rôle dans la protection de votre entreprise.

Préparez-vous dès maintenant

Utilisez le Plan d'intervention en cas d'incident de cybersécurité de la FCEI pour exposer en détail qui prévenir et comment réagir si une cyberattaque potentielle se produit, afin de minimiser l'impact sur votre entreprise.

Découvrez comment Intel vPro® peut vous aider à assurer la cybersécurité de votre entreprise. Visitez la page sur les fonctions de sécurité offertes par la plateforme Intel vPro® pour en savoir plus.

1 — Microsoft, Digital Defence Report, 2022.

Présenté par FCEI | intel vPRO