Priorités en cybersécurité et plan budgétaire pour les PME

STREAMSCAN

www.streamscan.ai

1-877-208-9040

Sommaire

Pour les PME, la cybersécurité est maintenant non-négociable

Vous vous demandez par où commencer et combien investir en cybersécurité ?

Comme vous le voyez de plus en plus dans les nouvelles, il y a une augmentation drastique des cyberattaques ces dernières années. Celles-ci ne visent pas seulement le gouvernement et les multinationales, elles visent aussi des entreprises comme la vôtre entraînant d'importants coûts et de réels impacts. Investir dans des solutions de cybersécurité est nécessaire et primordial pour les PME. Mais dans quelles mesures devez-vous investir et quel est le prix à payer ? Regardons le tout de plus près.

Quelques chiffres clés

- Selon un récent **rapport publié par Verizon**, 63% des PME ont déclaré avoir été victime d'une fuite de données
- Au total, 28% des intrusions concernent une PME et ce pourcentage ne cesse d'augmenter en raison de la COVID-19 et du télétravail
- Pire encore, 46% des organisations de moins de 1000 employés ont été fermées entre 5 et 16 heures et 12% ont subi un arrêt de production entre 17 et 48 heures
- Et la cerise sur le sundae, le coût moyen des cyberincidents causés à l'interne pour les petites entreprises est de 7,68 millions de dollars, selon IBM et le Ponemon Institute

Définir les priorités - votre top 3

Il est maintenant question de savoir quoi faire et combien investir. En termes de priorités, il y a un certain consensus sur le marché. Voici les trois principaux éléments que chaque organisation devrait avoir à la base.

1. TRAITEZ LES PROBLÈMES ORGANISATIONNELS.

Menez un audit pour comprendre où vous en êtes, créez un plan à suivre pour la suite et éduquez votre personnel. Selon une étude récente, la sensibilisation des employés face à la cybersécurité devrait être l'une des trois priorités des responsables de la cybersécurité et des professionnels en technologie de l'information dans les PME.

2. SÉCURISEZ VOTRE RÉSEAU.

Le Centre canadien de cybersécurité a publié une liste des 10 principales mesures de cybersécurité à prendre et la mise en place d'une solution de surveillance des réseaux est la recommandation numéro 1. Vous devez également penser à inclure le coût des solutions complémentaires comme un pare-feu et un antivirus.

3. L'APPLICATION DE CORRECTIFS (PATCH) DE SÉCURITÉ.

Vous pensez peut-être que c'est une évidence, mais un logiciel non patché est un important vecteur d'attaque. Selon une publication sur ZDNet 33% des brèches sont dues à des vulnérabilités non corrigées et seulement 50% des entreprises interrogées ont appliqué tous les correctifs en une semaine. Faites-en donc une priorité et allouez-lui du temps et un budget.

Établir votre budget

2 Approches

La question à se poser maintenant est : combien ça coûte? Il n'y a pas de réponse simple à cette question, mais voici deux scénarios pour vous aider à déterminer quel devrait être votre budget en cybersécurité. Mais au-delà des chiffres, il faut se rappeler qu'investir dans la cybersécurité sous sa forme la plus simple est une question de coût-avantage.

SCÉNARIO 1 : Proportion des revenus

D'une part, l'organisation génère un chiffre d'affaires de montant X. Pour ce faire, l'organisation dépend principalement de ses ordinateurs, d'autres infrastructures informatiques et de la production. Il faut donc se demander combien je dois investir pour sécuriser mon réseau, mon infrastructure de production et mes employés? Selon une **étude récente de Deloitte**, le ratio recommandé est de 0,3 % à 0,5 % du chiffre d'affaires annuel pour assurer un niveau de sécurité adéquat contre les cybermenaces en constante évolution et en augmentation.

Exemple : La compagnie ABC a un chiffre d'affaires de 50.000.000 $. Afin de maintenir un niveau de sécurité acceptable, elle doit prévoir un budget entre (50.000.000 x 0,3%) et (50.000.000 x 0,5%), soit 150.000 à 250.000 dollars par an.

SCÉNARIO 2: Proportion des investissements informatiques

Une autre approche courante consiste à définir un pourcentage d'investissement approprié sur les dépenses totales consacrées à l'informatique. Ce type d'information est difficile à obtenir, car les entreprises ne veulent pas divulguer de chiffres. Mais selon **une etude d'IDC,** le pourcentage convenable est 14 %. À titre d'exemple, une PME de 50 millions de dollars consacre environ **8.2 % de son chiffre d'affaires aux TI** (bien que cela peut varier considérablement d'un secteur à l'autre). Pour une entreprise de 50 millions de dollars, cela représente 410 000 $. 14 % de ce montant donne un budget de cybersécurité de 57 400 $.

Priorités en cybersécurité pour les PME

Voici trois types d'initiatives de cybersécurité classées par ordre d'importance pour les PME. Dans un monde idéal, votre organisation serait capable de tout faire. Mais si vous ne le pouvez pas, voici comment hiérarchiser vos efforts.

NIVEAU 1 **Sécurité critique de base**	TIER 2 **Sécurité de base** (comprends les initiatives du niveau 1)	TIER 3 **Sécurité avancée** (comprends les initiatives du niveau 1 et 2)
• Audit de sécurité / Plan / Éducation des employés • Service de Détection et Réponse Gérées et autres outils de sécurité (antivirus, pare-feu, etc.) • Application des patchs de sécurité	• Test d'intrusion • Scans des vulnérabilités • Sécurisation des applications critiques (liste blanche) • Sauvegardes de données sécurisées • Budget de réponse aux cyberincidents • Responsable de la cybersécurité (CISO) virtuel	• Appliquer une stratégie de gouvernance • Obtenir une certification de sécurité (CyberSecure Canada, CMMC, etc.) • Engager un responsable de la cybersécurité (CISO) ou un directeur de la cybersécurité à plein temps

Comment répartir votre budget ?

Là encore, il n'existe pas de règles absolues sur le coût des choses. Il existe des milliers de fournisseurs de logiciels et de services qui proposent chacun des tarifs différents. La taille et la complexité de votre réseau ont également un impact sur les coûts finaux. Mais les informations budgétaires annuelles ci-dessous représentent notre compréhension basée sur l'expérience du monde réel. Il ne s'agit que d'un guide - les prix réels peuvent varier.

NIVEAU 1 - SÉCURITÉ DE BASE	
Initiative	**Coût**
Audit de sécurité / Plan	5 000 $
Solutions logicielles : Détection et Réponse Gérées (MDR) , pare-feu, antivirus	40 000 $
Soutien opérationnel et patchs de sécurité	5 000 $
Total (annuel)	50 000 $ *

NIVEAU 2 - SÉCURITÉ DE BASE (comprends les initiatives du niveau 1)	
Initiative	**Coût**
Audit annuel et plan	10 000 $
Test d'intrusion (2)	30 000 $
Scan des vulnérabilités (4)	10 000 $
Surveillance des réseaux - Détection et Réponse Gérées (MDR) + budget d'intervention d'urgence	60 000 $
Outils de sécurité complémentaires (antivirus, pare-feu, EDR, etc.)	30 000 $
Responsable de la cybersécurité (CISO) virtuel	40 000 $
Soutien opérationnel et patchs de sécurité	20 000 $
Total (annuel)	200 000 $ *

NIVEAU 3 - SÉCURITÉ AVANCÉE (comprends les initiatives du niveau 1 et 2)	
Initiative	**Coût**
Audit annuel et plan	10 000 $
Test d'intrusion (2)	30 000 $
Scan des vulnérabilités (4)	10 000 $
Surveillance des réseaux - Détection et Réponse Gérées (MDR)+ budget d'intervention d'urgence	60 000 $
Outils de sécurité complémentaires (antivirus, pare-feu, EDR, etc.)	30 000 $
Responsable de la cybersécurité (CISO) ou un directeur de la cybersécurité	140 000 $
Soutien opérationnel et patchs de sécurité	20 000 $
Programme de gouvernance de la cybersécurité	30 000 $
Obtenir une certification de sécurité (CyberSecure Canada, CMMC, etc.)	30 000 $
Total (annuel)	365 000 $ *

*Les chiffres relatifs au budget annuel peuvent varier jusqu'à 25 % selon la taille de votre organisation et le nombre d'appareils dans votre réseau.

Prenez en main votre cybersécurité dès aujourd'hui

Comment pouvons-nous vous aider?

Pour en savoir plus sur la conduite d'un audit de sécurité, l'élaboration d'un plan de sécurité ou la mise en place d'une solution de Détection et de Réponse Gérées, contactez-nous à l'adresse suivante : securitepme@streamscan.ai

À propos de StreamScan

La cybersécurité est tout aussi importante pour les moyennes entreprises que pour les multinationales. La réalité est que chaque année, une entreprise canadienne sur quatre, quelle que soit sa taille, voit son réseau être compromis. Avant StreamScan, il n'existait pas de solutions de sécurité conçues et tarifées spécifiquement pour les moyennes entreprises.

Le service de **Détection et de Réponse Gérées** de StreamScan s'appuie sur la technologie CDS, un outil de surveillance de réseaux basée par l'IA pour fournir une protection optimale, à un prix qui vous conviendra.

Pour en savoir plus, visitez notre site web : **www.streamscan.ai**

