Devolutions

Portrait de la cybersécurité dans les PME : comparaison entre les enquêtes de Devolutions 2020-2021 et 2021-2022

NOUS AVONS ÉTABLI DES FAITS ET CONSTATATIONS POUR LE MOINS INTÉRESSANTS!

Nous avons rassemblé les données récoltées dans l'enquête de **Devolutions 2021-2022 sur le portrait de la cybersécurité dans les PME** (téléchargez le rapport PDF ici). En comparant les résultats de cette année à ceux de l'année dernière, nous avons établi des faits et constatations pour le moins intéressants!

Six thématiques ont retenu notre attention :

- **Les préoccupations en cybersécurité**
- **La menace la plus inquiétante**
- **L'utilisation d'un gestionnaire de mots de passe**
- **L'utilisation des solutions PAM**
- **La formation en cybersécurité**
- **Les audits de cybersécurité**

1. Les préoccupations en cybersécurité

Constatation : Dans l'enquête 2021-2022, 72 % des PME ont déclaré être plus préoccupées par la cybersécurité aujourd'hui qu'il y a un an. Dans l'enquête de l'année précédente, ce taux était à 88 %.

Remarques : Nous constatons qu'un nombre croissant de PME fournissent des efforts et investissent afin d'améliorer leur posture en matière de cybersécurité. Il s'agit de l'une des deux améliorations significatives identifiées par l'enquête. L'autre amélioration, c'est la fréquence des audits en cybersécurité, que nous abordons plus loin dans cet article.

Une autre raison qui peut expliquer cette tendance à la baisse peut être le faux sentiment de sécurité de certaines PME, pensant être trop petites pour pouvoir être la cible d'une cyberattaque. Certaines personnes pensent aussi que la pandémie a contrecarré les plans des pirates informatiques (comme elle a contrecarré tous nos autres plans!).

Malheureusement, ces deux croyances sont fausses. Les pirates informatiques ont au contraire intensifié leurs attaques contre les PME pendant la pandémie. Ils ont pris pour cible les employés en télétravail qui sont plus vulnérables à la maison que dans le réseau de l'entreprise.

2. La menace la plus inquiétante

Constatation : Dans l'enquête 2021-2022, les PME ont déclaré que les rançongiciels étaient la cybermenace qui les préoccupait le plus. Dans l'enquête de l'année précédente, c'était les vulnérabilités infonuagiques.

Remarques : Il n'est pas surprenant que les rançongiciels détiennent la première place lorsqu'il s'agit de la cybermenace la plus redoutée. Pensez-y :

- D'ici fin 2021, on estime qu'un rançongiciel va attaquer une PME toutes les 11 secondes.
- 20 % des victimes de rançongiciels sont des PME.
- Le prix de la rançon moyenne a grimpé à 170 704$ par incident. Seulement 8 % des victimes qui paient une rançon récupèrent 100 % de leurs données.

Cependant, les PME ne devraient pas exclusivement se concentrer à combattre les logiciels malveillants. D'autres menaces existent comme l'hameçonnage, les vulnérabilités infonuagiques et les attaques de la chaîne d'approvisionnement . Nous offrons des conseils sur la manière de combattre ces menaces dans la section des recommandations du rapport de l'enquête 2021-2022.

3. L'utilisation d'un gestionnaire de mots de passe

Constatation : Dans l'enquête 2021-2022, 71 % des PME ont déclaré utiliser un gestionnaire de mots de passe pour stocker leurs mots de passe. Dans l'enquête de l'année précédente, ce nombre était à 81 %.

Remarques : Pourquoi les PME sont-elles 10 % de moins à utiliser un gestionnaire de mots de passe aujourd'hui qu'il y a un an? La raison la plus probable (comme nous l'avons vu plus haut) serait le faux sentiment de sécurité des PME par rapport aux grandes entreprises. L'autre raison serait que, parce qu'elles n'ont pas encore été piratées, les PME croient que leurs méthodes de stockage et de partage des mots de passe sont sûres et fiables.

Nous savons tous que cette croyance n'est pas fondée. Pas plus que la croyance voulant que de laisser la porte de l'auto déverrouillée soit plus sécuritaire. Ce n'est qu'une question de temps avant que la vulnérabilité ne soit exposée aux voleurs. Dans les deux cas, c'est une affaire de chance. Et la chance, ce n'est pas une stratégie de cybersécurité!

Comme nous l'expliquons dans la section des recommandations du rapport de l'enquête 2021-2022, toutes les PME (pas 71 %, ni 81 %, mais 100 %) devraient avoir recours à un gestionnaire de mots de passe robuste qui présente les caractéristiques suivantes :

- Un puissant chiffrement de bout en bout;
- L'authentification multifacteur (AMF);
- Un coffre sécurisé (pour le partage);
- Un générateur de mots de passe robuste;
- L'autorisation basée sur les rôles.

4. L'utilisation des solutions PAM

Constatation : Dans l'enquête 2021-2022, 13 % des PME ont déclaré avoir mis en place une solution de gestion des accès privilégiés entièrement déployée. Dans l'enquête de l'année précédente, ce nombre était à 24 %.

Remarques : La raison la plus probable qui explique cette baisse de 11%, c'est que certaines PME se tournent vers les gestionnaires de mots de passe pour remplacer leur solution PAM. Bien que ça semble à priori une bonne idée, c'est en réalité une énorme erreur!

Un gestionnaire de mots de passe robuste joue un rôle important dans une stratégie de sécurité, mais il n'est pas conçu pour gérer l'accès aux comptes privilégiés et ne peut fournir la visibilité, le contrôle et la gouvernance nécessaires pour :

- Protéger les données sensibles;
- Prendre en charge les exigences de conformité;
- Faire de la gestion à grande échelle.

5. La formation en cybersécurité

Constatation : Dans l'enquête 2021-2022, 74 % des PME ont déclaré offrir une formation en cybersécurité à leurs employés. Dans l'enquête de l'année précédente, ce nombre était à 88 %.

Remarques : Sans surprise, la pandémie est la raison la plus probable pour expliquer cette baisse de 14 %. Devoir faire face à des changements rapides et sans précédent a obligé de nombreuses PME à se concentrer sur leurs activités principales. Or, la formation de leurs employés en cybersécurité est une partie intégrante de ces activités! Comme nous l'avons vu, les pirates informatiques ont multiplié les attaques contre les PME pendant la pandémie. Il suffit d'un seul utilisateur malavisé, négligent ou imprudent pour déclencher une coûteuse violation de données.

6. Les audits de cybersécurité

Constatation : Dans l'enquête 2021-2022, 50 % des PME ont déclaré effectuer au moins deux audits complets de cybersécurité par an. Dans l'enquête de l'année précédente, ce nombre était à 38 %.

Remarques : Nous terminons notre comparaison comme nous l'avons commencé : sur une bonne note! Plus de PME ont compris qu'il était plus intéressant de détecter elles-mêmes leurs vulnérabilités et failles au lieu d'attendre que les pirates ou les utilisateurs malhonnêtes le fassent pour elles.

Sans vouloir être pessimiste, mais plutôt pragmatique, la proportion de PME qui effectuent au moins deux audits complets de cybersécurité par an devrait pourtant être de 100 %. La raison pour laquelle la moitié des PME ignorent ou revoient à la baisse cette priorité, c'est qu'elles ne disposent pas de l'expertise en interne. Dans ce cas, il est fortement conseillé aux PME de s'associer à un fournisseur de services gérés expérimenté et réputé. Voici pourquoi :

- Il possède les compétences et outils essentiels à la réalisation d'un audit complet en cybersécurité.
- Il peut effectuer un audit sans (ou à peine) perturber les opérations quotidiennes.
- Il est un tiers qui n'a pas de parti pris pouvant fausser les conclusions et les recommandations.

Dans la section des recommandations du rapport 2021-2022, nous prodiguons des conseils aux PME pour mieux évaluer les fournisseurs de services gérés potentiels.

À l'avenir

Le point le plus important à retenir, c'est que la situation entourant les cybermenaces s'aggrave. Il est nécessaire plus que jamais d'être proactif plutôt que réactif. En 2021, le coût moyen d'une violation de données dans une PME devrait atteindre la stupéfiante somme de 2,98 millions de dollars américains par incident.

Mettre en place un profil de cybersécurité solide, bien géré et surveillé, soutenu et optimisé par des technologies, des outils et des formations appropriés n'est plus seulement une priorité informatique. C'est une nécessité organisationnelle.

Pour rendre votre entreprise plus sûre, obtenir des informations et recommandations sur la protection des données, des clients et de la réputation des PME, téléchargez le rapport d'enquête Devolutions sur le portrait de la cybersécurité dans les PME en 2021-2022.