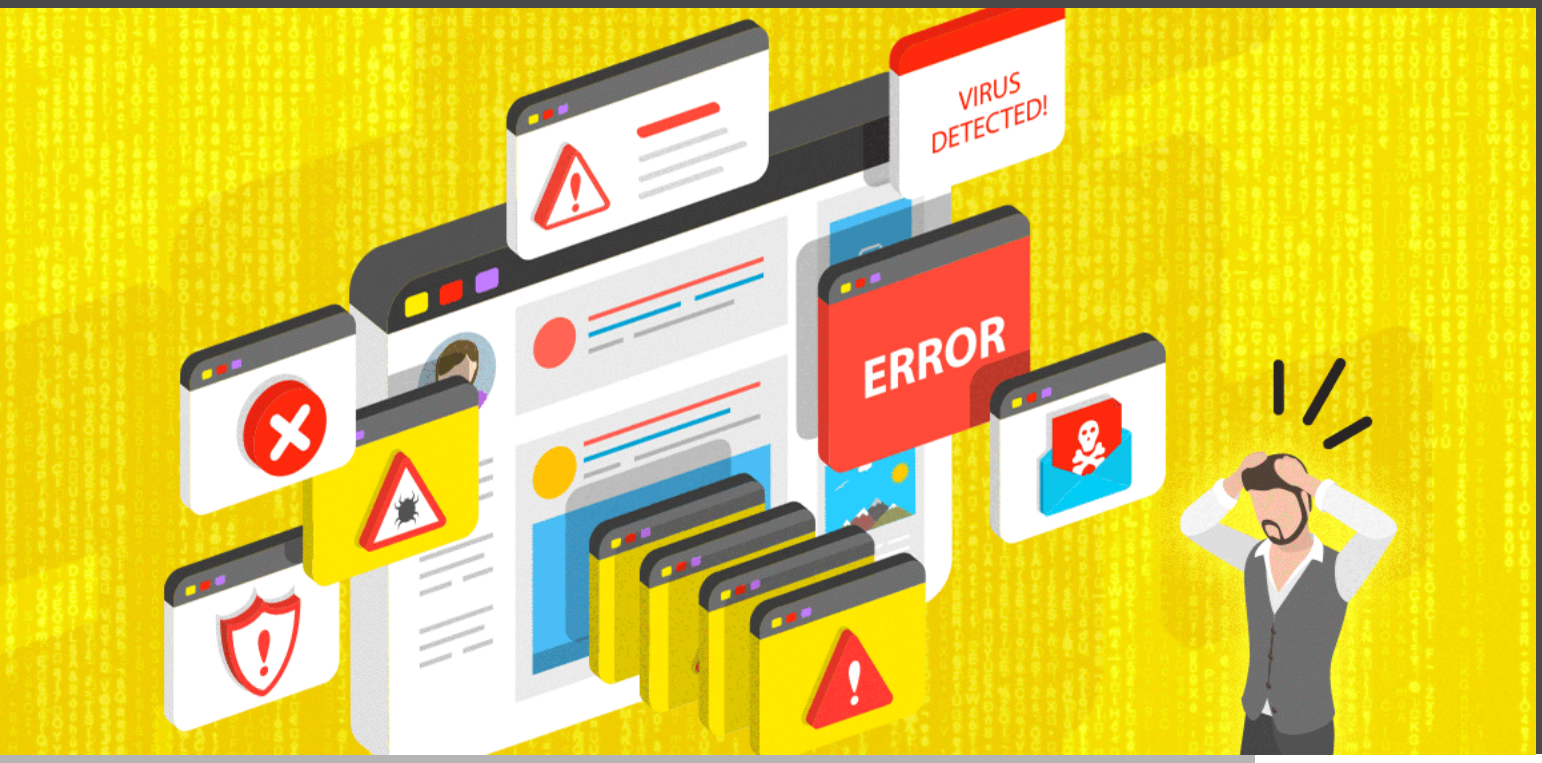
Devolutions

5 erreurs fréquentes des PME en matière de cybersécurité et comment les corriger



LES PME PEUVENT RENFORCER DE MANIÈRE PROACTIVE LEUR DÉFENSE EN MATIÈRE DE CYBERSÉCURITÉ

Le crooner légendaire Frank Sinatra, ainsi qu'un nombre incalculable d'invités de mariage ivres qui se considéraient comme de grandes vedettes du karaoké, ont pris le microphone et entonné la chanson classique My Way contenant les paroles « regrets, I've had a few, but then again, too few to mention » (en français, cela donne quelque chose comme : « des regrets, j'en ai eu quelques-uns, mais trop peu pour les mentionner. »)

De nos jours, de nombreuses petites et moyennes entreprises (PME) ont quelques regrets liés à la cybersécurité. Cependant, au lieu d'être trop peu nombreux pour être mentionnés, ils sont trop graves pour être ignorés. Le coût moyen de l'enquête et du nettoyage d'une brèche dans une PME est passé à plus de 200 000 dollars par incident et 60 % des PME font faillite dans les six mois suivant une cyberattaque. Même un guerrier intrépide comme Sinatra tremblerait devant ces statistiques.

Cependant, il y a une bonne nouvelle : les PME peuvent renforcer de manière proactive leur défense en matière de cybersécurité et réduire considérablement la probabilité et la gravité des attaques. Dans cette optique, voici cinq erreurs courantes de cybersécurité commises par les PME et comment les corriger.

1. Assumer qu'elles sont trop petites pour être attaquées

Non seulement les pirates ciblent les PME, mais ils intensifient leurs attaques pour une raison très pratique : les PME ont des défenses plus faibles par rapport à la plupart des grandes organisations et dans certains cas, pratiquement inexistantes.

Ainsi, en matière d'exposition aux menaces de cybersécurité, la première et la plus importante chose que les PME doivent accepter est que leur taille relativement petite n'est pas un avantage. C'est en fait un handicap, car les pirates supposent qu'elles sont vulnérables. C'est aux PME de démontrer le contraire. En effet, ce n'est pas de savoir SI une attaque va se produire, mais QUAND va-t-elle se produire et sa gravité.

2. Ne pas utiliser l'authentification multifacteur

Depuis que l'authentification multifacteur a fait son apparition il y a plusieurs années, il était difficile pour de nombreuses PME de l'utiliser, parce que les outils étaient coûteux et difficiles à configurer. En plus, les utilisateurs finaux étaient réticents à l'adopter, soit parce qu'il s'agissait d'une étape de connexion supplémentaire, soit parce qu'ils ne possédaient pas de téléphone intelligent (oui, oui, c'était le cas jadis!).

Aujourd'hui, il n'y a plus de raison ou d'excuse pour les PME de ne pas utiliser l'authentification multifacteur, que Microsoft considère d'ailleurs comme « l'outil le plus efficace contre les cybermenaces au sein d'une entreprise ». De nombreux outils MFA robustes et crédibles sont abordables et, certains, comme Devolutions Authenticator, sont gratuits.

Est-ce que cela veut dire l'authentification multifacteur est à toute épreuve ? Non. Des cybercriminels peuvent pirater l'authentification multifacteur par des tactiques comme les courriels d'hameçonnage, les échanges de

cartes SIM, les attaques de type « homme du milieu » ou même en reconstruisant le générateur de mots de passe. Cependant, malgré ces possibilités, le MFA doit être considéré comme obligatoire et non comme facultatif. Voyez cela comme la sécurité de votre maison : des cambrioleurs très expérimentés peuvent, avec suffisamment de temps et les bons outils, s'introduire dans n'importe quelle maison. Ça ne signifie pas que les gens doivent laisser leurs portes et leurs fenêtres déverrouillées. L'authentification multifacteur n'élimine pas totalement le risque, mais l'atténue certainement. C'est donc un pas dans la bonne direction.

3. Mauvaises pratiques de gestion des mots de passe

L'un des principaux avantages des PME par rapport aux grandes entreprises est qu'elles sont davantage agiles et flexibles. En effet, une bureaucratie excessive peut se révéler funeste. Cependant, la recherche de l'efficacité peut parfois s'avérer dangereuse plutôt que d'être rentable, et il n'y a pas de meilleur (ou pire, si vous préférez) exemple que des mauvaises pratiques de gestion des mots de passe. Par ailleurs, l'enquête de Devolutions sur l'état de la cybersécurité dans les PME pour 2020/2021 a révélé que :

- 57% des PME ne pensent pas que l'application d'une politique de longueur minimale des mots de passe soit très utile.
- 47 % des PME autorisent les utilisateurs finaux à réutiliser leurs mots de passe sur leurs comptes personnels et professionnels.
- 29 % des PME se fient à la mémoire humaine pour stocker les mots de passe.

Bien que les PME puissent (et franchement doivent) prendre plusieurs mesures pour améliorer la gestion des mots de passe, les pratiques essentielles et les plus efficaces sont les suivantes :

- Utilisez l'authentification multifacteur (comme indiqué précédemment).
- Utilisez un outil de gestion des mots de passe fiable (cliquez ici pour une comparaison des différentes options populaires).
- Utilisez un coffre sécurisé pour le partage des mots de passe.
- Utilisez des phrases de passe.
- Changez les mots de passe après la preuve d'une compromission.
- Comparez les mots de passe avec une liste de mots de passe faibles et compromis.
- Interdisez la réutilisation des mots de passe.
- Appliquez une politique d'historique des mots de passe.
- Activez le copier-coller des mots de passe.
- Inscrivez les utilisateurs finaux à une formation à la cybersécurité.

4. Ne pas auditer et surveiller les comptes privilégiés

Comme le note l'organisation internationale et indépendante d'analystes KuppingerCole Analysts : « Les comptes privilégiés sont attribués aux administrateurs et aux autres utilisateurs d'une entreprise pour accéder aux données et aux applications critiques. Cependant, si ces comptes ne sont pas gérés de manière sécurisée, les PME peuvent se retrouver avec des comptes ouverts pour des personnes qui ont quitté l'entreprise, pour des personnes qui n'ont plus besoin d'accès ou tout simplement en donnant des comptes privilégiés à trop de personnes. »

Alors, comment les PME peuvent-elles suivre ce conseil et gérer en toute sécurité leurs comptes privilégiés ? La réponse est d'utiliser une solution PAM qui répond à tous les critères suivants :

- Facile à déployer et à gérer.
- Disponible en plusieurs modèles de licence et à un prix abordable.
- Fournit un coffre sécurisé pour les mots de passe.
- Prend en charge la journalisation et les rapports complets.
- Fonctionnalité d'authentification multifacteur intégrée.
- Prend en charge le courtage de comptes (c'est-à-dire que les utilisateurs finaux autorisés peuvent se connecter à des comptes/accéder à des zones du réseau, mais sans avoir besoin de voir les mots de passe).
- Permet l'accès aux informations d'identification en fonction des rôles.
- Épaulé par un soutien technique réactif.

5. Essayer de tout faire à l'interne

Ce qui est amusant avec les titres des postes dans les PME, c'est que personne n'en a qu'un seul. Bien sûr, ils peuvent avoir quelque chose comme « chef de projet » ou « développeur de logiciels » sur leur signature de courriel et leur carte de visite, mais, en réalité, ils jouent plusieurs rôles et portent plusieurs chapeaux. C'est comme ça que cela fonctionne dans le monde des PME. Tout le monde doit être flexible et polyvalent.

Cependant, il est parfois nécessaire d'obtenir une aide extérieure. Pour de nombreuses PME, cela signifie travailler avec un fournisseur de services gérés afin de diminuer la charge de leur « gourou informatique » qui, en plus de veiller sur l'infrastructure, gère le programme de cybersécurité. Un fournisseur de services gérés prend en charge une partie du travail et comble les lacunes, ce qui fait la différence entre une défense solide et une vulnérabilité aux attaques. Cliquez ici pour obtenir des conseils sur la manière de choisir le bon fournisseur de services gérés.

Le mot de la fin

Comme on nous l'a rappelé de façon dramatique pendant la pandémie, les PME sont l'épine dorsale de l'économie. Par exemple, aux États-Unis, les PME génèrent 66 % des nouveaux emplois et représentent 43,5 % du PIB. Et dans de nombreux autres pays, l'impact est encore plus important, comme au Canada où les PME représentent plus de 99 % de l'économie et emploient près de 90 % de la main-d'œuvre privée totale.

Toutefois, pour rester fortes et optimiser leur potentiel de croissance, les PME ne doivent pas se contenter de se concentrer sur leur marché et leur chaîne d'approvisionnement. Elles doivent également prêter attention à leur profil de cybersécurité et, si nécessaire, apporter des améliorations rapides et essentielles. Il n'est pas judicieux d'attendre que quelque chose de grave se produise avant de prendre des mesures… Parce qu'à ce moment-là, il est généralement déjà trop tard.