Devolutions

5 stratégies pour améliorer la cybersécurité des PME en 2021

CET ARTICLE A ÉTÉ RÉDIGÉ PAR L'ÉQUIPE DE PETRI EN COLLABORATION AVEC DEVOLUTIONS.

Il ne fait aucun doute que les incidents de sécurité sont en augmentation pour les entreprises de toutes tailles. Avec la récente pandémie, il est clair que les menaces de cybersécurité sont devenues un problème plus important que jamais.

Cependant, il y a une croyance qui persiste dans les petites et moyennes entreprises (PME), selon laquelle les vulnérabilités les plus critiques n'existent que dans les grandes organisations. La réalité est toute autre : les PME sont en fait plus vulnérables aux cyberattaques que les grandes entreprises, et ce, pour plusieurs raisons.

Premièrement, bien que les grandes organisations aient tendance à avoir une plus grande surface d'attaque, ces entreprises disposent généralement d'un personnel de sécurité spécialisé qui se consacre à la protection de l'organisation. Les compétences et les ressources dont elles disposent dépassent généralement de loin celles des PME.

Deuxièmement, l'impact des attaques de cybersécurité ou de rançongiciels peut être dévastateur pour une PME. Une organisation plus grande dispose généralement des ressources nécessaires pour résister à ces types d'attaques et, bien que ça puisse engendrer des coûts importants, l'entreprise devrait pouvoir rester opérationnelle. Ce n'est pas toujours le cas pour les PME, puisqu'une longue interruption de service pourrait les mettre en faillite.

Dans son rapport sur le portrait de la cybersécurité dans les PME en 2020-2021, Devolutions a interrogé les décideurs des PME du monde entier et a découvert plusieurs failles critiques en matière de sécurité. Premièrement, 80 % des PME admettent que les logiciels malveillants ont échappé à leur logiciel antivirus. Deuxièmement, 66 % des PME ont déclaré avoir subi au moins une cyberattaque au cours des 12 derniers mois et que chaque cyberattaque a entraîné en moyenne huit heures d'arrêt. Enfin, et plus inquiétant encore, 60 % des PME ont cessé leurs activités dans les six mois suivant une cyberattaque.

Cinq étapes fondamentales pour renforcer la protection de la cybersécurité des PME

Dans les sections suivantes, vous apprendrez cinq stratégies de cybersécurité que les PME peuvent mettre en œuvre et qui généreront des gains rapides. Dans chaque section, vous découvrirez certaines des principales conclusions de la recherche sur la cybersécurité des PME de Devolutions ainsi que des recommandations sur la manière de traiter efficacement les différents problèmes pour améliorer la sécurité de votre organisation.

1. Mettre en œuvre une gestion des accès privilégiés

Les PME s'appuient sur des comptes privilégiés pour augmenter l'efficacité et la productivité de leurs employés.

Malheureusement, les pirates informatiques comptent également sur l'accès à des comptes privilégiés vulnérables pour infiltrer les réseaux, accéder aux systèmes critiques et voler des données confidentielles. La gestion des accès privilégiés (ou PAM, de l'anglais ***Privileged Access Management***) fait référence à une classe de solutions qui aident à sécuriser, gérer et surveiller l'accès privilégié aux actifs critiques. Les recherches de Devolutions

ont montré que 76 % des PME ne disposent pas d'une solution PAM entièrement déployée, même si Gartner a identifié la mise en œuvre d'une solution PAM comme l'une de ses 10 priorités de sécurité pour 2019.

Les solutions PAM peuvent empêcher l'accès à des comptes hautement privilégiés. Elles protègent non seulement contre les cybermenaces externes, mais elles peuvent également empêcher les menaces internes comme l'utilisation abusive accidentelle ou délibérée de comptes privilégiés. Pour contrer ces types de menaces, les solutions PAM vous fournissent les outils dont vous avez besoin pour restreindre, révoquer et surveiller l'accès aux comptes hautement privilégiés.

Néanmoins, de nombreuses PME hésitent encore à adopter une solution PAM, parce qu'elles estiment que ça peut être trop coûteux et trop compliqué. Il vaut la peine de considérer qu'une solution PAM de qualité aidera à rendre plus efficace la gestion des utilisateurs privilégiés : en réduisant le temps consacré à ces tâches. Elle libérera donc des ressources qui pourront se concentrer d'autres tâches à valeur ajoutée. Les solutions PAM sont un composant essentiel de la cybersécurité et elles peuvent fournir des informations vitales sur vos comptes privilégiés. Par exemple, elles peuvent vous indiquer le nombre de comptes privilégiés dont vous disposez qui n'expirent jamais ou le nombre de comptes privilégiés qui devraient être supprimés.

Les solutions PAM offrent une protection et une surveillance des comptes privilégiés. Lorsque des comptes privilégiés sont créés ou définis, les outils PAM offrent une protection unique pour leurs informations d'identification. Une solution de stockage des informations d'identification ou un système de gestion des mots de passe est utilisé pour stocker en toute sécurité les informations des comptes privilégiés et peuvent donc empêcher tout accès non autorisé.

Pour accéder à ces comptes privilégiés, les utilisateurs doivent passer par la solution PAM. À chaque fois qu'un utilisateur accède à ces comptes, la solution PAM enregistre la session et suit les actions effectuées. Un enregistrement complet de l'accès au compte privilégié comprend le nom de l'utilisateur, l'heure à laquelle sa session a commencé, sa durée et les actions effectuées.

Les types de comptes que les solutions PAM doivent surveiller et auditer comprennent :

- Comptes d'administrateur de domaine
- Comptes d'utilisateurs privilégiés
- Comptes d'administrateur local
- Comptes d'accès d'urgence
- Comptes d'application
- Comptes système
- Comptes de service de domaine

Pour répondre efficacement aux besoins des PME, les solutions PAM doivent offrir une facilité de déploiement et de gestion, un coffre de mots de passe sécurisé, une journalisation et des rapports, une authentification à deux facteurs intégrée, l'injection des identifiants et un contrôle d'accès aux informations d'identification basé sur les rôles. Idéalement, la solution ne nécessiterait aucune modification de l'infrastructure Active Directory (AD) et devrait s'intégrer à Azure AD.

2. Utiliser un gestionnaire de mots de passe pour faire appliquer des politiques de mots de passe strictes

Les mots de passe faibles et réutilisés sont deux des plus grands risques de sécurité des PME. Des recherches ont effectivement montré que 81 % des violations de données sont causées par des mots de passe compromis, faibles et réutilisés. Aussi, 29 % de toutes les violations impliquent l'utilisation d'informations d'identification volées, et une mauvaise utilisation du mot de passe en est une des principales causes.

D'autres études ont montré que 59 % des utilisateurs finaux utilisent les mêmes mots de passe pour tous les comptes. En effet, les utilisateurs ne peuvent simplement pas se souvenir de tous les différents mots de passe requis pour accéder aux ressources dont ils ont besoin. Une enquête récente a montré que les utilisateurs professionnels doivent se souvenir en moyenne de 191 mots de passe. Ils doivent aussi saisir leurs informations d'identification pour divers sites Web et applications jusqu'à 154 fois par mois.

Les gestionnaires de mots de passe peuvent considérablement renforcer la cybersécurité des PME en facilitant l'application de politiques de mots de passe strictes au sein de l'organisation. Cela permet par le fait même d'éliminer les mots de passe faibles et réutilisés.

Les gestionnaires de mots de passe suppriment également le fardeau d'avoir à mémoriser et gérer plusieurs mots de passe, parce qu'ils stockent toutes les informations d'authentification requises dans un emplacement sécurisé et centralisé. Les gestionnaires de mots de passe peuvent générer automatiquement des mots de passe forts pour les utilisateurs finaux et restreindre les mots de passe faibles et interdits. Ils peuvent également appliquer plusieurs politiques de mots de passe différentes qui garantissent la sécurité des mots de passe de votre organisation.

Les politiques de mots de passe fournies par les gestionnaires de mots de passe doivent inclure :

- **Mots de passe uniques** - Empêche la réutilisation du mot de passe et exige que chaque compte ait un mot de passe différent.
- **Longueur minimale du mot de passe** - Nécessite un nombre minimal de caractères dans un mot de passe.

- **Exigences de complexité** - Garantit que le mot de passe ne peut pas contenir le nom d'utilisateur et qu'il doit utiliser une combinaison de lettres minuscules, majuscules, chiffres et symboles.
- **Historique des mots de passe** - Empêche la réutilisation des anciens mots de passe pendant une période donnée.
- **Âge du mot de passe** - Un utilisateur doit modifier son mot de passe après une période de temps spécifiée.

Deux autres bonnes pratiques pour la gestion des mots de passe pour les PME consistent à utiliser l'authentification à 2 facteurs (2FA) lorsque possible et à adopter l'utilisation de phrases secrètes pour créer des mots de passe longs qui peuvent être plus facilement mémorisés. Le 2FA ajoute un niveau de sécurité en exigeant que l'utilisateur présente quelque chose qu'il possède, comme une clé de sécurité, en plus de quelque chose qu'il connaît (un mot de passe). L'utilisation de phrases secrètes rend les mots de passe plus sécuritaires parce qu'ils sont plus longs. Finalement, les PME doivent veiller à modifier tous leurs mots de passe en cas de preuve d'une faille de sécurité.

Bien qu'il existe des gestionnaires de mots de passe gratuits et d'autres options telles que les coffres de mots de passe intégrés au navigateur Web, ces solutions gratuites sont limitées. Les offres gratuites n'ont pas de soutien téléphonique, elles peuvent être difficiles à déployer, ont des fonctionnalités restreintes et n'ont généralement pas de sauvegarde en ligne. Il vaut mieux utiliser ces solutions que rien du tout, mais cela présente également plusieurs limites critiques pour les entreprises.

Premièrement, le navigateur fonctionne généralement pour une personne à la fois et il n'est pas possible de sécuriser ou de gérer vos mots de passe de manière centralisée. Plus important encore, la gestion des mots de passe du navigateur est simpliste et ne fournit pas les règles de génération, de complexité et de réutilisation de mots de passe fournies par un véritable gestionnaire de mots de passe. Les navigateurs n'enregistrent également que les mots de passe des sites Web, ce qui signifie qu'ils ne peuvent pas fonctionner avec d'autres types d'applications utilisées dans les PME.

3. Bâtir votre stratégie de sécurité autour du principe du moindre privilège

Le principe du moindre privilège (ou POLP, de l'anglais ***Principle of Least Privilege***) stipule essentiellement que chaque processus, utilisateur ou programme n'est autorisé à accéder qu'aux informations et aux ressources nécessaires aux fins prévues.

Malheureusement, de nombreuses PME ne suivent pas ce principe. Au lieu de cela, ils ont souvent des utilisateurs qui travaillent avec des autorisations plus élevées que ce dont ils ont réellement besoin. L'inconvénient de ne pas utiliser le principe du moindre privilège est que cela peut ouvrir la porte à des cyberattaques. Les recherches de Devolutions ont démontré que 74 % des violations de données proviennent d'une utilisation abusive d'identifiants privilégiés.

Si l'utilisation de privilèges élevés peut faciliter l'exécution de certaines tâches, les risques encourus l'emportent largement sur les avantages. Permettre aux utilisateurs de travailler avec des privilèges administratifs réduit considérablement la protection des autres structures de sécurité.

Par exemple, si un utilisateur qui possède des autorisations élevées clique sur un lien dans un courriel infecté, il peut installer des logiciels malveillants sans être analysé par un logiciel antivirus ou il peut permettre à un pirate de localiser et d'identifier d'autres vulnérabilités dans votre environnement informatique. Cela aurait non seulement un impact sur le système de l'utilisateur, mais pourrait également avoir un impact sur d'autres systèmes du réseau ainsi que sur les données des partenaires et des clients.

La mise en œuvre du principe du moindre privilège peut réduire la surface d'attaque de l'organisation et arrêter les cyberattaques et les logiciels malveillants avant qu'ils ne fassent des dommages à l'entreprise. La première étape consiste à analyser les responsabilités et les niveaux d'accès actuels de tous vos utilisateurs. Comme son nom l'indique, l'accès par défaut doit être les moindres privilèges. Tout privilège supplémentaire ne doit être accordé qu'en cas de nécessité.

L'utilisation de l'accès basé sur les rôles peut vous aider à commencer à implanter le POLP. Avec l'accès basé sur les rôles, vous affectez des utilisateurs à différents groupes en fonction de leurs rôles de travail, puis appliquez les privilèges appropriés pour ces groupes.

Le POLP garantit que les utilisateurs finaux n'utilisent pas couramment des comptes hautement privilégiés, ce qui les empêche d'effectuer des actions qui pourraient affecter l'ensemble de l'environnement informatique de l'entreprise ou d'autres systèmes en réseau. Le POLP peut aider à contenir les attaques et les logiciels malveillants à un seul utilisateur ou appareil. Il est toutefois important de se rappeler que le POLP doit travailler main dans la main avec une solution PAM pour limiter, contrôler et surveiller l'utilisation des comptes privilégiés - c'est une bonne pratique pour aider à garder vos systèmes en sécurité.

4. Mettre en œuvre la séparation des tâches

Les PME doivent mettre en œuvre une politique de séparation des tâches (ou SoD de l'anglais ***Segregation of Duties***) qui sépare les comptes administrateur des comptes standards, de même que les fonctions système de niveau supérieur des fonctions système de niveau inférieur. L'objectif derrière une politique SoD est de réduire les possibilités d'utilisation abusive non autorisée ou non intentionnelle des actifs de l'organisation. La SoD répartit les responsabilités de l'organisation entre plusieurs employés.

Les mêmes facteurs qui rendent les PME vulnérables aux pirates externes les rendent également vulnérables aux attaques d'employés mécontents, d'anciens employés, de sous-traitants et d'autres personnes malhonnêtes.

Cependant, de nombreuses petites entreprises pensent que la SoD perturbe les utilisateurs finaux en les limitant dans leurs activités et en réduisant leur efficacité et leur productivité.

La mise en œuvre d'une politique SoD stricte peut pourtant aider à protéger les PME des pirates externes ainsi que des menaces internes et c'est une étape fondamentale pour renforcer vos contrôles internes. Les audits de sécurité peuvent aider à appliquer une SoD, mais l'enquête de Devolutions a révélé que 62 % des PME ne mènent pas d'audits de sécurité annuels et que 14 % des PME n'effectuent jamais d'audit.

Il est préférable que la PME puisse travailler avec un cabinet ou un consultant externe pour ses audits. Néanmoins, de nombreuses PME préfèrent mener des audits internes, puisqu'ils sont moins coûteux et plus pratiques. Dans les deux cas, l'utilisation d'une SoD comblera les failles de sécurité et peut rendre le processus d'audit beaucoup plus efficace.

5. Former ses utilisateurs en matière de cybersécurité

Les utilisateurs finaux peuvent être les principaux atouts en matière de sécurité… ou l'une des plus grandes failles. 79 % des responsables informatiques estiment qu'au cours des 12 derniers mois, leurs propres employés ont accidentellement mis en danger les données de l'entreprise.

Pour atténuer ce problème, 88 % des PME offrent de la formation en cybersécurité à leurs utilisateurs finaux. Cependant, compte tenu des risques, le niveau d'éducation des utilisateurs devrait être de 100 %.

Par exemple, la vulnérabilité aux attaques d'hameçonnage est un domaine où l'éducation des utilisateurs peut avoir un impact significatif. Des recherches ont montré que 56 % des décideurs informatiques estiment que la prévention des attaques d'hameçonnage est la priorité de leur entreprise en matière de cybersécurité. La même étude a révélé que 90 % des violations de cybersécurité incluent un élément d'hameçonnage et que 94 % des logiciels malveillants sont envoyés par courriel.

Sensibiliser les utilisateurs pour éviter qu'ils ouvrent un courriel suspect ou qu'ils cliquent sur d'éventuels liens d'hameçonnage peut suffire à empêcher tout ce mécanisme d'attaque. Des utilisateurs informés et consciencieux sont la meilleure défense contre les attaques de cybersécurité. L'éducation des utilisateurs sur les risques et les meilleures pratiques en matière de cybersécurité peut être l'une des défenses les plus complètes et les plus rentables pour la cybersécurité des PME.

Les utilisateurs avertis n'ouvriront pas des courriels et des pièces jointes d'expéditeurs inconnus. Ils ont des pratiques de mots de passe sécuritaires et ils adhèrent mieux aux politiques de cybersécurité.

L'une des méthodes les plus efficaces pour promouvoir l'éducation des utilisateurs consiste à les inscrire à une formation en ligne sur la cybersécurité. La formation en ligne est généralement personnalisée et basée sur une approche pratique, en fonction des compétences. Les utilisateurs apprennent des techniques de détection et d'atténuation des menaces. Ils reçoivent une rétroaction immédiate par rapport à leurs progrès et peuvent avancer dans la formation en fonction de leurs performances. Les gestionnaires peuvent également accéder à la plateforme de formation pour suivre les progrès de leurs employés.

En résumé

Les PME ne peuvent pas supposer que leur petite taille les protégera des cyberattaques. En fait, comme vous l'avez appris dans ce document technique, les PME sont plus vulnérables aux attaques de cybersécurité que les grandes organisations. Comme on dit, ce n'est pas **si** ces attaques se produisent - c'est **quand**. Ne rien faire peut avoir des conséquences désastreuses et c'est possible qu'une PME ne survive pas à une cyberattaque. En suivant les cinq stratégies en matière de sécurité pour les PME présentées dans ce document technique, vous pouvez renforcer votre sécurité et contrer la plupart des cyberattaques avant qu'elles ne surviennent.