Devolutions

Portrait de la CYBERSÉCURITÉ dans les PME en 2020-2021

Nos prédictions pour 2021

Lorsque nous envisageons l'année 2021, plusieurs estiment que la pandémie du coronavirus prendra fin, et qu'éventuellement, la peur et l'angoisse feront enfin place à l'espoir et à l'optimisme.

Toutefois, la situation pour les petites et moyennes entreprises en matière de cybersécurité s'est aggravée dans les derniers mois. Et elle continuera de se détériorer au cours de l'année.

TENDANCES À VENIR + RECOMMANDATIONS

Selon notre rapport sur le portrait de la cybersécurité dans les PME en 2020-2021 et les derniers développements depuis sa publication, quatre principales tendances dans la prochaine année ressortent du lot :

1 LES PIRATES INFORMATIQUES VISERONT DE PLUS EN PLUS LES TRAVAILLEURS À DISTANCE.

Le travail à la maison est là pour de bon. Un sondage mené par Gartner révèle que 82 % des chefs d'entreprise permettront aux employés de télétravailler après la pandémie (du moins, à temps partiel, et dans certains cas, à temps plein). Malheureusement, les pirates informatiques ont flairé la bonne affaire et exploitent allègrement cette nouvelle vulnérabilité dans les PME. Le FBI a rapporté que le nombre de plaintes concernant des cyberattaques a atteint le plateau de 4000 plaintes par jour, ce qui représente une augmentation de 400 % par rapport aux chiffres prépandémiques.

En 2021, nous croyons que les pirates informatiques continueront de cibler les télétravailleurs dans les PME. Au moins huit tactiques ou types d'attaques seront à surveiller : l'hameçonnage, des attaques XXS et de tiers, des vols de base de données et des rançongiciels. Cela inclut également du minage clandestin (de l'anglais *cryptojacking*), des attaques sur les terminaux et des attaques de l'intérieur menées par des employés mécontents (anciens ou actuels).

Pour contrer cette menace, les PME doivent implanter une solution de gestion d'accès privilégiés. Celle-ci doit comprendre les fonctionnalités suivantes : le contrôle d'accès basé sur les rôles, des politiques de mots de passe robustes, l'intégration d'Active Directory. Elle doit aussi fournir des pistes d'audit et de la journalisation, l'authentification à deux facteurs, la rotation de mots de passe automatique, l'injection d'identifiants, etc.

De plus, les PME doivent migrer leurs données vers le nuage informatique, appliquer le principe de moindre privilège et s'assurer que les télétravailleurs sécurisent leur réseau sans fil à la maison. Elles doivent également protéger et surveiller les accès à distance afin de protéger à la fois les travailleurs et l'organisation contre les acteurs malveillants.

2 LA PÉNURIE DE MAIN-D'ŒUVRE QUALIFIÉE EN CYBERSÉCURITÉ AUGMENTERA.

En août 2020, la firme de recherche et de formation SANS dévoilait une grande pénurie de personnel compétent dans le domaine de la cybersécurité. En effet, la majorité des candidats ne maîtrisent pas des concepts de base comme les techniques d'exploitation les plus courantes, l'architecture d'ordinateur et la virtualisation, la réseautique, la programmation et la cryptographie. Mauvaise nouvelle : cette pénurie n'est pas près de se résorber en 2021. Les PME n'auront toujours pas les moyens financiers pour engager une équipe de spécialistes en sécurité de l'information et en TI à l'interne.

Pour combler ce manque, les PME devraient faire appel à des fournisseurs de services gérés qui offrent l'expertise et les ressources nécessaires à un prix abordable. Un bon fournisseur de services gérés offre une gamme complète de services, répond rapidement, surveille votre infrastructure 24/7 et implante des outils et des politiques permettant la continuité et la reprise des activités après un incident. Il choisit des technologies ou des fournisseurs en fonction de vos réels besoins, communique de façon exemplaire et déploie des efforts soutenus pour vous servir.

3 LES EMPLOYÉS NÉGLIGENTS DEMEURERONT LE MAILLON LE PLUS FAIBLE DE LA CHAÎNE.

En plus de se défendre contre les acteurs malveillants, les PME doivent prendre en compte une menace insoupçonnée qui continuera de semer le chaos en 2021 : les utilisateurs finaux imprudents.

Ces utilisateurs sont des employés, des sous-traitants ou d'autres personnes gravitant autour de l'entreprise qui, par leur négligence ou leur incompétence (parfois une combinaison des deux), exposent les PME au danger. Par exemple, ils ont envoyé des informations confidentielles par accident à une source non autorisée; n'ont pas considéré l'importance d'apporter des correctifs nécessaires à un logiciel; n'ont pas sécurisé les ordinateurs, tablettes et téléphones intelligents à l'extérieur du bureau.

Pour réduire les risques, les PME devraient inscrire leurs équipes sur une plateforme de formation en ligne. Cette formation en cybersécurité devrait traiter de sujets spécifiques tels que l'ingénierie sociale, la sécurité sur les courriels, les appareils mobiles et les réseaux sociaux. Elle devrait aussi couvrir la navigation Web sécuritaire, la protection des informations relatives à la santé et bien plus.

Les utilisateurs ne deviendront pas des experts du jour au lendemain, mais ils auront les connaissances de base nécessaires pour faire partie de la solution, et non du problème.

4 DE PLUS EN PLUS DE PME ADOPTERONT UNE STRATÉGIE CONFIANCE ZÉRO.

La montée en flèche du télétravail a provoqué de nouveaux maux de tête aux PME en lien avec l'utilisation de réseaux privés virtuels. Notons les contraintes de bande passante, la perte de productivité des utilisateurs et la difficulté à configurer des systèmes requis sans expertise interne. De plus, les travailleurs à distance peuvent laisser tomber la garde en utilisant un ordinateur personnel et ainsi ouvrir la porte à une brèche dans le réseau de l'entreprise.

Pour se protéger contre les menaces, les PME devraient sérieusement considérer l'implantation d'une architecture Confiance zéro. Il s'agit d'un système présumant qu'il y a présence d'une brèche, alors il vérifie chaque requête comme si elle provenait d'un réseau public. Toute requête d'accès est authentifiée, autorisée et chiffrée, réduisant le mouvement latéral dans le réseau interne, surtout lorsque le principe de moindre privilège a été mis en place.

Implantée correctement, cette méthode s'avère efficace contre des attaques sophistiquées d'envergure semblables à l'attaque de chaîne d'approvisionnement Solorigate. À la base, le concept repose sur le principe de « ne jamais faire confiance, toujours vérifier ». En présumant que rien n'est digne de confiance et en authentifiant chaque opération et appareil, la stratégie Confiance zéro aide les PME à améliorer leur posture de sécurité.

CE QUE L'AVENIR NOUS RÉSERVE

2021 sera une année difficile pour les PME en ce qui a trait à la lutte contre les cybermenaces et à la prévention de fuites de données. Or, si les PME suivent les conseils ci-dessus ainsi que ceux figurant dans notre rapport sur la cybersécurité dans les PME en 2020-2021, elles seront mieux outillées pour faire face à d'éventuelles cyberattaques.

En résumé, la cybercriminalité est en plein essor partout dans le monde, alors les PME se doivent d'agir maintenant, avant qu'il ne soit trop tard.