« The Enemy Within »: 72 % des professionnels des TI avouent être vulnérables aux attaques qui viennent de l'intérieur

Devolutions

72% DES PROFESSIONNELS DES TI ADMETTENT QUE LEUR ENTREPRISE EST VULNÉRABLE AUX ATTAQUES DE L'INTÉRIEUR

Les films d'horreur les plus terrifiants ne traitent jamais de menaces de l'au-delà. Ce sont toujours des dangers qui se cachent à l'intérieur - dans le sous-sol, le grenier ou la télévision (« Ils sont iciiii »). Les professionnels des TI, eux, restent éveillés la nuit en agrippant leurs draps non pas parce qu'ils ont peur des possessions démoniaques ou des fantômes, mais parce qu'ils sont terrifiés par les utilisateurs finaux.

Une récente étude réalisée par la société d'analyse en sécurité et fraude Gurucul a révélé que 72% des professionnels des TI admettent que leur entreprise est vulnérable aux attaques de l'intérieur - et 11% se disent « extrêmement vulnérables ». Les résultats contiennent plusieurs autres révélations effrayantes :

- Les erreurs des utilisateurs (40 %) constituent la principale source de craintes, suivies des utilisateurs et administrateurs malveillants (35%).
- Les entreprises du secteur des technologies sont celles qui s'inquiètent le plus des utilisateurs et administrateurs malveillants, tandis que les commerces de détail s'inquiètent le plus des erreurs des utilisateurs.
- 74% des professionnels des TI ne sont pas en mesure de détecter une menace interne avant l'exfiltration de données.
- 64% des professionnels des TI ne peuvent pas détecter une menace interne en temps réel.
- 61% des professionnels des TI ne surveillent pas les comptes privilégiés ou les comptes de services.

Selon nous, bien que toutes ces statistiques soient inquiétantes, la plus alarmante est la dernière: 61% des professionnels des TI ne surveillent pas les comptes privilégiés ou les comptes de services. Ces comptes sont largement connus – malheureusement pas seulement par les professionnels des TI, mais aussi par les pirates informatiques – comme une porte d'entrée pour accéder aux données sensibles des entreprises. Une fois ces comptes compromis, des acteurs malveillants peuvent voler des données et des identités. Cela leur ouvre également une porte pour lancer des campagnes persistantes sur plusieurs appareils et réseaux.

Selon un sondage réalisé par l'entreprise spécialisée en services de sécurité Centrify, 74% des atteintes à la sécurité des données commencent par une utilisation abusive des identifiants privilégiés.

À la lumière de cette énorme lacune en matière de sécurité, il n'est pas surprenant que les solutions de gestion des accès privilégiés (PAM) figurent au premier rang du top 10 des meilleurs projets de sécurité 2019 de Gartner. Les analystes de cette firme estiment que les projets de PAM devraient inclure à la fois des systèmes et des comptes humains et non humains. Ils devraient également supporter une combinaison d'infrastructures infonuagiques, sur site et hybrides, ainsi que des interfaces de programmation applicative (API) pour l'automatisation.

Bien que les conseils de Gartner soient pertinents, le problème est que les solutions PAM disponibles actuellement sur le marché sont très dispendieuses – au-delà du budget de la plupart des petites et moyennes entreprises (PME). De plus, celles qui peuvent se permettre l'achat d'une telle solution n'ont habituellement pas l'expertise technique interne pour comprendre les différences entre les exigences de base et les parties non essentielles d'une solution PAM.

Chez Devolutions, nous nous sommes donnés comme mission de changer cela et nous sommes donc sur le point de lancer une plateforme PAM robuste et complète, spécialement conçue pour les PME. Le lancement est prévu d'ici novembre 2019. Cliquez ici pour en savoir plus.

Conseils de notre Chef de la sécurité, Martin Lemay

Même si la technologie peut aider à prévenir, détecter et réagir aux attaques de l'intérieur, de nombreuses entreprises n'envisagent pas de contrôles non technologiques. Par exemple, une vérification périodique des antécédents criminels et du dossier de crédit par les ressources humaines devrait empêcher les personnes à haut risque d'accéder aux données sensibles et systèmes critiques de votre entreprise. Le coût d'un tel contrôle est beaucoup moins élevé que l'achat d'une solution technique.

D'autres contrôles fondés sur la séparation des tâches (SoT) et le principe de moindre privilège (POLP) ne nécessitent pas non plus de technologie spécifique. Ces principes peuvent réduire considérablement les risques d'attaque et limiter les gestes indésirables des employés malveillants et non malveillants.

Un autre élément négligé est la règle des « quatre yeux », renforcée par de solides processus de gestion du changement et d'audit. Cette dernière recommandation aidera non seulement à prévenir, mais également à favoriser la détection d'abus et de mauvaises conduites potentielles. Enfin, j'aimerais ajouter que le concept de défense en profondeur devrait être mis en œuvre en combinant des contrôles techniques et non techniques afin de limiter les risques d'attaques de l'intérieur et leurs impacts.