Quest

90 %

des entreprises se sentent vulnérables aux menaces internes[1].

Attaques internes : détectez-les, défendez-vous et restaurez votre système

Vous avez créé un système de défense du périmètre impressionnant, mais êtes-vous prêt à affronter les menaces qui se trouvent à l'intérieur de votre réseau ?

LE DÉFI

Les fuites des données font la une des journaux presque chaque semaine. Atteintes de phobie des hackers, les entreprises ont donc toujours investi massivement dans la protection du périmètre. Mais en réalité, plus de la moitié des cyberattaques sont causées par des utilisateurs qui se trouvent déjà à l'intérieur du réseau[2] : par exemple, un collaborateur qui vole une adresse IP pour son nouveau travail ou un administrateur maladroit qui fait une grave erreur de configuration. Le plus souvent, il s'agit d'un pirate externe qui prend le contrôle d'un compte légitime. Microsoft indique que, chaque jour, 95 millions de comptes Active Directory sont la cible de cyberattaques[3] et 10 millions de tentatives de connexion Azure AD sont des cyberattaques[4].

En conséquence, les experts en sécurité recommandent aux entreprises d'assumer ces failles et d'accepter d'être tôt ou tard victimes d'une intrusion sur leurs réseaux visant à endommager ou à voler leurs données stratégiques. Même les meilleurs systèmes de défense du périmètre ne peuvent pas empêcher ces attaques. Il est donc essentiel de disposer d'une sécurité et d'une gouvernance renforcée Active Directory.

L'IMPACT SUR VOTRE ENTREPRISE

Afin de lutter efficacement contre les menaces internes, vous devez :

- **Répondre aux besoins de votre entreprise de manière sécurisée avec de nouvelles technologies.** Accélérer l'accès au Cloud ou développer une politique BYOP peut vous permettre d'atteindre vos objectifs, mais vous devez minimiser les risques de sécurité.
- **Protéger vos données sensibles.** Ces dernières années, le volume des données a connu une croissance fulgurante. Pour la majeure partie, il s'agit de données non structurées dans des référentiels Cloud, comme SharePoint Online et OneDrive, tandis qu'il serait préférable de disposer de quelques bases de données dans des datacenters verrouillés situés dans le bâtiment de l'entreprise. Ainsi, il est plus difficile de savoir ce que vous possédez et plus facile de sécuriser vos données.
- **Respecter un nombre croissant de réglementations toujours plus strictes en matière de protection des données.** Il n'y a pas si longtemps, seuls certains secteurs étaient sévèrement réglementés et la certification ISO s'avérait suffisante. Désormais, les réglementations telles que la norme PCI, le RGPD et le CCPA influencent toutes les branches. Vous devez à la fois prendre des mesures en matière de conformité, mais aussi les maintenir suite à l'émergence et à l'évolution de réglementations.
- **Réussir les audits et éviter de faire les gros titres.** Une fuite des données peut entraîner des coûts catastrophiques (3,86 millions de dollars en moyenne[5]). Échouer aux audits peut donner lieu à de lourdes amendes, voire mettre votre entreprise en faillite. La protection de votre entreprise ne dépend que de vous.

Pour atteindre ces objectifs, vous devez contrôler les autorisations utilisateur et surveiller de près les actions de chacun. Toutefois, les outils natifs ne rendent pas la tâche facile. En effet, 62 % des utilisateurs admettent posséder plus d'accès qu'ils ne devraient en avoir[6]. Les solutions SIEM offrent une visibilité sur l'activité des utilisateurs, mais leur configuration et leur utilisation sont complexes, etle coût des licences est élevé. De plus, leur performance dépend des données avec lesquelles vous les alimentez. Les journaux natifs présentent également des lacunes importantes et manquent de fiabilité dans des domaines critiques. Il n'est pas surprenant que les hackers ne soient interceptés qu'au bout de 101 jours (en moyenne[7]).

1 Cybersecurity Insiders, « Insider Threat 2018 Report » (Rapport 2018 sur les menaces internes).

2 Ibid.

3 ZDNet, « Active Directory czar rallies industry for better security, identity » (Le tsar d'Active Directory se joint à la demande d'un renforcement de la sécurité et des identités exprimée par le secteur), 9 juin 2015.

4 Softpedia News, « Microsoft Sees Over 10 Million Cyberattacks per Day on Its Online Infrastructure » (Microsoft enregistre plus de 10 millions de cyberattaques par jour contre son infrastructure en ligne), 6 mai 2016.

5 Institut Ponemon, « 2018 Cost of a Data Breach Study » (Étude 2018 sur le coût des violations de données).

6 Institut Ponemon, « Closing Security Gaps to Protect Corporate Data: A Study of US and European Organizations » (Combler les lacunes de sécurité pour protéger les données d'entreprise : étude menée par les organisations américaines et européennes).

7 FireEye, « M-Trends 2018 Report » (Rapport M-Trends 2018)

« Avant, je n'avais aucun contrôle sur les modifications apportées aux groupes d'administration. Grâce à Change Auditor, je peux désormais les surveiller en toute facilité, en consultant simplement un dossier dans mes e-mails. »

— Dennis Persson, Technicien des systèmes informatiques, Region Halland

La solution incontournable en matière de sécurité et de conformité

UNE MEILLEURE SOLUTION

Et si vous pouviez limiter les dommages causés par un utilisateur, ou toute personne ayant volé ses identifiants, en veillant à ce que chaque collaborateur possède uniquement les accès nécessaires pour ses tâches ? Et si vous pouviez être immédiatement averti lors d'une opération risquée ? Et si vous pouviez établir des comportements normaux de référence pour chaque utilisateur et rapidement déceler toute déviation ? Et si vous pouviez étudier les menaces et réagir rapidement ?

CE QUE VOUS NE POUVEZ FAIRE QU'AVEC QUEST

Quest est le fournisseur de choix en matière de solutions de sécurité et de conformité pour tout environnement Microsoft hybride ou sur site. Nous proposons une suite complète de solutions qui vous permettent de sécuriser votre environnement interne aussi efficacement que votre périmètre et de garantir une conformité continue aux normes en vigueur.

Corriger et limiter les risques

Le premier système de défense contre les menaces internes est la mise en place d'une gouvernance adaptée. Les solutions Quest® permettent d'automatiser les tâches administratives,y compris le provisioning et le déprovisioning des comptes utilisateurs, afin de combler les failles de sécurité et de réduire les risques. Les workflows basés sur les approbations ajoutent une couche supplémentaire de gouvernance et de contrôle.

Identifier les vulnérabilités de manière proactive

Les environnements informatiques sont dynamiques, vous devez donc régulièrement rechercher la présence de vulnérabilités. Les solutions Quest fournissent des rapports automatisés et consolidés dans votre environnement sur site, hybride ou Cloud, afin que vous puissiez déterminer les accès de chacun et comment ils ont été obtenus. De plus, vous avez la possibilité de restreindre les autorisations à partir des rapports. Vous pouvez également connaître l'emplacement de vos données les plus sensibles afin de garantir leur protection, passer en revue vos objets de stratégie de groupe (GPO), voire empêcher la modification des objets stratégiques.

Détecter et configurer des alertes sur les activités suspectes

Les solutions Quest vous permettent également d'alerter plus rapidement en cas de menaces actives en fournissant un audit en temps réel de l'activité des utilisateurs et des administrateurs, ainsi que des alertes sur l'escalade des privilèges, les modifications inappropriées et autres activités suspectes. L'analyse avancée des comportements des utilisateurs modélise les schémas de comportement des utilisateurs et détecte les actions anormales. Vous pouvez même automatiser les réponses, comme le blocage de l'activité, la suspension de l'utilisateur ou l'annulation des modifications effectuées.

Évaluer les attaques rapidement et effectuer une restauration

Il faut environ 69 jours aux entreprises pour détecter une fuite des données[8]. Quest vous permet d'aller à la racine des incidents de sécurité avec rapidité et en toute simplicité grâce à la collecte centralisée des données et un moteur d'analyse légale et de recherche informatique semblable à Google. En outre, vous pouvez créer un laboratoire de test virtuel pour les plans de reprise d'activité et réduire le long processus de restauration des forêts Active Directory à un simple processus basé sur une interface graphique.

Maintenir et prouver la conformité aux normes en vigueur

Ensemble, ces fonctionnalités vous permettent d'établir, de maintenir et de prouver la conformité à une large gamme de réglementations. De plus, les solutions Quest proposent une compression intelligente et extensible des journaux afin que vous puissiez stocker vos données d'audit de manière économique pendant plusieurs années, et garantissent leur disponibilité pour les enquêtes et les audits de sécurité.

8 Institut Ponemon, « 2018 Cost of a Data Breach Study » (Étude 2018 sur le coût des violations de données).

Quest
quest.com/fr
Rendez-vous sur (quest.com/fr-fr/locations) pour obtenir les coordonnées de notre bureau local.

SolutionBrief-MPM_SecurityCompliance-US-FR-WL-38251