Cybersécurité : 4 pistes pour se protéger face aux menaces internes

Le coût estimé d'une violation de sécurité est en moyenne de plusieurs centaines de milliers d'euros pour une entreprise de taille moyenne.

Le préjudice moyen d'un détournement de données pour chaque entreprise victime est évalué à plusieurs millions d'euros. Le rapport sur la cybermenace, publié en mai 2019 par le ministère de l'Intérieur, dresse un constat implacable.

A l'image du piratage des données personnelles de 106 millions des clients américains et canadiens de la banque américaine Capital One Financial, ou des données personnelles de 90.000 clients allemands de Mastercard, on observe une augmentation importante du volume et de la fréquence des atteintes à la sécurité causées par des personnes présentes dans l'entreprise (initiés), imprudentes ou négligentes.
Dans son livre, Philippe Trouchaud, associé au sein du cabinet PwC estime que « 35 % des incidents sont générés par des collaborateurs internes », invitant à repenser la cybersécurité en se réappropriant l'humain.

La technologie est rarement mise en défaut. Alors quels sont les défis de sécurité posés par ces menaces d'initiés ? Comment la transition vers le Cloud a rendu encore plus difficile la protection contre ces menaces ? Quels outils sont disponibles pour aider les entreprises à protéger leurs données sensibles indépendamment de l'endroit où elles se trouvent ?

Les dangers des menaces d'initiés

Dans la plupart des cas, les initiés représentant une menace sont des employés autorisés ou des sous-traitants munis d'un code d'identification valide et disposant d'un accès physique aux bâtiments de l'entreprise : il est naturellement plus difficile pour les équipes de sécurité de se protéger face à la menace qu'ils représentent. En ayant accès à l'organisation, ils ne sont pas détectés par les mesures de sécurité périmétrique traditionnelles.

En outre, il est important de noter que toutes les menaces d'initiés ne sont pas forcément malveillantes. Dans bien des cas, il s'agit d'employés négligents qui cliquent sur des liens présents dans des courriels malveillants, ouvrent des pièces jointes nuisibles sans le savoir, utilisent un Wi-Fi public non sécurisé ou laissent accidentellement leur ordinateur portable dans un endroit public. Pour autant, ces atteintes à la protection des données peuvent avoir des conséquences graves pour l'entreprise tant sur le plan financier que pour sa réputation.

Un problème croissant au sein des environnements cloud

Avec la montée en puissance du Cloud et des applications SaaS, il est plus facile que jamais d'exposer des données confidentielles ou sensibles. De nombreux chiffres soutiennent l'idée que les incidents de sécurité impliquant des menaces d'initiés sont à la hausse.

Ainsi, plus des deux tiers (73 %) des personnes interrogées dans le cadre d'une étude menée par Bitglass ont estimé que les attaques d'initiés étaient devenues plus fréquentes au cours de la dernière année. Et 59 % ont même déclaré que leur propre organisation avait subi au moins une attaque d'initié au cours des 12 derniers mois – contre seulement 33 % l'année précédente.

Les 5 principales raisons évoquées pour expliquer ce phénomène sont les suivantes :

– Les initiés disposent d'autorisations valides

– L'utilisation croissante au sein de l'entreprise d'applications non managées

– L'accès aux données à distance

– L'augmentation du nombre d'équipements utilisateurs susceptibles d'être ciblés pour dérober des données

– Le stockage des données dans le Cloud

Quatre de ces cinq raisons sont liées au transfert de données hors site vers un nombre croissant d'appareils mobiles et d'applications dans le Cloud, avec les risques inhérents que cela engendre. Avec l'adoption massive du Bring your own device (BYOD), il est encore plus difficile pour une organisation d'assurer un environnement de données sécurisé et/ou de repérer rapidement les appareils compromis.

Face à la popularité croissante du Cloud, le périmètre de sécurité traditionnel n'est plus d'aucune utilité et l'adoption d'outils spécialisés – encore trop peu répandus en entreprise – devient une urgence. Or, 41% des personnes interrogées ont déclaré qu'elles ne surveillaient pas les comportements anormaux des utilisateurs à travers leur empreinte Cloud. Difficile dans ces conditions de pouvoir détecter une attaque d'initié le jour même où elle s'est produite.

4 actions clés à mettre en œuvre au sein des entreprises

Face aux menaces imprévisibles d'un côté, et la complexité des environnements Cloud, de l'autre, seule une solution intégrée dite « multi-couche » offre la meilleure défense aux entreprises. Elle se composera de quatre éléments essentiels :

1 – Prévention contre la perte des données (DLP) : Le DLP dans le Cloud, correctement intégré, permet aux employés de travailler quand et où ils le souhaitent, tout en préservant la sécurité des données. Une offre DLP dans le Cloud de qualité comprend le chiffrement des fichiers, la rédaction, le filigrane/traçage et d'autres outils qui permettent de s'assurer que les données sensibles restent protégées à tout moment.

2 – Contrôle d'accès et gestion des identités : Les solutions de gestion dynamique des identités qui s'intègrent aux systèmes existants, gèrent l'accès des utilisateurs et utilisent l'authentification multifactorielle, se révèlent beaucoup plus efficaces que la protection par mot de passe de base. Par exemple, si un système enregistre la connexion d'un employé à partir d'un nouveau pays dans lequel il ne s'est jamais authentifié, il peut alerter l'équipe informatique d'un comportement suspect et l'aider à sécuriser le compte avant qu'une violation ne se produise.

3 – **Automatisation**
Dans les environnements Cloud, les solutions de sécurité automatisées deviennent de plus en plus cruciales car les solutions réactives, qui reposent sur une analyse manuelle ne sont tout simplement pas assez rapides. Grâce au machine learning, les solutions automatisées peuvent identifier les comportements suspects au fur et à mesure qu'ils se produisent.
Ainsi, si un utilisateur télécharge soudainement des quantités importantes de données ou se connecte et accède aux données en dehors des heures traditionnelles de travail, ces outils peuvent utiliser une approche analytique en temps réel pour identifier les comportements anormaux et prendre les mesures correctives nécessaires.

4 – Formation
Si la technologie est considérée comme un moyen puissant au service de la sécurité d'une entreprise, il convient de ne pas négliger un autre outil efficace et beaucoup plus simple à mettre en œuvre : la formation régulière des employés. Elle favorise les pratiques les plus sûres au sein de l'entreprise et contribue ainsi à minimiser la menace de vol de données en rappelant aux collaborateurs la gravité et les conséquences du vol ou du détournement des données – que ces actions soient intentionnelles ou non.

Travail à distance et Cloud bouleversent non seulement la façon de travailler, mais aussi l'organisation des entreprises. Ils engendrent également de nouveaux défis en terme de sécurité, à commencer par les menaces d'initiés. Les entreprises doivent veiller à comprendre les risques modernes auxquelles elles sont désormais exposées, et y faire face avec les outils adaptés. Ainsi elles pourront continuer à profiter pleinement des avantages du Cloud tout en garantissant la sécurité des données.