Cybersécurité : Active Directory, PAM et Zero Trust, un trio gagnant ?

Comment la crise sanitaire (Covid-19) impacte l'activité des équipes informatiques en charge de la gestion des identités ? C'est la question posée à 1 216 professionnels IT dans le cadre d'une étude* internationale publiée par One Identity, filiale de Quest Software.

Quels sont les principaux résultats ?

37% des répondants ont cité les changements qui bousculent la gestion des services Microsoft d'identité d'entreprise Active Directory (AD) et Azure Active Directory (AAD).

À l'ère de la massification du télétravail, des budgets serrés (34%), ainsi que les difficultés pour faire face à l'évolution de profils utilisateurs (30%) sont d'autres défis à relever.

Les professionnels interrogés ont aussi mentionné les défis de sécurité (27%) et de conformité (27%) amplifiés par la crise sanitaire de 2020. Ils ont été surpris, de plus, par l'inadaptation de la stratégie cloud (citée par 26% du panel), des programmes administrateur d'accès à distance (24%) et d'authentification multifacteur (multi-factor authentication, MFA) de leur organisation (20%), face à l'ampleur des bouleversements.

Cloud oui, mais…

89% ne sont pas sereins à l'idée de stocker des identifiants dans le cloud. Pourtant, si 29% des répondants disent n'y stocker aucun identifiant business, 71% déclarent le faire.

Parmi eux, 45% utilisent des services de gestion de clés cryptographiques de fournisseurs de services cloud (AWS KMS, Azure Key Vault, Google Cloud KMS, etc.). 35% s'appuient sur des gestionnaires de mots de passe « as-a-service » (LastPass, Dashlane, KeePass…), 17% utilisent des modules matériels de sécurité (hardware security modules, HSM) hébergés dans un cloud public. Enfin, 13% disent opter pour des solutions en tant que service (SaaS) de gestion des accès à privilèges ou PAM (privileged access management).

Par ailleurs, lorsqu'ils sont interrogés sur leurs priorités des derniers mois, 62% donnent l'avantage aux investissements dans le cloud (62%). La gestion du cycle de vie des identités (57%), l'automatisation des processus et des workflows associés à la gestion des identités (55%), ou encore l'octroi/annulation d'accès via AD et AAD (48%), arrivent ensuite.

L'optimisme, relatif, est à conforter.

AD, PAM et Zero Trust

Une fois passés les premiers chocs de la crise, 66% se sont déclarés « un peu » ou « beaucoup plus » confiants dans l'efficacité du programme de gestion des identités de leur organisation. 60% le disent aussi pour la sécurité et la gestion des comptes à privilèges.

Pour Bhagwat Swaroop, président de One Identity, « face à l'essor rapide d'Azure et du cloud, AD et AAD sont aujourd'hui des points de départ logiques pour toute organisation qui souhaite mettre en œuvre un modèle de sécurité Zero Trust ». L'approche dite de zéro confiance vise à « toujours vérifier » avant d'autoriser ou de bloquer un accès.

Mais « AD n'est pas équipé pour répondre aux exigences d'une architecture Zero Trust. Le système n'est pas non plus capable de stocker, générer et gérer les informations d'identification à privilèges comme le ferait une solution PAM classique », a ajouté le dirigeant. Pour résoudre ces problématiques, le fournisseur américain de solutions recommande donc aux entreprises de se tourner vers les accès à privilèges temporaires, et d'associer une technologie PAM robuste à leur programme de gestion et de workflow AD.

L'enquête a été menée par Dimensional Research. 1 216 responsables de la sécurité informatique ont été interrogés entre le 20 août et le 3 septembre 2020. États-Unis, Canada, Royaume-Uni, Allemagne, France, Benelux, pays scandinaves, Australie, Singapour et Hong Kong sont couverts (source : « One Identity Global Study 2020 – Barriers to Adoption of Zero Trust »).

(crédit photo © Shutterstock)