Accès à privilèges : l'angle mort de la cybersécurité

Les entreprises tardent à consolider leur approche de la gestion des accès à privilèges (PAM). C'est l'enseignement d'une enquête internationale promue par One Identity.

Le sondage a été mené pour l'éditeur spécialisé de gestion des identités et des accès (IAM) par Dimensional Research. 1005 professionnels de la sécurité informatique ont été interrogés dans sept pays : France, Allemagne, États-Unis, Canada, Singapour, Hong Kong et Australie. Tous exercent dans des entreprises de 500 à plus de 5000 employés.

Résultat : le partage d'accès et comptes à privilèges (d'administrateur) est « courant ». 46% des répondants déclarent que leur organisation partage des accès privilégiés avec des partenaires, sous-traitants et fournisseurs. Et 20% déclarent le faire régulièrement.

De surcroît, 75% disent partager parfois des mots de passe privilégiés en interne. Et 31% que leur organisation utilise des méthodes manuelles pour gérer les comptes à privilèges… Une porte ouverte au détournement ?

One Identity rappelle que le vol d'identifiants est l'un des moyens les plus simples pour les individus « mal intentionnés » d'infiltrer le réseau d'une entreprise.

L'éditeur américain, qui prêche pour sa paroisse IAM, ajoute que la situation n'est guère plus satisfaisante pour l'accès utilisateur. Dans l'Hexagone, en particulier.

France à la traîne

En France, 50% des répondants déclarent que leur organisation met plusieurs heures avant de bloquer l'accès de salariés sur le départ aux systèmes de leur organisation.

Seuls 13% déclarent un blocage d'accès en quelques minutes après le départ d'un employé. Contre 24% en Allemagne, 31% en Amérique du Nord et 34% à Singapour.

Or, le risque d'exposer des données sensibles au détournement, voire à l'inflitration du réseau, augmente avec l'extension des délais de blocage d'accès utilisateur.

Pourtant, la crainte d'une exfiltration de données de l'entreprise par des initiés est bien réelle. Et 77% des professionnels de la sécurité IT eux-mêmes déclarent qu'il leur serait facile de détourner des données sensibles de leur organisation.

12% reconnaissent même qu'ils seraient prêts à passer à l'acte s'ils le jugeaient utile…

(crédit photo © Shutterstock)