Cybersécurité : l'approche Zero Trust gagne du terrain

Les organisations qui ont adopté un service ZTNA (zero trust network access) sont encore minoritaires. Mais la majorité s'oriente vers la « confiance zéro » en matière de sécurité réseau. C'est ce que montrent les résultats d'une *enquête américaine promue par Zscaler.

15% des décideurs informatiques et professionnels de la sécurité IT interrogés ont déjà adopté l'approche Zero Trust de la sécurité réseau. 19% ont engagé le processus et 44% envisagent de le faire pour protéger l'accès aux applications internes à leur organisation.

De surcroît, 59% prévoient de s'appuyer sur un service ZTNA dans les 12 prochains mois. En revanche, 41% n'ont toujours pas de projet dans ce domaine.

Les services d'accès sécurisés basés sur un périmètre défini par le logiciel (SDP), ou services d'accès réseau zero trust (ZTNA), établissent une autorisation d'accès utilisateur au niveau de l'application. Ces services fournissent ainsi une alternative à l'accès à distance « classique » par réseau privé virtuel (VPN) aux applications métiers.

Quels sont les enjeux ?

Authentification multi-facteurs

Les organisations qui ont opté pour une approche Zero Trust le font en priorité pour réduire l'accès inconsidéré de collaborateurs et de partenaires aux applications métiers (pour 66% du panel). Elles le font aussi pour limiter l'exposition d'applications privées sur Internet ou à des utilisateurs non autorisés (55%). Elles apprécient, enfin, que l'autorisation n'implique pas un accès direct au réseau interne (44%).

Les priorités de sécurité d'accès aux apps internes hébergées dans un datacenter dédié ou dans le cloud public sont : l'authentification multi-facteurs et la gestion des comptes à privilèges (pour 68% des répondants) ; la détection et la réponse aux activités douteuses (61%) ; la sécurisation de l'accès à partir de terminaux personnels non gérés par l'IT (57%).

Seule ombre au tableau pour Patrick Foxhoven, CIO du fournisseur de solutions de sécurité en mode cloud Zscaler, 53% des équipes pensent que leurs technologies existantes (Legacy) permettent de limiter le risque. « Bien qu'il soit encourageant de voir autant d'organisations prêtes à s'appuyer sur le ZTNA pour combler le fossé de sécurité créé par les VPN, je suis surpris de constater que plus de la moitié des professionnels interrogés pensent que leur infrastructure actuelle est suffisamment fiable pour protéger l'entreprise. »

**L'enquête a été menée durant l'été 2019 par Cybersecurity Insiders pour Zscaler auprès de 315 décideurs et professionnels de l'IT et de la cybersécurité aux États-Unis (source : Zero Trust Adoption Report 2019).*

(crédit photo © shutterstock.com)