Cybersécurité : comment le Zero Trust monte en puissance

Les entreprises sont plus nombreuses à adopter la « confiance zéro » (Zero Trust) en matière de sécurité réseau. C'est ce que montrent les résultats d'une enquête américaine publiée par Deloitte. Plus de 595 décideurs IT et métiers ont été interrogés en juillet.

Une minorité (18,4% des professionnels interrogés) juge que le rythme d'adoption a décéléré. 35,2% des répondants considèrent que l'engagement dans ce domaine est resté stable. En revanche, pour le plus grand nombre (37,4%), l'adoption de l'approche Zero Trust au sein de leur organisation s'est accélérée depuis la pandémie de Covid-19.

Le Zero Trust consiste à « ne jamais faire confiance » et « toujours vérifier » avant d'autoriser ou de bloquer un accès aux applications et microservices de l'entreprise.

« Toujours vérifier »

Quels sont les principaux moteurs d'adoption du Zero Trust ?

Pour 35,7% du panel, il s'agit en priorité de la gestion des risques liés aux collaborateurs, notamment les initiés et tous ceux qui travaillent à distance.

Près de 25% des répondants ont cité la gestion des risques liés aux tiers (fournisseurs, prestataires…). La gestion des risques liés au cloud (20,9%) arrive ensuite.

Quels sont les freins à la diffusion du Zero Trust en entreprise ?

Le déficit de compétences internes (pour 28,3% des répondants) et des budgets serrés (28,1%) sont les obstacles les plus souvent mentionnés.

Selon le rapport, moins de 13% des professionnels ont mentionné une incapacité à « discerner par où commencer » ou à différencier les technologies ou les fournisseurs.

(crédit photo via Pixabay)