Accès distants : un bilan contrasté pour les DSI

La firme de cybersécurité Fortinet a livré les résultats d'une étude* d'impact du télétravail sur l'IT et la sécurité. 122 directeurs des systèmes d'information (DSI) et profils techniques d'entreprises de 1000 à plus de 50 000 collaborateurs ont été interrogés en France.

66% disent que leur organisation est « plutôt ou très protégée ». Cependant, avec la généralisation du travail à distance, 34% considèrent le risque de sécurité « très important » (un taux en hausse de 11 points par rapport à la période pré-pandémique).

Les applications métiers dans le cloud, déployées et utilisées dans l'ombre de l'IT (Shadow IT), sont un autre sujet de préoccupation, devant les applications de stockage et partage de fichiers, y compris lorsque celles-ci sont approuvées par la direction SI.

En outre, 81% pensent que le BYOD (Bring your own device), ou l'utilisation de terminaux personnels à des fins professionnelles, et le CYOD (Choose your own device), ou le choix parmi des terminaux listés, financés et maintenus par l'entreprise, renforcent la tendance.

SD-WAN et authentification forte

Un tiers des répondants deplorent la vulnérabilité de leur entreprise face aux attaques par hameçonnage (phishing) et rançongiciels (ransomwares), entre autres. Interrogés sur les solutions utilisées pour réduire le risque, les équipes IT citent le plus souvent la :

1. Sécurité des accès par token et authentification forte (citée par 59% des répondants)
2. Protection du cloud privé et public (59%)
3. Sécurité des flux par réseau privé virtuel ou VPN (50%)
4. Sécurité des sites distants par SD-WAN (Software defined wide area network) (31%)
5. Protection EDR (Endpoint detection and response) des terminaux (30%)

* L'enquête a été menée en ligne pour le compte de Fortinet par Visionary Marketing en avril et mai 2021.