

Cybersécurité : comment les RSSI ont affronté la crise

Le [Cesin](#) (Club des experts de la sécurité de l'information et du numérique) a dévoilé les résultats de sondages* menés en 2020 auprès de ses membres. Confrontés à la bascule des équipes vers le travail à distance en période de Covid 19, ils se sont adaptés.

Durant le premier confinement, seules 25,7% des entreprises concernées disposaient d'un nombre suffisant de PC portables pour équiper leurs collaborateurs appelés à télétravailler. Parmi les organisations qui n'étaient pas prêtes pour le télétravail massif du personnel salarié, 50,8% disent avoir acquis et déployé, dans l'urgence, de nouveaux laptops. Et 38,7% ont migré des postes fixes vers le domicile de professionnels.

Qu'en est-il de la protection de ces postes de travail ?

28,7% des entreprises disent appliquer strictement l'approche [Zero Trust](#) (zéro confiance) en matière de cybersécurité. L'utilisateur n'a donc aucun droit d'administration de son poste de travail. Pourtant, 75% des répondants acceptent de gérer des exceptions. Une minorité déclare même que les utilisateurs sont administrateurs de leur poste.

Windows équipe l'essentiel du parc PC en entreprise. Or, 26,15% des organisations accordent aux utilisateurs sous Windows 10 un accès libre au store de Microsoft. Les employés peuvent ainsi installer toute application disponible dans le store, que l'application soit ou non validée par leur direction des systèmes d'information (DSI).

En revanche, 33,3% des entreprises ont bloqué l'accès au store de la firme de Redmond. 40% des organisations, enfin, privilégient un store applicatif d'entreprise.

VPN et authentification multifacteur

80% des sociétés concernées ont opté pour le chiffrement de leur parc de postes mobiles. 51% ont choisi de chiffrer ce parc dans son intégralité, 29% l'ont fait pour une partie.

La migration accélérée vers le cloud est un autre enjeu.

« Depuis le début de la crise, le *move-to-cloud* s'est accéléré sous ses différentes formes, de l'hébergement en mode IaaS, des services PaaS et des solutions en mode SaaS », a souligné le Cesin présidé par [Mylène Jarossay](#) (RSSI de LVMH).

Fallait-il « se connecter directement aux applications SaaS – parmi elles les outils collaboratifs en ligne – ou bien passer toujours par la case 'bureau' en empruntant un VPN (virtual private network) pour rejoindre le réseau d'entreprise. VPN systématique ou pas ? Et si oui, comment s'assurer de qui se connecte et avec quel *device* ? »

75% des entreprises optent pour l'authentification multifacteur (MFA). Parmi elles, 24% l'activent systématiquement, que le terminal soit présent dans ou hors du réseau, qu'il soit connecté en

direct sur le cloud ou via un réseau privé virtuel (VPN).

★
« *Les Instantanés 2020 du CESIN* ».

(crédit photo via Pexels)