Télétravail de masse : les premières mesures à prendre pour la cybersécurité

Valéry Marchive, Rédacteur en chef

Faire passer en masse des utilisateurs au télétravail est un énorme défi pour de nombreuses entreprises, notamment en matière de cybersécurité. Et pourtant, de nombreuses organisations sont confrontées à cette situation, dans le contexte de pandémie. Face à cela, les recommandations se multiplient.

Informative dresse une liste de dix conseils à l'intention des DSI. L'agence nationale pour la sécurité des systèmes d'informations (Anssi) vient de publier les siens, de même que le Cesin. Un épisode du podcast *No Limit Secu* vient d'être consacré au sujet. L'institut SANS s'est également mobilisé, avec notamment un kit de déploiement à télécharger gratuitement, pour les RSSI, et liste de contrôle, pour les utilisateurs. Et en tête de liste des conseils se trouve, la formation et la sensibilité de ces derniers.

Pour beaucoup, ce ne sera pas une surprise : la sensibilisation est le premier effort à conduire pour obtenir des gains significatifs, selon les retours d'un appel à suggestions lancé récemment par Matthieu Garin, de Wavestone. Le but est là d'aider à lutter contre les tentatives d'arnaques en tout genre – et notamment au président – ou encore de hameçonnage. Et cela peut notamment être l'occasion de (re)diffuser le kit de sensibilisation de Cybermalveillance.

Vient ensuite l'analyse de la sécurité des accès distants déployés dans l'urgence, entre vérification des configurations, tests d'intrusion, vérification des règles de pare-feu, etc. En troisième position s'inscrit la mise en place d'une gouvernance de crise spécifique à la sécurité du système d'information, devant le renforcement tactique des capacités de surveillance, entre gestion des journaux d'activité, mise en place d'outils de prévention des fuites de données (DLP), ou encore contrôle d'un Shadow IT qui risque de menacer plus que jamais. Car si le monde de la sécurité se souvient que des tableaux Trello mal configurés ont pu être à l'origine d'expositions de données, les utilisateurs n'en ont probablement même pas conscience.

Et puisqu'il ne faut pas oublier la gestion des correctifs – et encore plus de ceux qui seront téléchargés et déployés sur les postes de travail distants –, il convient d'ajuster la configuration VPN en conséquence afin d'éviter que les plus gros correctifs ne saturent inutilement la bande passante.

Vient ensuite la mise en place d'un helpdesk dédié à la sécurité, visant à décharger le support IT – qui ne manquera pas d'être bien occupé – des sujets relatifs à la sécurité. Et puis il faut compter avec les besoins des activités où la dématérialisation ne s'est pas pleinement faite. Ce qui impliquera de permettre l'impression locale, mais également de sensibiliser les utilisateurs à la manière de gérer ces sorties papiers dans la durée, au-delà de la crise.