Pourquoi les professionnels négligent-ils souvent la cybersécurité ?

Plus que jamais, les professionnels sont exposés à des risques non-négligeables liés à la cybersécurité. Cependant, les moyens appliqués dans la majorité des entreprises sont paradoxalement insuffisants. Comment expliquer ce phénomène ? Qu'est-ce qu'un VPN et pourquoi parler de « recommandation essentielle » ? Voici un article complet répondra à ces interrogations.

La cybercriminalité, un problème majeur pour les professionnels

Le hacking en perpétuelle croissance sur le web

Le cybersécurité et le hacking sont des sujets devenus bien plus préoccupants depuis ces dernières années. En effet, l'évolution du web au sein de la société rend aujourd'hui inévitable le transfert de fichiers. Ainsi, l'envoi d'un e-mail ou le partage de dossiers via une plateforme drive facilite la communication entre les professionnels et leurs clients.

Or, ces données précieuses sont particulièrement visées par les pirates. Certains cas font également mention de « sabotages volontaires » afin d'éliminer la concurrence. Bref, tous les coups sont permis sur internet où les chances de retrouver le responsable sont quasi nulles.

Les risques encourus par les professionnels

La fuite de données

Le premier scénario fréquemment constaté est lié à la fuite de données lors d'un transfert (ou depuis le périphérique de stockage). En tant que professionnel, ces informations peuvent parfois représenter un temps de travail conséquent. Les ransomwares (tentatives de racket) sont malheureusement fréquents dans ce type de situations.

La propagation de virus auprès des clients

La récupération de fichiers indésirables (virus ou malwares) ralentit ou empêche l'utilisation de l'appareil infecté. De plus, le partage de ces données auprès des clients peut être désastreux pour l'image d'une société.

La perte définitive d'une base de données

Dans certaines situations, il est également possible de perdre totalement toutes les informations stockées sur un ordinateur, smartphone ou tablette. Les conséquences évoquent souvent un chiffre d'affaires en baisse devant l'urgence d'une réorganisation.

Des faits inquiétants

D'après un article du Journal du Dimanche, la prise de conscience de ces risques se développe auprès des entrepreneurs. La réactivité est d'ailleurs une problématique puisque 2 à 5 jours sont souvent nécessaires pour confirmer le hacking réalisé sur l'appareil d'un professionnel. Or, ce laps

de temps est souvent trop important pour préserver des données sensibles.

Le ransomware « Petya » a particulièrement marqué les esprits des entrepreneurs. En 2007, ce virus attaqua le système informatique de Saint-Gobain jusqu'à paralyser la facturation de la société. Quelques semaines plus tard, le groupe déclara une perte de 220 000 euros sur son chiffre d'affaires ! Un résumé présenté sur le site de Sudouest.fr vous en dira davantage.

Cependant, malgré tous ces scénarios inquiétants, peu d'entreprises mettent en place des moyens suffisants pour garantir leur sécurité. Comment expliquer ce phénomène ?

Le budget : l'obstacle principal des entrepreneurs

Sans surprise, le budget alloué à la sécurité des systèmes informatiques de professionnels est le facteur principal d'une vulnérabilité. Pour un entrepreneur, il est toujours difficile d'investir sans pouvoir retrouver une rentabilité. En effet, à l'instar d'un service de sécurité, par exemple, la mise en place d'un système de cybersécurité n'engendre aucune productivité supplémentaire. Or, la réduction de risques onéreux reste un « argument de taille ».

Parfois, le manque de budget oriente les entrepreneurs vers des stratégies inefficaces ou perfectibles. Effectivement, la cybersécurité est un domaine encore trop incompris par les néophytes et nécessite souvent des connaissances basiques.

Pourtant, une solution financièrement et techniquement accessible est parfois omise : l'utilisation d'un VPN.

Qu'est-ce qu'un VPN et comment l'utiliser dans un contexte professionnel ?

La définition et les fonctionnalités d'un VPN

Un VPN est un réseau privé virtuel. Celui-ci peut être localisé sur différents continents en fonction du choix de l'utilisateur. L'objectif principal de cette solution est de modifier les informations de connexion afin de préserver l'anonymat et la sécurité de l'internaute. Certaines fonctionnalités supplémentaires viennent renforcer ces « bienfaits » :

- Le masquage de l'adresse IP grâce à l'utilisation de divers systèmes DNS (Domain Name System)

- Le chiffrage des informations partagées lors de chaque interaction sur le web grâce à un protocole de cryptage

En toute logique, ces fonctions sont particulièrement utiles pour protéger des données professionnelles. De plus, les frais d'abonnement pour ce type de services restent accessibles aux amateurs ou entrepreneurs.

Les réseaux privés virtuels et les appareils Android

Les VPN sont conçus pour fonctionner sur tous types d'appareils. Les smartphones ou tablettes Android des professionnels pourront ainsi profiter de cette protection. Avec de tels risques liés à la cybercriminalité, les réseaux privés virtuels méritent amplement d'être conseillés.

Pour résumer

Malgré de nombreuses menaces évoquant des conséquences inquiétantes, le budget réservé à la cybersécurité est trop souvent insuffisant au sein des entreprises. Néanmoins, l'accessibilité des VPN peut être une réponse adaptée aux besoins des professionnels.