ZENDATA
DON'T BE THE NEXT ONE

Recommandations sécuritaires

Alors que nombre d'entre nous vont être amenés à devoir travailler en « Home Office », nos organisations se précipitent pour déplacer leur activité de travail à la maison. Les cyber-criminels de leur côté innovent et adaptent leurs tactiques pour profiter que certains déploiements sont dépourvus d'une sécurité adéquate. Il est heureusement possible de sécuriser correctement du « Home Office », mais cela ne s'improvise pas et dans l'empressement lié au COVID-19 beaucoup de configurations sont malheureusement problématiques.

Il y a plusieurs points fondamentaux à considérer lors de la mise en place du télétravail :

La sécurisation des postes de travail – en amenant du travail sur son ordinateur personnel, que ce soit en direct ou virtuellement (avec Citrix, RDP, etc.) il faut le protéger correctement et limiter son accès. Assurez-vous de l'utilisation de mot de passe fort et unique sur les appareils, de ne pas utiliser un compte administrateur pour faire vos activités quotidiennes et qu'il ait les outils de sécurité de base (antivirus, firewall, mise à jour) correctement configurés. Il est aussi commun que les enfants et adolescents installent des jeux à réputation discutable ou des logiciels piratés qui peuvent infecter votre ordinateur ; il faut donc correctement y limiter l'accès.

La protection de son wifi – lorsqu'on connecte un ordinateur à du Wifi, il est directement en contact avec tous les autres appareils sur le même wifi et s'expose à de nouveaux risques si ces appareils sont vérolés ou malveillants. Il est donc impératif de correctement protéger le wifi auquel vous vous connectez avec un mot de passe fort et de vous assurer que seules des personnes de confiance le connaissent. Il est donc à fortiori encore plus dangereux lorsqu'on se connecte à un wifi ouvert, public ou gratuit.

La résidence des données – beaucoup de métiers, dont celui des avocats, sont soumis à des régulations très strictes. Celles-ci peuvent inclure la territorialité des données en Suisse, l'accès aux informations uniquement depuis des appareils sécurisés ou encore l'assurance de l'exécution de certaines procédures. Il est donc opportun de vérifier les contrats et accords avec vos clients avant d'autoriser du télétravail ainsi que de mettre en place une granularité d'accès adéquate.

Le facteur humain - Les collaborateurs travaillant à domicile ou sur leur smartphone sont facilement distraits, surtout lorsqu'ils sont habitués à travailler au bureau. Ils risquent d'utiliser leur email personnel pour transmettre du contenu de travail et de rapidement pivoter entre leur vie professionnelle et privée engendrant ainsi une navigation web potentiellement dangereuse ou le clic sur des liens malveillants.

Vous devez systématiquement verrouiller votre ordinateur, utiliser les moyens de communication (email, Teams, SMS, iMessage, WhatsApp, Signal, weTransfer, etc.) approuvés par l'étude et traiter avec le même soin qu'au bureau, les informations confidentielles. Il faut faire attention aux documents imprimés ainsi que de s'assurer de leur destruction si tel est la procédure.

Les Études d'avocats sont un élément essentiel du tissu économique genevois, mais aussi une cible privilégiée par les hackeurs qui doivent donc se protéger de façon adéquate et proportionnée à cette menace.