FINANCIAL
INTELLIGENCE
& PROCESSING

Les cybercriminels sont déjà au télétravail !

Le placement en confinement de la population afin de limiter le plus possible la propagation du virus a précipité le télétravail pour de nombreuses entreprises qui n'y étaient pas forcément préparées.

L'adaptation des postes informatiques pour permettre une connexion extérieure au système informatique des entreprises a été souvent faite dans l'urgence. Pour celles pour lesquelles des procédures de télétravail et les matériels adaptés avaient été mis en place avant le confinement, seul l'accroissement des capacités a été nécessaire en vue de faire face à l'augmentation du nombre de télétravailleurs.
Le constat est bien différent pour les entreprises qui, suite au confinement, ont dû improviser en toute hâte des solutions pour assurer leur continuité d'exploitation.

Les failles de sécurité sont alors multiples. Quelques exemples parmi les plus sérieuses :

- L'utilisation de l'ordinateur personnel du salarié à vocation familiale;
- L'utilisation d'une connexion Wifi mal sécurisée et partagée avec les voisins;
- La mise en place de protocoles de communication informatique antédiluviens non sécurisés et non chiffrés;
- Du personnel non formé aux règles de sûreté informatique dans des conditions dégradées.

Tout ceci est « pain béni » pour les cybercriminels qui, eux, n'envisagent pas un seul instant de mettre en pause leur « business ».
Ils surfent déjà sur la vague du coronavirus avec des campagnes de mailing frauduleux ou la diffusion d'applications compromises (modifiées et qui désormais intègrent un malware caché), afin de prendre le contrôle des ordinateurs. À chaque évènement majeur, les criminels se servent de l'actualité pour diffuser de tels malwares en utilisant les ressorts psychologiques de la peur. Ils pourraient alors attaquer le système d'information de l'entreprise pour soit voler des informations sensibles qu'ils pourront ensuite monétiser, soit installer un ransomware. →

Pour réduire ces risques, il existe un certain nombre de bonnes pratiques :

■ Vous devez impérativement fournir à chaque salarié en situation de télétravail, un ordinateur portable à usage exclusif professionnel. Cet ordinateur doit contenir une solution antivirus efficace et mise régulièrement à jour ainsi que le chiffrement des données afin de les protéger en cas de vol du matériel.

■ Utiliser une connexion VPN. La connexion du salarié au système d'information de son entreprise doit être sécurisée. Un VPN va cacher l'activité en ligne de votre entreprise et vous protéger vous et vos salariés des cybercriminels en cachant le trafic de vos données à travers un tunnel crypté. Le firewall matériel possède aussi la plupart du temps une fonction VPN qu'il suffit d'activer. Ainsi, ces solutions sont abordables pour toutes les entreprises.

■ Le service informatique ou l'infogérant doit veiller à l'installation des mises à jour du système d'exploitation et des applications. Les mises à jour ont pour principale fonction de combler les failles de sécurité qui ont été identifiées. Nous pouvons rappeler que le fonctionnement des malwares repose sur l'exploitation de ces failles de sécurité. Une fois ces failles comblées, les malwares qui l'exploitent ne sont plus des menaces.

■ Veiller à la sauvegarde périodique des données des utilisateurs sur des supports amovibles comme des clés USB.

■ Demander à vos salariés d'utiliser dans le cadre professionnel des mots de passe uniques et dans un format différent des mots de passe qu'ils utilisent pour leur usage personnel. Certains sites ou services en ligne enregistrent en clair les mots de passe associés aux comptes utilisateurs. Les pirates ont depuis longtemps pris l'habitude de tester sur tous les services en ligne les couples login & mot de passe qu'ils ont récupéré afin d'obtenir des accès.

■ Demander encore plus de vigilance qu'à l'accoutumée à vos salariés sur les sollicitations par courriel ou par téléphone. Toute demande inhabituelle doit obligatoirement passer par une validation auprès de sa hiérarchie par un autre canal de communication que celui utilisé par la sollicitation.

■ La mise à jour de la charte d'utilisation du matériel informatique. Ce document doit être une référence pour les salariés qui doivent pouvoir s'y rapporter en cas de doute. Il leur rappelle ce qu'il est autorisé de faire sur le poste mis à leur disposition et en quelles circonstances. Il convient aussi de s'assurer que des préconisations spécifiques au télétravail y figurent et, le cas échéant, les ajouter. Enfin, il ne sera pas vain de rediffuser cette charte. ■

FIP en bref

FIP est un cabinet de conseil indépendant fondé en 2005 et réunissant les compétences d'experts de l'ingénierie financière, de l'examen de fraude, de l'investigation et de l'évaluation des préjudices. FIP a développé une expertise reconnue dans le décryptage d'organisations juridiques offshore et de transactions financières opaques mises en place afin de détourner des actifs et d'en dissimuler les bénéficiaires ultimes. FIP intervient à tous les niveaux de la lutte contre la criminalité financière, aussi bien de manière préventive que réactive.

Notre indépendance garantit le respect strict de la confidentialité des informations qui nous sont communiquées par nos clients.

Nos expertises

- **Due Diligence** pré-investissement
- **Pré-qualification** et conformité des partenaires
- **Recherche d'éléments de preuve** dans tout contexte de litige commercial ou patrimonial
- **Expertise financière** dans le cadre de litiges ou d'arbitrage
- **Prévention des risques** de fraude et de corruption
- **Enquête interne** indépendante et examen de fraude
- **Investigation numérique** et audit de sécurité informatique
- **Assistance aux huissiers** (constat et Art. 145 du CPC)
- **Recherche d'actifs** saisissables