Le télétravail a facilité la tâche des cybercriminels qui sévissent entre fraudes et hameçonnages

CYBERATTAQUES EN FORCE

« THIERRY JACOLET

Télétravail » En ces temps de pandémie, il y a une catégorie d'infectés un peu oubliée: les ordinateurs. Depuis le début de la pandémie, les hackers (pirates informatiques) profitent de l'avènement du télétravail pour multiplier les cyberattaques contre les utilisateurs, avec une préférence pour les privés et les PME. Explications.

Avec le télétravail, l'employé est plus que jamais le point faible du système informatique de l'entreprise. Keystone

1 Quelle est l'ampleur des cyberattaques?

«Depuis le début de la pandémie, nous constatons une augmentation des attaques ciblant tant les sociétés, les administrations que les privés, avec une utilisation accrue de *ransomwares* (logiciel de rançons) et de *phishing* (captation de données)», observe Guillaume Saouli, directeur de Sémafor Conseil SA, société basée à Pully et active en cybersécurité. Ce que confirme Steven Meyer, directeur de Zendata, une entreprise spécialisée en cybersécurité, à Genève, chiffres à l'appui: «Dès le mois d'avril 2020, nous avons observé en temps réel une augmentation de l'activité criminelle de 400%. Ce niveau est resté la norme jusqu'à aujourd'hui.»

Cette envolée se traduit aussi dans le nombre d'annonces de cybermenaces et de demandes de renseignement du public enregistré par le Centre national pour la cybersécurité (NCSC): entre 2019 et 2020, ce nombre a doublé pour atteindre 10 606 unités. Si cette progression est attribuée notamment à une plus grande sensibilité de la part des entreprises et des individus, «seule une partie des cas est portée à notre connaissance», reconnaît Gisela Kipfer, responsable médias. «Nous observons une évolution notable des attaques qui cherchent à tirer parti de la pandémie.»

2 Quel est le rôle joué par le télétravail?

Un jeune télécharge un jeu illégalement sur l'ordinateur familial. Le hic, c'est que son père utilise cette bécane pour travailler sur le serveur de son entreprise. Mal protégé, l'outil informatique laisse apparaître des failles dans lesquelles s'engouffre un hacker. Celui-ci va entrer dans le serveur et rafler les données sensibles, censées être sécurisées. Un dérapage typique que la société Zendata a dû gérer depuis que le télétravail s'est imposé il y a un an.

«Dans ce cas précis, c'est en surveillant le darknet que nous avons découvert en temps réel que des hackers étaient en train de vendre les accès de l'entreprise», se souvient Steven Meyer. «Nous avons pu avertir le client, une grande société genevoise, qui a changé tous les codes d'accès à temps.» D'autres entreprises n'ont pas eu cette chance: certaines ont perdu des données importantes, d'autres ont dû fermer leurs portes, témoigne le spécialiste.

Avec le télétravail, le réseau des entreprises a été étendu à un environnement privé souvent moins sécurisé. «La surface d'attaque a été augmentée», avance Alexis Roussel, directeur des opérations de la société Nym Technologies SA, une entreprise basée à Neuchâtel qui construit un réseau de protection de la vie privée. «Chaque nouvelle connexion informatique est une porte d'entrée potentielle pour une personne malveillante.»

L'employé n'a jamais été autant le point faible du système informatique de l'entreprise, d'autant que les utilisateurs n'adoptent pas toujours les bonnes pratiques à distance. «Ils n'utilisent pas forcément les logiciels prévus par l'entreprise, par exemple en téléchargeant des films aux origines douteuses, et la mise à jour des objets connectés n'est pas forcément faite régulièrement», souligne Guillaume Saouli.

«Sur Zoom, les cybercriminels peuvent aller espionner»

Guillaume Saouli

Les nouvelles habitudes de communication offrent aussi des opportunités aux cybercriminels. «Sur Zoom, on peut aller espionner, chercher des données, perturber les conversations. Les usages sur ce genre de réseau ne sont pas toujours judicieux car les gens partagent leurs ressources, leur clavier, leur souris», complète Guillaume Saouli.

3 Quels sont les types d'attaques?

Les cyberattaques de type BEC (Business Email Compromise), ou compromission d'e-mails, sont aujourd'hui les plus fréquentes. Un clic d'un employé sur un courriel frauduleux suffit au pirate pour pénétrer sans effraction dans le réseau. Les messages dits d'hameçonnage sont, après les fraudes, la méthode la plus courante en Suisse.

Ces dernières semaines, le NCSC a reçu des annonces concernant des courriels frauduleux au nom de l'administration des douanes, du chantage à l'attaque à l'acide ou des messages de *sextorsion*. L'organisme fédéral conseille d'ignorer ces messages.

4 Comment renforcer les entreprises?

Des milliers d'entreprises ont dû s'équiper à la va-vite pour faciliter la transition vers le nomadisme. Malgré les ajustements ultérieurs, elles n'ont pas pu bétonner entièrement la sécurité. Même la fourniture du matériel informatique et de logiciels n'est pas une assurance anticyberattaques. Prenons le VPN que conseille le CNSC, cette connexion censée être sécurisée entre l'ordinateur et le serveur distant sur lequel l'employé travaille. Il suffit d'une simple mauvaise configuration pour mettre en danger l'entreprise.

Pour éviter au maximum les mauvaises surprises, Guillaume Saouli préconise le système «zéro confiance», qui vise à empêcher tout accès non autorisé et à restreindre les données mises à disposition par l'entreprise. «On n'utilise que les données dont on a besoin», précise-t-il. «Par exemple, un employé des ressources humaines ne consulte depuis chez lui que les dossiers assignés et ne verra pas les autres.»

D'où l'importance d'une bonne coordination entre la cybersécurité et la partie «business». «La cybersécurité n'est pas une problématique informatique», insiste Steven Meyer. «C'est un élément clé du système lié à l'opérationnel de la compagnie et à la stratégie.» »

LES UTILISATEURS SE FORMENT

Des entreprises se laissent attaquer pour apprendre à mieux résister. La formation avec mises en situation est encouragée.

Les entreprises développent diverses stratégies pour éviter que leur système de sécurité informatique soit perforé par les cybercriminels. Au mois d'avril, La Poste a par exemple invité les hackers à pirater ses sites web à travers le programme *bug bounty*. «Nous testons ainsi la vulnérabilité de tous les produits et systèmes», éclaire la porte-parole Silvana Grellmann. «Nous utilisons intentionnellement l'intelligence collective de la communauté internationale des hackers pour compléter l'expertise interne et externe existante.»

Une stratégie qui existe depuis une vingtaine d'années. «C'est le minimum à faire si l'entreprise est menacée», estime Alexis Roussel, directeur des opérations de la société Nym Technologies SA, qui est allé plus loin avec son projet NYM. «Nous laissons aussi les hackers nous attaquer mais à la différence de La Poste, c'est le projet tout entier qui est développé publiquement. Nous invitons continuellement notre communauté à tester et attaquer notre réseau, et pas seulement dans le cadre d'un concours défini. Les projets qui font cela sont plus robustes.»

La formation des employés est un élément clé du verrouillage du système informatique. La Poste propose par exemple aux développeurs spécialisés une formation spéciale aux techniques de sécurité. Les collaborateurs d'Alpiq, premier fournisseur d'énergie en Suisse, reçoivent «régulièrement des formations sur l'importance et le traitement des cyberrisques, par exemple les e-mails suspects», informe le porte-parole Guido Lichtensteiger.

La formation n'en reste pas moins lacunaire au niveau pratique en Suisse. C'est pourquoi Sémafor, entreprise déjà active dans la sensibilisation de l'ensemble des utilisateurs aux enjeux de la cybersécurité, proposera, dès le 26 mai, 29 cours différents couvrant aussi bien la sécurité des systèmes de contrôle industriels, que celle des *webapps*. «Le but n'est pas de vendre un produit ou une certification, mais de donner les moyens aux spécialistes de s'aguerrir avec les outils qui sont le standard en termes de cybersécurité», détaille le directeur Guillaume Saouli.

Et le volet pratique? «Nous mettons à disposition une plate-forme de formation unique avec des laboratoires virtualisés, intégrant également la gestion de l'apprentissage», poursuit le spécialiste. Ils reproduisent, en direct, des situations réelles telles qu'un problème de refroidissement dans une centrale nucléaire, un déraillement de train ou un piratage sur Instagram. Sans oublier de mettre à disposition les outils nécessaires pour faire face à chaque cas. » TJ