Les nouvelles menaces informatiques profitent de la crise sanitaire et ciblent les PME

La pandémie de Covid-19 provoque des dégâts sociaux et économiques sans précédent. Les conséquences de cette crise sont multiples et se nichent dans les endroits les plus inattendus. Ainsi, la cybersécurité doit prendre en considération le contexte sanitaire actuel, car les menaces informatiques ont muté. Les criminels utilisent les attentes et les craintes de responsables et des collaborateurs des entreprises – PME en tête – pour mieux manipuler, tromper, extorquer. Les organisations doivent plus que jamais se protéger contre les nouvelles cyberattaques. Si les spécialistes de la sécurité numérique demeurent très recherchés, des assurances spécifiques existent pour couvrir les risques liés à des actions malveillantes ou à des erreurs humaines.

UN DOSSIER RÉALISÉ PAR GRÉGORY TESNIER

«Il y a quelques années, la cybersécurité n'était qu'un créneau thématique suscitant, au niveau international, des débats généralement réservés aux experts techniques. Aujourd'hui, elle est devenue un enjeu fondamental et un sujet brûlant en politique internationale, d'autant plus brûlant que les technologies numériques jouent un rôle central à l'ère de la société de l'information. Les technologies clés se retrouvent ainsi au cœur des conflits mondiaux.» C'est par ces mots que Jon Fanzun, envoyé spécial de la Confédération pour la politique étrangère et de sécurité relative au cyberespace, ouvre le dernier rapport semestriel de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), publié il y a quelques semaines. Depuis juillet dernier, date d'entrée en vigueur de l'ordonnance sur la protection contre les cyberrisques dans l'administration fédérale (ordonnance sur les cyber-risques, OPCy), MELANI fait partie du Centre national pour la cybersécurité (NCSC). Ce centre de compétences est le premier interlocuteur pour les milieux économiques, l'administration, les établissements d'enseignement et la population pour toute question relative à la cybersécurité.

«La Suisse se doit de défendre activement ses propres intérêts dans le cyberespace», dit Jon Fanzun. Dans cette perspective, le fait que le NCSC fédère et coordonne les initiatives de tous les acteurs des différents départements fédéraux est «très précieux pour la cybersécurité internationale» du pays. Cette phrase prend toute sa signification quand on lit plus avant le rapport semestriel de MELANI: parmi les principaux cyberincidents observés au cours du premier semestre 2020 en Suisse et à l'étranger, la pandémie de coronavirus a servi d'appât pour un grand nombre de cyberattaques. Dès lors, on se rend compte que la gestion de la crise du coronavirus – paroxysme de crise aux dimensions mondiales – implique de prendre en considération non seulement, bien évidemment, des enjeux sanitaires et économiques, mais encore des enjeux inattendus comme ceux liés aux nouvelles menaces informatiques.

TÉLÉTRAVAIL ET NOUVEAUX RISQUES

La coordination des actions de toutes les forces et compétences présentes au sein de tous les départements fédéraux apparaît plus que jamais nécessaire pour gérer des problématiques internationales désormais toujours plus complexes et aux multiples dimensions. «Les cyberacteurs exploitent régulièrement pour leurs attaques les grands événements qui bénéficient d'une grande couverture médiatique, comme c'est le cas des catastrophes naturelles. C'est ce qu'ils ont fait durant le premier semestre 2020 dans le cadre de la pandémie de Covid-19. Fausses promesses sur des informations concernant le virus ou sur la possibilité de commander des masques pendant la pénurie, communications sur des commandes en ligne: les agresseurs ont instrumentalisé toutes sortes de sujets pour induire leurs proies en erreur ou pour propager des maliciels.» Le rapport de MELANI s'intéresse particulièrement aux conséquences de ces actes malveillants pour les entreprises. En effet, pour Max Klaus, responsable adjoint pour la cybersécurité opérationnelle au sein du NCSC, «les offres frauduleuses s'adressent principalement aux particuliers. Néanmoins, les entreprises peuvent également être victimes d'actes hostiles». Les sociétés de toute taille ont par exemple eu massivement recours au télétravail pendant le semi-confinement du printemps, ce qui implique l'apparition de nouveaux risques. Que dit MELANI à ce propos? «Les téléconférences ou vidéoconférences ont pris le relais des séances présentielles. Prises de court, les organisations ont parfois adapté à la hâte leur infrastructure informatique au télétravail sans avoir correctement pris les mesures de sécurité nécessaires, mettant ainsi leurs réseaux en danger. Les agresseurs ont intensifié leurs activités de reconnaissance afin d'identifier les solutions d'accès à distance vulnérables et de trouver les failles existantes ou les implémentations mal protégées de solutions RDP (Remote Desktop Protocol) et de serveurs VPN (Virtual Private Network) susceptibles de leur livrer accès aux réseaux des entreprises. Les attaques de *phishing* ont également tiré parti du chamboulement des habitudes de travail. Bien des personnes utilisaient pour la première fois des logiciels de conférence ou de collaboration et, faute d'avoir reçu jusque-là les messages émanant de telles plateformes, il leur était difficile de reconnaître les contrefaçons.» Conclusion: les collaborateurs effectuant du télétravail sont souvent livrés à eux-mêmes face aux attaques d'ingénierie sociale et les campagnes de sensibilisation demeurent particulièrement utiles pour diffuser les bonnes pratiques en matière de cybersécurité. Celle-ci n'est pas du seul ressort des informaticiens, mais nécessite bel et bien la participation de l'ensemble du personnel d'une organisation.

LE TÉLÉTRAVAIL NE CONSTITUE PAS LA SEULE SOURCE DE VULNÉRABILITÉ NUMÉRIQUE DES ENTREPRISES.

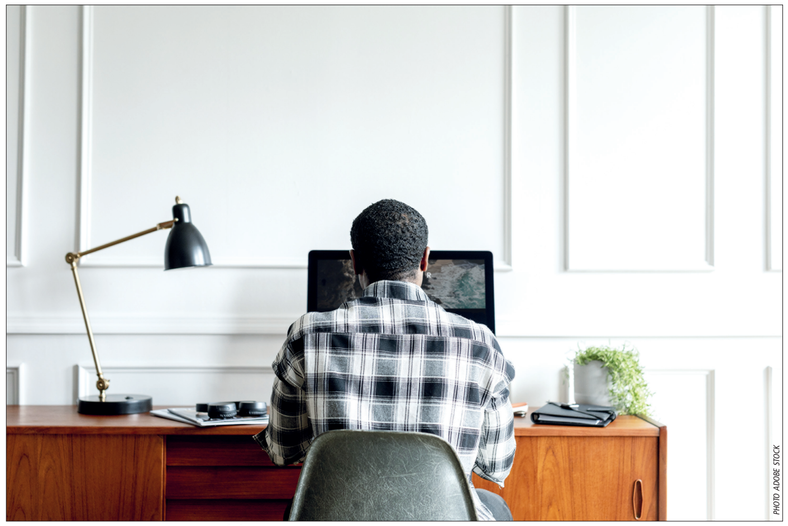

PHOTO ADOBE STOCK

***LES COLLABORATEURS EFFECTUANT DU TÉLÉTRAVAIL** sont souvent livrés à eux-mêmes face aux cyberattaques.*

PRISE DE CONSCIENCE NÉCESSAIRE

Le rapport de MELANI insiste vraiment sur les efforts globaux à fournir pour sécuriser le télétravail: «Il est trop tôt pour dire quand la pandémie actuelle prendra fin et quand la vie reprendra son cours normal. Mais il ne faut pas oublier qu'un retour à la situation d'avant la pandémie n'est peut-être ni possible ni souhaitable. Si quelques entreprises se sont dotées depuis longtemps d'une infrastructure stable et sécurisée propice au nomadisme numérique, d'autres ne disposent que de solutions installées à la hâte et plutôt improvisées. Il vaut donc la peine de profiter dès à présent des expériences réalisées et de contrôler les solutions utilisées afin de les améliorer ou de lancer un projet de refonte complète pour intégrer dès la phase de conception, outre les capacités des infrastructures, la sécurité des appareils, des réseaux ainsi que des données.»

Le télétravail ne constitue pas la seule source de vulnérabilité numérique des entreprises pendant cette période de pandémie. Les rançongiciels font également de nombreuses victimes, surtout des PME. Ce sont des logiciels malveillants qui bloquent l'accès à un ordinateur ou à des fichiers en les chiffrant et qui réclament à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès. MELANI a recensé quarante-deux attaques de ce type contre des entreprises pendant le premier semestre 2020. Max Klaus rappelle que «la plupart des cyberattaques sont menées selon le principe de l'arrosoir, de sorte que toute entreprise, quelle que soit sa taille et quel que soit son secteur d'activité, peut être victime d'une cyberattaque».

Quelles sont alors les bonnes pratiques à adopter pour une PME qui veut se protéger de la cybercriminalité, particulièrement dans ce contexte de pandémie de coronavirus? «En principe, une combinaison de mesures techniques et organisationnelles devrait être mise en place dans chaque entreprise. Les mesures techniques comprennent, par exemple, la mise à jour continue des programmes, l'utilisation d'une protection antivirus, d'un parefeu, la sauvegarde régulière des données, etc. Les mesures organisationnelles concernent quant à elles, par exemple, la rédaction précise du règlement interne de l'entreprise pour le traitement des paiements. Il est également important de sensibiliser les employés à la manière correcte de traiter les cyber-risques.» ■

LE RAPPORT DE MELANI INSISTE VRAIMENT SUR LES EFFORTS À FOURNIR POUR SÉCURISER LE TÉLÉTRAVAIL.

Télétravail: sécuriser son accès à distance

Le Centre national pour la cybersécurité (NCSC) propose une brochure qui rappelle les bonnes pratiques afin de minimiser le risque lié aux technologies d'accès à distance utilisées pour le télétravail.
Pour plus d'informations:
www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/fernzugriff.html

Préoccupation grandissante

Récemment, deux études ont montré une prise de conscience plus forte de ces problématiques au sein des entreprises. D'abord, c'est une enquête de la société d'audit Deloitte qui signale que le thème de la cybersécurité a nettement gagné en importance ces derniers mois parmi les points qui préoccupent les directeurs financiers suisses. «Cela s'explique principalement par l'avancée de la numérisation observée depuis le début de la pandémie et la multiplication des cyberattaques», selon cette enquête. «Les directeurs financiers ont compris que le flux de données initié par le télétravail devait être mieux protégé», explique aussi Jean-François Lagassé, associé et responsable du secteur des services financiers chez Deloitte Suisse. Il poursuit: «C'est maintenant aux entreprises qu'il revient de prendre des mesures ciblées afin que le télétravail ne constitue pas un point d'entrée pour les cybercriminels. Cela implique notamment que les collaborateurs soient mieux formés et que des investissements ciblés dans des solutions informatiques sécurisées soient réalisés». L'autre étude qui vient d'être publiée et qui signale que la cybersécurité se place maintenant «au cœur des préoccupations des dirigeants» est celle du spécialiste de l'audit et du conseil PwC: PwC Digital Trust Insights 2021. Sur plus de trois mille entreprises interrogées au niveau mondial, 96% ont modifié leur stratégie de cybersécurité en raison du Covid-19. En Suisse, elles sont 89% dans ce cas. Toujours en Suisse, 34% des entreprises interrogées envisagent d'augmenter leurs «cyberbudgets» pour 2021. Et les risques numériques attendus pour l'année prochaine? Près de 80% des entreprises craignent des attaques de ransomware et des cyberattaques contre les services cloud, avec de graves répercussions.

Vers un besoin accru de formations en cybersécurité

Le Clusis, association suisse de la sécurité de l'information, a récemment organisé deux séminaires en ligne consacrés aux besoins de formation en cybersécurité. Plusieurs représentants de différents secteurs de l'économie ont exprimé leurs points de vue à ce sujet, à l'heure où «la situation sanitaire que nous vivons depuis le début de cette année montre l'importance d'investir dans des profils spécialisés en sécurité de l'information».

Ce fut l'occasion, pour les uns et pour les autres, de rappeler par exemple qu'il existe un manque de spécialistes en cybersécurité sur le marché du travail suisse ou que «l'apprentissage des bonnes pratiques en matière de cybersécurité ne concerne pas que les collaborateurs de l'informatique, mais tous les salariés».

OFFRE EXCELLENTE EN SUISSE ROMANDE

Un intervenant, issu du secteur bancaire, a souligné l'excellence de l'offre de formations en cybersécurité en Suisse romande: «Les programmes disponibles vont dans le bon sens et sont pertinents». Ici, il faut mentionner que deux aspects des formations apparaissent comme incontournables: d'abord le fait que les programmes présentent l'état complet des connaissances théoriques et techniques et, ensuite, que ceux-ci n'oublient pas de favoriser, chez les étudiants, la capacité future à mobiliser tous les collaborateurs, la direction et l'ensemble du management d'une entreprise dans la lutte contre les cyberattaques. Des compétences poussées en communication orale et écrite sont donc primordiales pour un professionnel de la cybersécurité. Dans cette perspective, un expert a souligné que «notre époque est celle des millennials et de la génération Z où personne n'accepte d'être formé à quelque chose ou de suivre des directives sans qu'on lui explique les tenants et aboutissants de la démarche souhaitée». Un autre intervenant s'est posé la question suivante: «Ne devrait-on pas davantage intégrer la dimension sécurité dans toutes les formations de base en informatique?». ■

Pour plus d'informations:
www.clusis.ch

Cybercriminels arrêtés

Les cybercriminels sont-ils capables de se cacher indéfiniment en utilisant les failles du système d'entraide judiciaire internationale? Non. Les efforts pour les stopper paient. Le dernier rapport de MELANI indique que les autorités de poursuite pénale suisses et polonaises ont démantelé en avril 2020, avec l'aide d'Europol, le groupe InfinityBlack. «Ce groupe de cybercriminels, dont des mineurs et de jeunes adultes, était actif dans la diffusion de données d'utilisateurs dérobées, dans la création et la propagation de maliciels ou d'outils de piratage, ainsi que dans des fraudes diverses. La police a confisqué du matériel électronique, des disques durs externes et des portefeuilles de cryptomonnaies pour une valeur de cent mille euros. Elle a également fermé deux plateformes, dont les bases de données renfermaient plus de cent septante millions d'entrées. Le modèle d'affaires du groupe de pirates consistait à créer des plateformes en ligne pour la revente de listes de milliers de «combos» (binôme identifiant/mot de passe). La principale source de revenus des pirates consistait à subtiliser les données d'accès au programme de fidélisation d'un grand distributeur suisse pour les revendre à d'autres groupes criminels moins avancés techniquement.» ■

Des assurances spécifiques pour protéger les entreprises contre les risques liés à la cybercriminalité

Les premiers produits d'assurances pour protéger les entreprises contre les risques liés à la cybercriminalité semblent être nés au début des années 2000 dans le monde anglo-saxon. Il a fallu attendre ces trois ou quatre dernières années pour voir apparaître de façon assez généralisée des produits similaires en Suisse romande.

De quoi s'agit-il? De produits d'assurances destinés à la cyberprotection des entreprises, des PME en particulier. La crise sanitaire actuelle et les risques accrus de cyberattaques qu'elle entraîne pourrait accélérer l'attrait pour des contrats de ce type. «Le monde numérique n'est pas sans dangers. Si internet nous ouvre les portes du monde numérique, il les ouvre malheureusement aussi à des visiteurs indésirables. Notre assurance cyberprotection pour entreprises est donc depuis 2017 la réponse à ce défi. Les entreprises bénéficient d'un paquet de prestations exhaustif en cas de cyberincident (interlocuteur central, assistance de spécialistes expérimentés, prise en charge des frais de reconstitution des données endommagées, etc.)», explique Isabelle Schmidt-Duvoisin, membre du département communication et porte-parole de la Mobilière Suisse. Jesús Pampín, chef du service Souscription Choses à la Vaudoise Assurances, avance la même année de naissance pour «l'extension cyber» proposée par son entreprise. «Il y a cinq ou six ans, en Suisse, les clients n'auraient pas fait le pas vers une solution comme celle-ci. Le contexte a rapidement changé, les enjeux numériques sont beaucoup plus nombreux – digitalisation des processus, nouveaux moyens de paiement, nouvelles règles juridiques, hausse des attaques informatiques, etc. –, et notre clientèle de petites et très petites entreprises est aujourd'hui à la recherche d'une couverture des risques liés à la cybercriminalité. La Vaudoise propose une couverture très large – les événements assurés comprennent les attaques contre les données ou systèmes, les accès non autorisés aux données, les intrusions dans les systèmes ou l'action de programmes malveillants – à un prix très accessible, simple à souscrire sans questionnaire et en mettant l'accent sur l'assistance.» Stéphane Fleury, responsable des souscriptions en cyber-assurances pour les grands clients à la Bâloise Assurances, indique que le produit Bâloise cyberassurance PME a été lancé courant 2018 «afin de parer aux nouveaux risques liés à la digitalisation dans les domaines d'activité de nos clients privilégiés que sont les PME». Il poursuit: «Nous proposons une solution complète, simple, sous forme de paquets ou de formules qui permettent de couvrir l'ensemble des conséquences financières qui pourraient faire suite à un événement cyber. Par «événement cyber», il faut comprendre tant les actes criminels, comme le piratage, les maliciels ou les attaques par déni de service, que les erreurs humaines comme la divulgation par erreur d'informations confidentielles dans le domaine public, l'effacement de données, etc.».

COVID-19: DEMANDES DIFFÉRENTES?

Le contexte de la pandémie de coronavirus a-t-il accru, d'une façon ou d'une autre, les risques liés à la cybercriminalité pour les PME romandes? Constate-t-on plus de demandes ou des demandes différentes de la part de PME désireuses de souscrire une assurance contre les risques liés à la cybercriminalité? Les spécialistes de l'assurance ont des réponses variées. Jesús Pampín n'a pas constaté de différences ou de variations inhabituelles ces derniers mois par rapport aux cas de fraudes ou d'attaques signalées ou par rapport à des demandes plus nombreuses de la part des PME, assurées ou non. Il mentionne l'importance du rôle de l'Etat – soit le Centre national pour la cybersécurité (NCSC) – pour le bon suivi des cyberattaques à un niveau très global et signale deux «maillons potentiellement vulnérables» dans les entreprises ou autour des entreprises: les employés et les sous-traitants. Certains, pour diverses raisons, peuvent se trouver pris au piège d'une arnaque numérique capable de prendre rapidement des dimensions importantes et de constituer, notamment, une porte d'entrée pour les criminels vers des données protégées. Isabelle Schmidt-Duvoisin rappelle que «les cybercriminels apprécient tout particulièrement les situations et les événements inhabituels. Ils leur servent de prétextes pour amener des personnes à agir – par curiosité, par peur ou par ignorance – dans le sens qu'ils souhaitent. Pendant le semi-confinement, la Mobilière a enregistré un nombre accru d'attaques par *phishing* qui profitaient du thème coronavirus. Le nombre de sinistres n'a toutefois pas augmenté. En ce qui concerne un éventuel effet Covid-19 sur les assurances, il est encore trop tôt pour relever une tendance». Pour Stéphane Fleury, «lors du premier semi-confinement, les entreprises étaient, dans un premier temps, plutôt occupées à trouver des solutions techniques pour pouvoir continuer leurs activités et des soutiens financiers afin de pouvoir assurer la survie de leurs exploitations». Les choses ont changé dans un deuxième temps, dès la fin du semi-confinement: «Nous avons senti en regain d'intérêt pour des solutions d'assurance «cyber», les entreprises ayant été sensibilisées aux questions de protection informatique par les nouveaux risques liés à des processus récemment mis en place, notamment le travail à la maison». ■