Les PME romandes, cibles privilégiées des cyberattaques

CYBERCRIMINALITÉ De plus en plus organisées, les attaques en ligne visent les PME romandes. Quelques bonnes pratiques permettent de se préparer face à ce type de menaces.

GRÉGORY TESNIER

Être la proie de criminels en ligne est traumatisant pour les chefs d'entreprise. Des organisations mafieuses se cachent souvent derrière les vols de données et autres chantages financiers à distance (*ransomware*) exercés de plus en plus fréquemment sur les organisations publiques et privées de Suisse romande.

Lourdes conséquences

Les PME constituent une cible de choix pour mener des cyberattaques qui répondent à quelques scénarios connus: il s'agit soit d'empêcher le bon fonctionnement de l'entreprise, soit de nuire à son image en diffusant très largement des informations confidentielles dérobées. La récente enquête annuelle *Allianz Risk Barometer 2024* concernant les principaux risques commerciaux dans le monde – trois mille sondés – a montré que les cyberincidents et les interruptions d'activité occupent respectivement la première et la deuxième place, tant au niveau mondial que suisse.

Le guide *Cyber-risques* proposé en ligne par le Département genevois de l'économie et de l'emploi et présenté en décembre dernier lors du Forum économie numérique, qui a eu lieu dans les locaux de la FER Genève, rappelle qu'en compromettant «la sécurité de données, qu'elles soient sensibles ou non, les cyber-risques peuvent avoir de lourdes conséquences comme des pertes financières, l'interruption des activités commerciales, la perturbation de l'activité, des risques de sécurité, l'arrêt de la production ou des dommages à la réputation».

Que faire? Comment et pourquoi les PME doivent-elles réagir? Pour Sylvain Porchet, responsable du département sécurité et RSSI de l'entreprise spécialiste en informatique Evo-Link, les PME doivent d'abord être attentives à la gestion de leurs vulnérabilités.

Concernant celles-ci, quelques points faibles ressortent fréquemment: les mises à jour des logiciels ne sont pas effectuées ou sont trop tardives, l'inventaire des applications installées sur l'ensemble des stations de travail n'est pas complet ou actualisé, la sensibilisation des collaboratrices et des collaborateurs aux risques de cyberattaques n'est pas assez poussée.

«Pour une entreprise, le défi en matière de cybersécurité est moins de protéger les serveurs informatiques principaux que de veiller aux risques ayant pour origine les stations de travail des employés.» Les ordinateurs des collaborateurs d'une organisation représentent des portes d'entrée plus accessibles pour les criminels.

Emmanuel Meurant, directeur du département contrôle et sécurité de la FER Genève, souligne qu'il ne faut pas, pour une PME, minimiser la charge de travail nécessaire pour inventorier et mettre à jour régulièrement tous les logiciels de l'entreprise et combler leurs vulnérabilités. Faire appel à des spécialistes externes correspond à une solution efficace. Il faut prendre en considération que les enjeux commerciaux et financiers sont élevés.

Des criminels de plus en plus organisés

«La cybercriminalité continue de se perfectionner et s'organise désormais comme une véritable industrie avec une grande multiplicité d'acteurs (investisseurs, fournisseurs, prestataires, sous-traitants, R&D, etc.). Par exemple, des organisations commercialisent des modèles d'attaque et font appel à des sous-traitants pour les concevoir. Ils vont jusqu'à vendre les mises à jour de leurs logiciels malveillants! Des exploitants mènent les actions pour leur propre compte ou pour distribuer ensuite les données volées à d'autres cybercriminels», explique un récent ouvrage sur la cybersécurité dirigé par le spécialiste Daniel Benabou. Une professionnalisation à l'extrême des cybercriminels que confirme Pascal Rochat, responsable réseau pour la direction générale de la FER Genève: «Certains groupes de pirates informatiques se concentrent dorénavant dans la seule détection des vulnérabilités, tandis que d'autres axent leurs actions sur l'exploitation de ces vulnérabilités».

Chantage

Dans le détail, les attaques des criminels peuvent être de deux types, comme le note Albert Rossier, directeur du Master of Advanced Studies en Management de la sécurité des systèmes d'Information de la Haute école de gestion de Genève et membre du comité consultatif de l'Association suisse de la sécurité de l'information.

Le premier type d'attaques vise à trouver une vulnérabilité – grâce à une manœuvre d'ingénierie sociale ou à des processus numériques automatisés – qui permette d'entrer dans le système informatique d'une organisation pour «chiffrer» des données et empêcher l'entreprise de fonctionner normalement.

Les criminels se livreront à un chantage et réclameront une rançon pour autoriser l'entreprise à récupérer ses données.

Le deuxième type d'attaques – a priori en hausse ces derniers mois – consiste à voler des données confidentielles et à menacer l'entreprise de les diffuser à grande échelle. Là aussi, un chantage financier s'exerce.

Dans ce dernier cas, des aspects de la nouvelle loi sur la protection des données, entrée en vigueur en septembre 2023, et de l'ordonnance sur la protection des données du 31 août 2022 pourraient avoir des effets inattendus et indésirables, comme le note Sylvain Porchet. En obligeant les entreprises à signaler aux autorités un vol et une diffusion de données confidentielles et en fixant une amende possible d'un montant maximum de 250 000 francs – cinq fois plus qu'auparavant – aux entreprises concernées par ce type de vol, les autorités, paradoxalement, ont offert un moyen de pression supplémentaire aux criminels dans leurs pratiques d'intimidation.

Des cibles intéressantes

Cela s'ajoute au fait que les cybercriminels jugent les PME comme des cibles intéressantes, car moins bien préparées aux attaques que les grandes structures et, toutefois, sensibles comme elles aux risques qui menacent leur réputation. Albert Rossier insiste, en plus de tous les éléments mentionnés ici, sur les plans de continuité des activités – ils permettent à une organisation de continuer à agir en cas d'interruption non souhaitée de ses services ou d'attaques en ligne – que les PME doivent absolument élaborer. De même, ces dernières sont tenues de transmettre régulièrement à leurs collaborateurs les bonnes pratiques en matière de cybersécurité. ■



Une cyberattaque est vécue comme un lourd traumatisme par les responsables de PME.

Cybersécurité: la FER Genève renforce les services proposés à ses clients

La FER Genève renforcera prochainement les services de sensibilisation et de soutien en matière de cybersécurité qu'elle propose à ses clients. La fédération est déjà active depuis plusieurs années dans ce domaine et, dans la continuité de cette action, elle déploiera bientôt une nouvelle plateforme de support, de veille et de mise en relation qui réunira les informations et les aides précises dont les entreprises ont besoin avant, pendant et après une crise informatique.

Olivier Bridel, chef de projet chez Fréquence TV

«La cybersécurité représente un enjeu très important pour les PME romandes»

«Les questions de cybersécurité sont fréquemment abordées dans notre entreprise, qui compte une trentaine de collaborateurs. Les équipes de direction nous sensibilisent régulièrement aux multiples risques informatiques et à leurs conséquences potentiellement graves. L'année dernière, encouragés par les autorités du canton de Vaud, nous avons suivi une formation spécifique concernant ces thématiques: Trust4SMEs. Ce programme d'accompagnement en cybersécurité et confiance numérique pour PME est mis en place par Trust Valley, le pôle de compétences lémanique en matière de confiance numérique et de cybersécurité. Dans le cadre de cette formation, des spécialistes nous ont montré différentes techniques utilisées par les cybercriminels pour pénétrer dans un système informatique d'entreprise, notamment celles liées aux attaques par hameçonnage. La cybersécurité représente un enjeu très important pour les PME romandes.»

Thierry d'Autheville, directeur Général de Parkgest

«J'encourage les chefs d'entreprise à faire appel à des spécialistes externes»

«La gestion des risques informatiques s'insère dans la gestion globale des risques d'une entreprise. J'ai pour ma part besoin d'une méthodologie matricielle de travail – qui implique de déterminer l'impact de chacun des risques en utilisant des coefficients pour les conséquences financières et les probabilités d'occurrence – afin de les prioriser et de les mitiger avec le plus d'efficience possible. Quoi qu'il en soit, nous demeurons, en tant que PME, souvent très exposés, notamment aux risques informatiques. Ils sont toujours très complexes à gérer. J'encourage les chefs d'entreprise à faire appel à des spécialistes externes s'ils ne disposent pas à l'interne des compétences pour préparer et maîtriser la cybersécurité de leur organisation.»