POINT FORT

Cybercriminalité: les entreprises suisses ne luttent pas toutes à armes égales

Nombre de firmes manifestent un manque de prise de conscience sur cette problématique. D'autant que les attaques informatiques étatiques sont impossibles à contrer, selon Laurent Balmelli.

MAUDE BONVIN

En 2018, plus de 30% des entreprises suisses ont subi une perte financière, suite à une cyberattaque. Selon le CEO du spécialiste de la sécurité informatique ZENData Steven Meyer, il y a un réel manque de prise de conscience de la part des firmes à cet égard. «J'entends encore des PME affirmer qu'elles ne sont pas concernées par ce problème car elles n'ont rien à voler», déclare-t-il. Pour le spécialiste en cybersécurité Laurent Balmelli, cette question est encore trop banalisée par les entrepreneurs. «Or, au niveau des start-up et des petites structures, si leur valeur ajoutée est volée, soit leur innovation, les conséquences peuvent être désastreuses», abonde-t-il.
En matière d'attaques numériques, ce n'est pas la taille du groupe qui compte. «Beaucoup de petites sociétés nous appellent après coup, alors qu'elles en ont été victimes», indique le patron. La clientèle-cible de ZENdata? Les entreprises employant moins de 200 collaborateurs, même si la firme genevoise compte aussi, dans son escarcelle, quelques multinationales.

LAURENT BALMELLI. *Selon l'expert, ceux qui ciblent un très grand nombre de gens ne sont pas des professionnels du hacking.*

De la pêche au large à l'attaque ciblée

Il existe plusieurs profils de pirates informatiques. «Les hackers peuvent agir par pur opportunisme, au hasard et sans trop de réflexion, lorsque l'attaque est aisée à réaliser. A ce niveau, tous les secteurs d'activité peuvent être touchés», poursuit le directeur général. Dans ce cas de figure, les escrocs cherchent à se faire un peu d'argent facilement, via l'envoi par exemple d'un email vérolé à un très grand nombre de personnes. «Ce ne sont pas forcément des professionnels du hacking», ajoute Laurent Balmelli.
D'autres pirates informatiques mènent des actions plus poussées. Ils ciblent alors prioritairement les structures qui brassent beaucoup d'argent, afin de maximiser leur méfait. Les emails malveillants envoyés sont alors très personnalisés, ce qui rend ce genre d'atteinte plus difficile à éviter.
«Soumises à la réglementation de la Finma, les banques sont généralement bien armées contre ce type de dommage, même si certaines règles du gendarme financier en la matière sont désormais obsolètes», soutient Steven Meyer. Selon le CEO, les fiduciaires, gestionnaires de fortune, études d'avocats et family offices sont par contre moins bien protégés contre ce genre d'atteinte alors qu'ils sont tout autant des cibles.
Pour l'expert en cybersécurité, la menace à l'interne ne doit par ailleurs pas être sous-estimée. «Par vengeance, un collaborateur peut tout-à-fait effacer toutes les données d'une entreprise ou y introduire un virus», illustre-t-il.

Gouvernement espion

Le dernier type de dommage se situe au niveau étatique, lorsqu'un pays pirate une entreprise ou un particulier. «Il est quasiment impossible de lutter contre ces attaques», soutient Laurent Balmelli.
C'est le cas du Kazakhstan qui intercepte les données de ses citoyens pour avoir un contrôle sur leurs activités en ligne. Le gouvernement prétexte un renforcement de la sécurité et la lutte contre la cybercriminalité pour forcer les résidents à installer du code espion sur leurs machines.

«CETTE ACTION QUI RENFORCE LA PUISSANCE D'UN PAYS TOTALITAIRE EST ASSEZ PRÉOCCUPANTE, D'AUTANT PLUS QUE L'ON PEUT S'ATTENDRE À CE QUE D'AUTRES ETATS SUIVENT LE MÊME CHEMIN.»

«C'est le premier pays à faire cela. Cette action qui renforce la puissance d'un pays totalitaire est assez préoccupante, d'autant plus que l'on peut s'attendre à ce que d'autres Etats suivent le même chemin. Je pense notamment aux gouvernements répressifs et aux dictatures», s'inquiète Steven Meyer.

Dans une situation compliquée

Concrètement, les fournisseurs de services Internet doivent forcer leurs utilisateurs à installer un certificat gouvernemental sur tous leurs appareils et dans tous leurs navigateurs. Ce certificat décrypte toutes les connexions HTTPS.
Aux yeux du patron, les navigateurs web (Chrome, Firefox, Edge) se trouvent dans une situation difficile. Soit ils n'interviennent pas dans la décision du gouvernement, soit ils décident de bloquer le contenu incriminé ou d'informer leurs utilisateurs. Dans le second cas de figure, le risque est alors grand que le gouvernement kazakh les interdise sur son territoire et impose un navigateur gouvernemental moins sûr et donc plus susceptible d'être attaqué.
Au niveau des entreprises, cela pose la question du secret des affaires. «Pour l'heure, nous ne savons pas si un businessman suisse qui se rend au Kazakhstan est concerné par cette mesure», précise le directeur général. Ce dernier conseille toutefois aux entrepreneurs qui souhaitent se rendre dans ce pays de se doter d'un ordinateur et d'un téléphone propres à ce voyage. Ces appareils ne devront contenir que le strict minimum et tout leur contenu devra être effacé, une fois de retour en Suisse. Les données devront par ailleurs être cryptées. Il convient également de se doter d'un vpn, pour assurer la confidentialité des communications. Ces conseils sont aussi valables pour les séjours en Chine.■

Le crime organisé a remplacé l'idéalisme

Quelque 300.000 nouveaux virus sont créés, chaque jour, dans le monde. Si les anti-virus permettent de contrer la plupart d'entre eux, il en restera toujours un centième impossible à repérer. Les attaques concernent aussi désormais les applications. «Aucune n'est sûre à 100%», prévient le CEO de ZENData, Steven Meyer. A l'instar de FaceApp, l'application russe de vieillissement du visage, si les données transmises, via ces canaux, sont cryptées, cela ne veut pas dire qu'elles sont sécurisées. Des chercheurs ont, par exemple, réussi à modifier un document transmis par WhatsApp et Telegram, malgré le cryptage de bout-en-bout. «Un utilisateur peut donc voir apparaître, dans sa conversation, une photo, un document ou encore un message audio différent de celui qui a été envoyé par l'expéditeur. Ce type de dommage peut mener à de fausses factures, beaucoup de PME utilisant WhatsApp pour leur facturation», explique Steven Meyer. L'atteinte ne fonctionne que sur Android, les iPhone ne sont pas concernés. Le malware transforme la pièce jointe enregistrée sur le téléphone portable de son destinataire, avant que WhatsApp ne l'affiche à l'écran. Très bref, ce laps de temps est néanmoins suffisant pour que le mal soit fait.
Pour le patron de ZENData, cette faille prouve qu'il faut sécuriser son smartphone, comme un ordinateur. «Il convient également de systématiquement vérifier la véracité d'une information via un autre canal que l'application, lorsque les conséquences peuvent être importantes», conseille-t-il.

STEVEN MEYER. *«Les demandes de rançon en ligne touchent autant les PME que les multinationales», dit le CEO de ZENdata.*

Extorsions en hausse ces dernières années

Ces dernières années, un autre type d'attaques a fait son apparition: les demandes de rançon. «Elles sont en progression, depuis la création de ZENData il y a six ans, et touchent aujourd'hui autant les PME que les multinationales», souligne Steven Meyer. Les rançongiciels auraient coûté huit milliards de dollars au plan mondial, l'an passé, selon une étude de l'Alliance pour la confiance en ligne. Les collectivités publiques ont en particulièrement fait les frais, notamment les villes d'Atlanta et de Baltimore aux Etats-Unis. Tous dommages confondus, les pirates informatiques ont mené deux millions d'attaques, en 2018, avec un coût estimé à plus de 45 milliards de dollars.
Les hackers se montrent également plus patients. «Ils peuvent observer une entreprise durant plusieurs mois, avant de passer à l'action. Cela leur permet d'optimiser leur attaque, en collectant notamment un gros volume de données», précise le spécialiste. Dernier changement? «Il y a, quelques années, c'étaient les activistes idéalistes, comme le groupe Anonymous, qui faisaient la majorité du bruit. Nous sommes désormais passés à l'ère du crime organisé, avec une recherche de profit maximale», conclut le responsable.■

Logiciels au secours de la valeur d'une société

«Toutes les entreprises ne connaissent pas toutes les données qu'elles possèdent. Elles n'ont donc pas conscience qu'il faut les protéger», déplore Nathalie Feingold. La fondatrice et directrice de l'entreprise active dans le big data NPBA conseille aux sociétés de se doter d'un logiciel dont les conditions générales sont en lien avec leur stratégie. Cela pose la question du stockage et du transit des informations détenues par les firmes, souvent des données sensibles. Or certains logiciels, notamment gratuits, revendent ces données.

Le risque de dépendance

Pour la spécialiste, la législation suisse accorde suffisamment de marge de manœuvre aux groupes en la matière. «C'est à eux de se prendre en main. Cela est d'ailleurs dans leur intérêt. En cas de faille, le risque de réputation est assez grand. Aujourd'hui, le consommateur attend que les compagnies empoignent ce sujet à bras-le-corps. Elles ne peuvent plus dire je ne savais pas.»
A ses yeux, cette question doit se régler au niveau de la gouvernance des entreprises. Les conseils d'administration doivent impérativement se doter d'une stratégie en la matière.
A côté du danger pour la réputation, existe aussi le risque de dépendance. «Si je confie mes données à un seul prestataire, que se passe-t-il en cas de faillite de ce prestataire?», s'interroge l'analyste de formation pour qui il convient aussi de bien former son personnel à la gestion des données.

«PAR MANQUE DE MOYENS, LES START-UP S'APPUIENT SOUVENT SUR DES LOGICIELS GRATUITS, SANS LIRE LES CONDITIONS GÉNÉRALES.»

Pour elle, il vaut la peine de se poser toutes ces questions car des données de bonne qualité représentent une classe d'actifs importante pour les entreprises et les start-up. «Or les jeunes pousses ne sont pas forcément data centrées. Nous ne les challengeons pas assez à ce propos car nous pensons qu'elles le sont d'office», souligne l'experte. A leurs débuts, les start-up misent tout sur le développement de leur produit et les levées de fonds, au détriment de la gestion de leurs données. «Par manque de moyens, elles s'appuient souvent sur des logiciels gratuits, sans lire les conditions générales. Elles génèrent donc beaucoup de risques à ce niveau-là, surtout qu'une mauvaise architecture des données péjore la valeur d'une société.» Il faut donc intégrer cette question, dès la création de l'entreprise, d'autant plus qu'elle influe tous les domaines d'activité d'une compagnie.

Cryptage au menu

Pour le spécialiste en cybersécurité Laurent Balmelli, une gestion adéquate des données passe d'abord par la création de mots de passe différenciés et appropriés, puis par une bonne administration des authentifications numériques. «Si toutes les clés d'accès sont distribuées sur les 50 ordinateurs de l'entreprise, alors l'infrastructure informatique sera très dure à protéger», prévient-il. Toutes les données, tant au repos qu'en transit, doivent ensuite être chiffrées.
Président de l'Observatoire des risques opérationnels (Oprisko), Cyrille Reynard recommande de tenir à jour systématiquement les systèmes et de renouveler les mots de passe fréquemment, tout en sauvegardant quotidiennement les systèmes. «Les entreprises doivent cependant partir du principe que tôt ou tard elles seront attaquées», estime-t-il.■