LES ENTREPRISES, CIBLES DE CHOIX POUR LES CYBERCRIMINELS

Entre 2020 et 2021, le nombre d'infractions numériques répertoriées en Suisse a augmenté de 24 % et les victimes hésitent encore bien souvent à s'annoncer ou à porter plainte. Or, une bonne connaissance des modes opératoires employés permet généralement d'éviter la catastrophe et de réagir adéquatement en cas de menace.

La cybercriminalité est un phénomène qui connaît une augmentation fulgurante. Les services de police suisses ont en effet identifié plus de 30 000 cas en 2021 contre près de 25 000 une année auparavant. Et tout porte à croire que ce chiffre n'est que la pointe de l'iceberg et que de nombreuses infractions numériques ne font pas l'objet de plaintes. Certaines entreprises, cibles de choix pour les cybercriminels, craignant bien souvent les répercussions dans l'opinion publique et auprès de leurs clients, hésitent à se faire connaître et préfèrent taire ce type d'incident, qui peut prendre plusieurs formes.

L'ARNAQUE AU PRÉSIDENT

L'arnaque au président est un bon exemple de cybercriminalité pour lequel la prévention ne pose en principe pas de gros défi à l'organisation. Pourtant, en Suisse, 412 cas ont été répertoriés par les autorités en 2021, infligeant des pertes parfois conséquentes pour les organisations victimes.

L'arnaque au président est une forme de fraude où l'escroc contacte l'employé d'une organisation en se faisant passer pour son dirigeant. Après avoir gagné sa confiance, il lui demande d'effectuer un virement en urgence pour un motif quelconque, généralement en lien avec les activités de l'organisation. Les escrocs qui réalisent ce genre de cyberescroquerie utilisent souvent le web et les réseaux sociaux pour s'informer sur une organisation, sa structure et ses employés. Les informations ainsi récoltées permettent de mettre l'employé contacté en confiance. Pour s'en prémunir, il est important de sensibiliser les collaborateurs de l'organisation et d'intégrer ce risque dans l'établissement des processus internes liés aux paiements. Par ailleurs, il ne faut pas hésiter à googler son entreprise et soi-même pour être conscient des informations qui peuvent être disponibles pour les escrocs.

LES RANÇONGICIELS

Les rançongiciels (ou *ransomware* en anglais) sont des logiciels malveillants qui se déploient sur des systèmes informatiques afin de chiffrer les données. La victime se voit ainsi dans l'incapacité d'accéder à ses différents fichiers.

Pour retrouver cet accès, il lui est demandé de payer une rançon, soit un certain montant généralement demandé en cryptomonnaies. En 2021 en Suisse, 340 cas ont été signalés aux autorités.

Comme déjà mentionné, il est fort probable que ce chiffre ne représente qu'une toute petite partie de la réalité. Bon nombre d'organisations victimes de rançongiciels préfèrent négocier et payer la rançon sans communiquer le cas aux autorités. Pour limiter les risques d'en devenir victime, il est important de procéder à la sauvegarde régulière des données en lieu sûr, de disposer de moyens techniques de cybersécurité et de former les collaborateurs aux risques de téléchargement de logiciels malveillants. Comme la plupart des autres types de logiciels malveillants, les rançongiciels sont souvent déployés en empruntant des canaux de communication réguliers: pièces jointes dans les e-mails frauduleux, liens de téléchargement compromis, etc.

LES CHEVAUX DE TROIE

Les chevaux de Troie bancaires sont également des logiciels malveillants que l'on retrouve en Suisse. En 2021, 82 cas ont été répertoriés par les autorités en Suisse. Il s'agit d'outils informatiques utilisés par les cybercriminels pour voler les données de connexion liées à l'utilisation du e-banking.

Tout comme les rançongiciels, les chevaux de Troie bancaires sont déployés en empruntant des canaux d'infection réguliers. Leurs conséquences sont toutefois différentes. Les victimes peuvent voir leurs comptes bancaires vidés par les cybercriminels qui usurpent leurs identifiants. Certains chevaux de Troie modernes parviennent même à contourner la double authentification. Pour s'en prémunir, il faut encore une fois se méfier des courriels non sollicités et être prudent avec les pièces jointes et les liens.

Il est difficile, voire utopique de prévoir une réponse adaptée à chaque type de cyberattaque, et ceci pour au moins trois raisons, la première étant que le mode opératoire utilisé peut être insolite. La créativité des cybercriminels est sans limites et l'actualité leur sert souvent de point d'appui. La crise d'approvisionnement en énergie dans laquelle nous entrons en est sans aucun doute une illustration.

La deuxième raison concerne le moment où une attaque va se produire, qui ne peut être prédit. De plus, contrairement à ce que l'on pourrait croire, une cyberattaque ne se déroule pas toujours en un instant, mais sur plusieurs jours, voire semaines, le temps nécessaire aux cybercriminels pour bien interpréter l'environnement dans lequel ils pénètrent et trouver la tactique la plus à même de leur garantir un gain maximal.

Enfin, la surface d'attaque ne cesse de s'étendre. La numérisation de la plupart des processus ainsi que la multiplication des objets connectés, parfois à l'insu de l'organisation, ainsi que les données qui y sont traitées, ne font qu'augmenter le terrain de jeu des cybercriminels, rendant une couverture sécuritaire complexe.

UN CONSTAT IMPLACABLE

Prévenir la cybercriminalité ne suffit pas! Certes, chaque organisation doit se doter d'équipements et de logiciels qui soient en permanence mis à jour. De même, l'entreprise doit veiller à tenir ses processus de travail à jour afin qu'ils intègrent de manière cohérente la dimension numérique. Et tous les acteurs de l'organisation doivent impérativement comprendre les enjeux liés à la cybercriminalité et adopter des comportements responsables et éclairés lorsqu'ils traitent des informations.

Mais il est désormais indispensable de préparer l'organisation à réagir face à une cyberattaque afin de développer sa résilience face à des événements qui risquent fort de produire des effets qu'elle n'aura pas pu entièrement empêcher atténuer. Connaître les processus essentiels, savoir comment assurer leur fonctionnement en «mode dégradé» et se préparer à les mettre en œuvre est désormais indissociable d'une politique de prévention efficace en entreprise.

OLIVIER BEAUDET-LABRECQUE ET SÉBASTIEN JAQUIER
Doyens de l'Institut de Lutte contre la criminalité économique (ILCE), Haute École de gestion Arc

L'ILCE PROPOSE SON EXPERTISE

Compte tenu de la hausse soutenue des cas de cybercriminalité en Suisse et des importantes conséquences qui peuvent en découler, toute organisation, indépendamment de sa taille, se doit de prendre en considération ces risques. Il n'est jamais trop tard pour commencer à thématiser ce sujet. La formation du personnel et la prise en compte des risques dans les différents processus sont des premiers pas tout à fait indiqués.

En ce sens et si vous le désirez, il vous est possible de prendre contact avec l'Institut de lutte contre la criminalité économique (ILCE) de la Haute École de gestion Arc pour obtenir des conseils adaptés ou des pistes de réflexion. Vous pouvez atteindre l'ILCE par courriel **ilce@he-arc.ch**, ou par téléphone au 032 930 20 15.