LA PANDÉMIE, PAIN BÉNI POUR LES CYBERCRIMINELS

Mis en place dans l'urgence, le télétravail a déclenché la multiplication des cyberattaques, fraudes en ligne et autres cyberextorsions, dont le nombre depuis mars 2020 a explosé. La prise de conscience de l'ampleur du phénomène semble pourtant demeurer bien en deçà de ce qui serait nécessaire, pour mettre des bâtons dans les roues aux malfrats. Qui eux, s'en frottent les griffes.

Nul besoin de briser des vitres ou de faire sauter des verrous pour opérer ce genre de « casse » : l'approche se fait moyennant des clics de souris. Le cybercriminel surfe non seulement sur notre naïveté – la majorité des fraudes demandent la collaboration de la victime – mais aussi sur notre incompétence en la matière.

Il est rarissime qu'un pirate informatique soit pris la main dans le sac. La plupart du temps, on découvre son passage des mois plus tard. Selon un récent rapport d'IBM, il faut en moyenne 280 jours aux entreprises pour remarquer une fuite de données. Neuf mois – chiffre on ne peut plus symbolique – durant lesquels le hackeur dispose de tout son temps pour affiner la suite des opérations, avant de porter l'estocade finale. Après nous avoir espionné (et infecté) durant des mois, et lorsque la « bombe » explose, les effets sont la plupart du temps dévastateurs. Listage non-exhaustif des dommages : du jour au lendemain, perte de documents confidentiels et de données stratégiques, fuite d'infos compromettantes, vol d'adresses et de contacts, plus de connexion internet ni de courriels, plus de ligne téléphonique, un système de gestion paralysé et donc plus de livraison, de paiement ni de commande possible. Certains spécialistes, telle l'incontournable Solange Ghernaouti, professeure à l'université de Lausanne et experte internationale en cybersécurité et cyberdéfense, estiment que le coût total de la cybercriminalité représente approximativement 1% du produit intérieur brut (PIB) des pays. Le PIB de la Suisse s'élevait en 2019 à 726'921 millions de francs (chiffre OFS). Un simple calcul permettra d'évaluer les dégâts occasionnés, et cela en temps normal.

La force du diable : faire croire qu'il n'existe pas

Avant la pandémie, le nombre de cyberattaques dans le monde évoluait déjà fortement à la hausse, dans une indifférence quasi généralisée. Une incroyable et inexplicable naïveté que même de grands groupes, entreprises et institutions ont payé au prix fort. Que l'on se souvienne, à titre d'exemple et pour ne parler que de ceux-là, du géant horloger Swatch Group (septembre 2020, dont la production s'est vue fortement entravée), de la compagnie d'aviation britannique EasyJet (mai 2020, vol des données de 9 millions de clients), ou encore du détournement de salaires d'employés de plusieurs universités alémaniques (octobre 2020). Rien qu'en Suisse, les cas se comptent par milliers, mais la plupart du temps, afin de ne pas nuire à leur image ou se décrédibiliser sur la scène publique, les victimes évitent soigneusement de crier leur mésaventure sur les toits. Ce qui ne contribue pas vraiment à une prise de conscience à plus grande échelle.

On se dira peut-être que l'on peint le diable sur la muraille. Erreur : la force no.1 du « diable » est de faire croire qu'il n'existe pas. Quant aux cybercriminels, leur force de frappe réside dans la supposition (bien répandue) qu'ils en sont encore au stade du hacker artisanal – alors qu'en réalité, ils ont franchi le cap de l'échelon industriel. Depuis le déferlement du SARS-CoV-2, le nombre d'incidents de cybersécurité a pris l'ascenseur. Le fameux télétravail, avec ses dizaines de milliers d'employés isolés, a démultiplié les points d'entrée dans les systèmes informatiques des entreprises. Autant de brèches par où les pirates s'infiltrent encore plus aisément. A la mi-mars 2020, date du début du télétravail recommandé, le nombre d'incidents de cybersécurité déclarés au Centre national pour la cybersécurité (NCSC) était déjà de 150 par semaine. (Une centaine, en temps normal.) A la mi-mai, ce chiffre atteignait les 400 cas hebdomadaires. A la fin du télétravail recommandé (fin juin), 250 cas étaient signalés au NCSC. Jusqu'à la fin de l'année 2020, le nombre de cas hebdomadaires (déclarés) fluctuait autour des 200, avec un pic à 270 à la mi-août. Notons que ces chiffres ahurissants ne trouvent pas seulement leur explication dans la multiplication des points d'entrée dans les systèmes informatiques des entreprises. Il y a ici un effet boule de neige : peu de moyens technologiques suffisent au cybercriminel pour multiplier le nombre de personnes ou d'entreprises touchées par une seule action. En d'autres mots : une fois dans la forteresse, le hacker en profitera pour repérer d'autres cibles, dont il étudiera et évaluera les faiblesses.

Le cybersniper fait feu de tout bois

La méthode d'une personne malintentionnée est de vous faire croire que ses intentions sont innocentes. C'est la stratégie adoptée par les cybercriminels. Ainsi le 90 % des cyberattaques débutent par du « phishing » (hameçonnage en bon français), technique consistant à faire croire à la victime qu'elle s'adresse à un contact auquel elle peut, ou devrait, faire confiance : banque, administration, chef d'entreprise, etc. Objectif : lui soutirer des renseignements confidentiels tels que numéros de carte de crédit, mots de passe, photocopie de carte d'identité, adresses électroniques et ainsi de suite. Stéphane Koch, spécialiste de la sécurité de l'information et vice-président d'Immuniweb – entreprise suisse spécialisée dans la cybersécurité – cite à titre d'exemple le cas d'une entreprise française victime d'une usurpation d'identité : se faisant passer pour le dirigeant de l'entreprise, le cybercriminel en

question a obtenu le versement d'un million et demi d'euros à l'étranger. Une année plus tard, la société a dû mettre les clés sous la porte, jetant des dizaines d'employés à la rue.

L'exemple montre non seulement que le cybercriminel fait feu de tout bois, visant les grandes entreprises jusqu'aux plus petites, mais aussi qu'une seule couche de protection (le fameux « informaticien responsable », travaillant en solo) ne suffit plus pour assurer un niveau de sécurité efficient. En 2016 déjà, dans une brochure de la Prévention Suisse de la Criminalité (PSC), le même Stéphane Koch soulignait l'importance « d'adopter une approche multiniveau de la sécurité », c. à d. impliquant un plus grand nombre d'acteurs capables de détecter et de neutraliser les attaques ciblant les postes de travail. « Ce qui fait la différence entre un pays et un autre, signalait-il, ce sont les moyens que ce pays va mettre en œuvre pour lutter contre la cybercriminalité ou d'autres formes d'attaques initiées par le biais des réseaux connectés, ainsi que le niveau de conscience de ses citoyens et des entreprises. Et dans ce domaine, la Suisse est à la traîne ! Il y a des manquements considérables dans les moyens de lutte contre la cybercriminalité, et le niveau de connaissance et de réactivité des entreprises et des individus est largement insuffisant. »

Mieux vaut agir en amont que de réagir en aval

Au train où vont les choses, la question n'est donc plus de savoir si un jour une entreprise se retrouvera dans le collimateur d'un cybersniper, mais QUAND. De se dire : « Ce genre de mésaventure, ça n'arrive qu'aux grandes boîtes », équivaut à signer son propre arrêt de mort. Il vaudrait mieux signer un contrat auprès d'une assurance, dont les prestations pourraient nous éviter le pire, tel un airbag qui nous sauve la vie en cas d'accident. Là aussi, force est de constater qu'insouciance et naïveté prévalent – même si les coûts de tels compléments d'assurance (des couvertures pourtant bien ficelées, pour les privés comme pour les PME, cf. internet), sont dérisoires. « Les clients plus jeunes ont de la peine à être sensibles à cette problématique, ils se sentent tout-puissants, témoigne Allan Briet, responsable de vente chez AXA à Delémont. La prise de conscience évolue un peu avec l'âge, mais le nombre de personnes qui arrivent spécifiquement à notre agence pour acquérir une couverture reste néanmoins très faible ! Même phénomène en ce qui concerne les entreprises. Et pourtant, nous passons notre temps à attirer l'attention de nos clients sur ce type de menace. Evidemment, chacun est libre d'agir comme il l'entend. »

Olivier Léchenne, Agent général de La Mobilière à Delémont confirme : « Nous savons bien que les hackeurs n'ont pas chômé lors de cette pandémie et que le nombre d'attaques continue à se multiplier. Il est donc du devoir de l'assureur d'attirer l'attention de ses clients sur les dangers encourus. Parce qu'à moins d'avoir été victime lui-même d'une cyberattaque, le client ne viendra pas de son propre chef pour demander une couverture. Pourquoi ? Parce que l'on pense trop souvent que ce genre de drame n'arrive qu'aux autres. Mais posez vous la question : si ce matin j'arrive au travail et que mon écran est tout noir, et que rien ne bouge plus, qu'est-ce que ça impliquerait ? Il n'y a pas besoin de diriger une entreprise de 200 personnes pour comprendre l'ampleur d'un tel drame. L'activité d'un simple salon de coiffure se verrait entravée net de la même façon.»

Pablo Davila

RAPPEL DES 5 RÈGLES DE BASE POUR VOTRE SÉCURITÉ NUMÉRIQUE

Nous le savons, mais il est bon de le rappeler : des logiciels malveillants cherchent constamment à infiltrer nos ordinateurs, tablettes et smartphones, sur lesquels nous stockons toutes sortes de données personnelles et confidentielles, mots de passe, numéros de carte de crédit, photos, etc., etc., en usant des moyens technologiques toujours plus sophistiqués. Aussi pensez toujours à...

1. Sauvegarder les données

Suppression accidentelle, défaut technique du disque dur, vol ou perte de votre dispositif, logiciels malveillants qui circulent dans l'internet (virus, vers, chevaux de Troie), infiltration d'un hacker : on ne peut jamais exclure l'éventualité que nos contenus puissent être perdus un jour. Sauvegardez régulièrement vos données sur un disque dur externe, sur DVD, CD ou bien sur une plateforme de stockage en ligne (cloud), en vérifiant qu'elles ont bien été copiées.

2. Surveiller avec l'antivirus et le pare-feu

Quelles « portes » votre dispositif laisse-t-il ouvertes et quels virus viennent s'y présenter ? Si vous avez activé un pare-feu et installé un programme de protection antivirus, activant aussi la fonction de mise à jour automatique, pratiquement aucune. Vérifiez régulièrement que votre dispositif n'a pas été infecté en procédant à un scan complet du système. Activez le pare-feu embarqué de Windows ou mac OS avant de connecter votre dispositif à Internet (ou à tout autre réseau).

3. Prévenir avec les mises à jour logicielles

Veillez à ce que votre système d'exploitation, de même que vos programmes et applications soient régulièrement mis à jour. Les programmes obsolètes présentent trop souvent des failles de sécurité, ce qui facilite la tâche des hackers cherchant à infiltrer et/ou à prendre le contrôle de votre dispositif. N'installez que les programmes et applications dont vous avez vraiment besoin et assurez-vous qu'ils proviennent de sources sûres, c'est-à-dire directement de l'éditeur ou des stores officiels (p. ex. Apple App Store ou Google Play Store).

4. Créér des mots de passe solides

Pour vos mots de passe, évitez les prénoms d'enfants, les noms d'animaux, les dates de naissance, les adresses, etc. L'idéal est de créer une combinaison arbitraire d'au moins 10 caractères contenant à la fois des lettres majuscules et minuscules, des chiffres et des caractères spéciaux. N'utilisez pas partout le même mot de passe : il faut en composer un pour chaque compte et ne jamais les communiquer à qui que ce soit. Si vous craignez ne plus vous en souvenir, conservez-les par écrit dans un lieu sûr.

5. Ne jamais baisser la garde

Sans devenir paranoïaque, montrez-vous toujours prudent lorsque vous surfez sur Internet et réfléchissez bien avant de communiquer vos données personnelles. Jamais aucun institut financier, opérateur téléphonique ou autre fournisseur de service véritable ne vous demandera (ni par courriel, ni par téléphone) de communiquer un mot de passe, ou de les modifier. En utilisant vos dispositifs mobiles, appliquez les mêmes mesures de précaution que celles utilisées sur votre ordinateur fixe