Les cyberattaques à l'heure du coronavirus

le 21 mars 2020
PÉNAL
EUROPÉEN | Pénal

Auteur : Myriam Quéméner et Clément Wierre

Au milieu des nombreuses communications officielles du ministère de l'intérieur de ces derniers jours, celle relative à l'augmentation du risque « cyber » et alertant les utilisateurs à « redoubler d'attention pour ne pas tomber dans [les] pièges » serait presque passée inaperçue. Pourtant, la menace est réelle.

L'ensemble des acteurs de la cybersécurité notent depuis plusieurs semaines une recrudescence des fraudes informatiques, en particulier celles utilisant très directement le covid-19 comme vecteur frauduleux.

Les fraudes ayant pour objet le covid-19

Le phénomène n'est pas nouveau : que ce soit le tsunami de 2004 en Asie ou le tremblement de terre en Haïti de 2010, les grandes catastrophes sont systématiquement exploitées par les cybercriminels à des fins pécuniaires ou d'espionnage.

Bien que cela puisse paraître contre-intuitif, l'une des premières failles exploitées par les cybercriminels demeure l'humain. Fort d'un travail d'ingénierie social abouti, les groupes de cybercriminels n'hésitent pas à jouer sur le registre émotionnel – la peur et l'urgence générée par toute catastrophe sanitaire – pour parvenir à leurs fins.

Le covid-19 n'échappe pas à la règle, la multiplication des *fake news* et l'augmentation des noms de domaine liés au coronavirus en sont des indices forts. D'ailleurs, le 16 mars 2020, la cellule d'accompagnement cybersécurité des structures de santé (ACSS) de l'Agence du numérique en santé (ANS) a publié une alerte indiquant que « le coronavirus est utilisé pour réaliser des cyberattaques ».

Ainsi, l'on ne compte plus les tentatives d'hameçonnage (*phishing*) ayant pour appât le virus. Cette forme d'escroquerie consiste à créer un message avec une apparence officielle (logo d'une organisation mondiale ou d'une ONG), à y inclure un lien malveillant ou un fichier vérolé que le destinataire sera incité à suivre ou télécharger et, enfin, à adresser ce message au plus grand nombre par plusieurs vecteurs (courrier électronique, Messenger, Whatsapp, etc.).

Plusieurs objectifs peuvent être poursuivis : le vol d'informations sensibles, de données bancaires *via* un lien renvoyant vers un faux site, imitant par exemple celui d'une banque, le téléchargement d'un logiciel dit *ransomware*, prenant en otage – par cryptage – les données de la cible et imposant le paiement d'une rançon pour obtenir le déchiffrement.

À date, il existe peu de retours sur les formes de *phishing* ayant commencé à sévir en France mais il semblerait que des invitations à télécharger des attestations de sortie sur des sites non officiels aient pu être utilisées. À l'étranger, IBM a identifié de faux courriers électroniques d'autorité de santé invitant à télécharger un bulletin de santé comportant un cheval de Troie bien connu, Emotet, qui permet aux hackers d'installer par la suite d'autres logiciels, notamment *ransomware*.

À noter également, le développement de sites marchands proposant la vente de produits en rupture (en particulier masques ou gel hydroalcoolique) sans jamais opérer la livraison. Au-delà de la déconvenue d'avoir réglé un achat qui ne sera jamais livré, les utilisateurs s'exposent à l'utilisation frauduleuse de leurs coordonnées bancaires.

Le covid-19, un facilitateur de fraudes numériques

Sans même utiliser directement le covid-19 comme vecteur d'une attaque ou d'une fraude, les cyberdélinquants voient dans la situation de crise générée par le virus une aubaine.

Le recours massif au télétravail et l'installation à la hâte d'une connexion à distance sont des facteurs aggravants du risque de fuite d'informations confidentielles ou d'identifiants de connexion. En particulier, et ainsi qu'identifié par le Département de la sécurité intérieure des États-Unis, l'utilisation massive de VPN (*virutal private network*) est susceptible d'accroître les failles, en particulier si l'entreprise renonce à sa mise à jour régulière afin d'éviter toute interruption de services.

En parallèle, les services informatiques des sociétés sont fortement mobilisés par la nécessité d'assurer la continuité de l'activité de l'entreprise grâce au télétravail alors que les infrastructures apparaissent sous-dimensionnées pour l'usage actuel. L'impératif de sécurité informatique peut alors être relayé au second plan et, bien que temporaire, une telle négligence peut se payer très cher.

Enfin, d'autres fraudes telles que les faux ordres de virement (FOVI) risquent de réapparaître massivement alors qu'une accalmie s'était dessinée ces dernières années. Bien que n'étant pas à proprement parler de la cybercriminalité, il est indéniable que l'outil informatique – en particulier les échanges de courriers électroniques – est un facilitateur des FOVI.

Pour rappel, il peut s'agir d'une « fraude au président » visant à convaincre le collaborateur d'une entreprise d'effectuer en urgence un virement important à un tiers sur ordre du dirigeant ou bien encore d'une fraude au « changement de RIB » qui consiste pour les fraudeurs à envoyer un courrier électronique à un salarié du service de comptabilité ou de trésorerie de l'entreprise en se faisant passer pour un fournisseur, et lui demander de diriger ses versements vers un autre compte bancaire appartenant aux escrocs, basés le plus souvent à l'étranger.

La période actuelle favorise ce type de fraude dès lors que le départ précipité de nombreux collaborateurs conduit à une désorganisation des services financiers ou comptables et que les vérifications « physiques » sont rendues complexes.

Dans une économie fragilisée, tout faire pour éviter l'effet dévastateur d'une cyberfraude ou d'une cyberattaque

Alors qu'il est indéniable que les entreprises s'apprêtent à traverser une crise économique sans précédent, il est impératif d'éviter le « suraccident » que représenteraient des cyberfraudes ou des cyberattaques massives.

Rappelons simplement qu'à lui seul, le *ransomware* WannaCry aurait causé en 2019 un préjudice de 4 milliards de dollars au niveau mondial. S'il est difficile d'obtenir un chiffre pour les seules entreprises françaises, l'exemple du géant Saint-Gobain est intéressant : le groupe a en effet estimé à 250 millions d'euros le préjudice causé par l'attaque qu'elle a subie à l'aide du *ransomware* NotPetya.

Autre information inquiétante dans le contexte : l'Agence nationale de sécurité des systèmes d'information (ANSSI) a traité dix-huit incidents liés à des rançongiciels dans la santé en 2019, ce qui en fait le secteur le plus visé, selon un rapport du centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR).

Aussi, il est impératif que les opérateurs de services essentiels (OSE) intervenant dans les secteurs tels que l'énergie, les transports, la santé ou le secteur bancaire respectent à un degré d'exigence accru les obligations qui leur incombent au titre de la directive NIS, transposée en France par la loi n° 2018-133 du 26 février 2018.

Sur le plan des libertés individuelles, mentionnons la vigilance de mise à la suite de

l'assouplissement jusqu'au 30 avril 2020 prévu par décret (n° 2020-227, 9 mars 2020, adaptant les conditions du bénéfice des prestations en espèces d'assurance maladie et de prise en charge des actes de télémédecine pour les personnes exposées au covid-19) des modalités de réalisation des actes de télémédecine. Cette situation inquiète les spécialistes de la protection des données de santé. Les téléconsultations peuvent être réalisées en utilisant n'importe lequel des moyens technologiques actuellement disponibles pour réaliser une vidéotransmission (lieu dédié équipé mais aussi site ou application sécurisé *via* un ordinateur, une tablette ou un smartphone, équipé d'une webcam et relié à internet).

Aussi, à l'occasion du débat sur le projet de loi sur l'état d'urgence sanitaire, les sénateurs Patrick Chaize et Bruno Retailleau ont réintroduit un amendement – bien que rejeté le matin même par la commission des lois – visant à faciliter la collecte et le traitement des données de santé durant six mois.

Encore une fois, l'urgence et la peur ne sauraient justifier un relâchement des obligations incombant aux opérateurs, en particulier lorsqu'il s'agit du traitement de données aussi sensibles que les données de santé.

Rappel des « gestes barrières » en matière informatique

Certes, certains hackers ont annoncé une trêve des attaques informatiques en cette période de crise mais cela est très loin d'être suffisant.

Il n'est pas inutile de rappeler l'existence de sites officiels d'information sur les cyberattaques comme la plateforme d'information du public et des PME sur le risque « cyber ». Il met notamment en garde contre les risques d'utilisation de la thématique coronavirus par les cybercriminels et qui présentent des conseils essentiels pour ne pas se faire piéger.

Aussi, l'agence nationale de sécurité des systèmes d'information (ANSSI) a publié un guide du nomadisme numérique. Le guide rappelle les définitions et les risques liés en la matière, puis étudie les différents éléments d'une infrastructure de connexion nomade pour en faire ressortir les bonnes pratiques.