Le Point

Le Point.fr, no. 202004
Mon petit droit m'a dit, mercredi 15 avril 2020 1940 mots

Cybercrime : « La vulnérabilité en mode télétravail est bien plus importante »

Par Laurence Neuer

Comment faire face aux cyberattaques favorisées par le confinement et par l'usage intensif des outils de télétravail ? Les réponses de deux avocats spécialistes.

« Restez zen ! » Ce conseil adressé aux particuliers et entreprises sur la plateforme gouvernementale dédiée aux cyberattaques n'est pas superflu à l'heure où, alors que la France entre en récession, le marché du cybercrime est en pleine euphorie. « 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 [...]. Ceux-ci jouent sur le registre émotionnel - la peur et l'urgence générée par toute catastrophe sanitaire - pour parvenir à leurs fins », écrivent la magistrate Myriam Quéméner et l'avocat Clément Wierte dans la revue Dalloz du 9 avril 2020.

Le recours massif au télétravail est une aubaine pour les cybercriminels. « N'ayant pas pu anticiper la situation, beaucoup d'entreprises ont mis en place dans l'urgence des protections plus ou moins artisanales, ce qui les rend vulnérables aux cyberattaques. Même celles qui sont habituées au télétravail doivent faire face à des risques d'intrusion dans les systèmes informatiques et de vol d'informations confidentielles de nature à engager leur responsabilité », préviennent Frank Valentin et Jean-Guy de Ruffray, avocats associés du cabinet Altana. Quelles sont les attaques les plus fréquentes ? Comment s'y préparer ? Que faire en cas d'intrusion dans son système informatique (SI) ? Entretien.

Lire aussi Cyberattaque : les hôpitaux, ces avant-postes de la bataille à sécuriser d'urgence

Le Point : D'après certains experts, c'est l'hameçonnage (phishing) qui a le vent en poupe. En quoi consiste cette escroquerie et quel en est l'objectif ?

Jean-Guy de Ruffray : C'est assez simple, vous recevez un message par e-mail, SMS ou encore par chat, qui a toutes les apparences officielles d'une banque ou d'une organisation internationale. Mis en confiance, vous tombez dans le panneau d'un lien ou d'un fichier à télécharger, ce qui permet au cybercriminel d'atteindre son objectif avec votre coopération : dérober vos informations confidentielles, vos mots de passe, et tous types de données personnelles sensibles, notamment bancaires !

Autre technique, encore plus pernicieuse : le ransomware avec paiement d'une rançon...

Frank Valentin : Ici, on passe à un système plus sophistiqué : ce type d'attaques suppose une intrusion sur le réseau de l'entreprise par ses accès à distance (parfois d'ailleurs par du phishing), en particulier par le biais de l'équipement d'un collaborateur distrait ou négligent. L'attaque consiste à identifier des données clés de l'entreprise, relatives à son fonctionnement, à ses comptes, à ses projets stratégiques, que le cybercriminel neutralise en les cryptant, les rendant inaccessibles ou inexploitables. Elles font alors l'objet de menaces de divulgation, de destruction ou de confiscation contre le versement d'une forte rançon, que l'entreprise est contrainte de payer afin que ses systèmes d'information échappent à la paralysie. Le ransomware s'accompagne de plus en plus souvent d'un vol ou d'une perte de données, et souvent d'une destruction des sauvegardes.

Une autre escroquerie est aussi à anticiper dans cette période : les faux ordres de virement (FOVI/BEC), via le piratage d'un compte de messagerie électronique ou par contact téléphonique d'une entreprise, prenant la forme de l'usurpation d'identité d'un dirigeant ou de l'un de ses mandataires, d'un fournisseur ou d'un prestataire, voire d'un collaborateur. Elle permet concrètement d'obtenir un virement exceptionnel et confidentiel, ou un changement des coordonnées de règlement (RIB) d'une facture ou de salaires.

Beaucoup d'attaques sont liées à de fausses annonces de vente de masques ou de gel hydroalcoolique.

Ces attaques sont d'autant plus probables qu'en cette période anxiogène les réactions individuelles ne sont pas toujours raisonnées...

Jean-Guy de Ruffray : C'est exact, la vulnérabilité en mode « télétravail » est bien plus importante de ce point de vue qu'au sein de l'entreprise : les outils à appréhender, l'éloignement physique des personnes, le nouvel environnement de travail, créent de la fragilité. Seul chez soi, on reçoit un mail d'hameçonnage, c'est-à-dire sous une fausse identité numérique pour un appel au don, par exemple, on est tenté de cliquer ou de répondre, et involontairement de créer un accès au système d'information. Dans le contexte de la crise sanitaire actuelle, beaucoup d'attaques sont liées à de fausses annonces de vente de masques ou de gel hydroalcoolique. Donc, on peut plus facilement se faire piéger. Et dès lors que l'ordinateur du salarié est connecté au réseau d'information de l'entreprise, c'est potentiellement coup double.

Lire aussi Phébé - Pourquoi il faut craindre les cybermercenaires

À ce péril s'ajoutent les sanctions encourues par l'entreprise...

Jean-Guy de Ruffray : L'entreprise risque la double peine avec un risque économique, voire réglementaire ! Un risque économique puisque la cyberattaque peut entraîner des fuites de données vers la concurrence, des violations du secret des affaires, etc. S'y ajoute un risque réglementaire qui touche cette fois à la question de la protection des données personnelles. En cas de captation de données à caractère personnel du fait d'une cyberattaque, l'entreprise a, en effet, l'obligation de notifier cette faille à la Cnil dans les 72 heures. Elle encourt des sanctions dès lors qu'elle ne le fait pas, et d'autres encore s'il est établi qu'elle n'a pas suffisamment sécurisé l'accès à son système d'information, et ce, même si elle a eu recours à un prestataire. Elle doit aussi informer les personnes dont les données ont été détournées, dès lors qu'il y a un risque d'atteinte à leur vie privée.

Quels cybergestes barrières préconisez-vous ?

Jean-Guy de Ruffray : Ce sont des réflexes tels que l'utilisation de VPN et d'antivirus, la restriction de l'accès au SI de l'entreprise à certains collaborateurs, la mise en place de systèmes de verrouillage automatique pour éviter qu'un enfant n'accède au poste de ses parents. La dimension humaine est ici très importante. C'est pourquoi certaines entreprises ont mis en place des tests pour « coacher » leurs salariés et mesurer leurs réactions en situation réelle lorsqu'ils reçoivent des mails frauduleux.

Dans la vie rêvée, pour cantonner les risques de phishing, chacun devrait avoir un ordinateur exclusivement professionnel sur lequel n'entre aucun mail personnel, afin de limiter les risques de phishing - qui ne seraient pas exclus, tant les adresses électroniques professionnelles font l'objet de collectes sauvages -, chacun devrait sauvegarder ses dossiers sur un disque dur externe à la fin de chaque journée pour limiter les risques de ransomware.

L'application de vidéoconférence Zoom est actuellement sous les feux des critiques. En cause, ses failles de sécurité, les entorses à la confidentialité des échanges, etc. Le ministère de la Défense britannique a d'ailleurs interdit à ses employés de l'utiliser...

Frank Valentin : En effet, la plateforme Zoom a vu son nombre d'utilisateurs quotidiens passer de 10 millions à 200 millions au cours des trois derniers mois. Et, de l'aveu même de son fondateur et PDG, Eric Yuan, Zoom a été submergée par son propre succès. Or, Zoom est confrontée depuis quelques semaines à une série de failles de sécurité. Les critiques se sont, de fait, multipliées, à la suite d'actes de « Zoombombing », consistant à faire irruption dans des téléconférences pour les perturber, en proférant des propos inadéquats ou en diffusant des contenus de type pornographique, selon certaines sources citant les investigations de la police fédérale américaine. Des défenseurs de la vie privée, des experts en sécurité, plusieurs procureurs généraux d'États américains, dont celui de New York, le FBI et des parlementaires américains ont ainsi révélé ces incidents au monde entier.

Lire aussi Coronavirus : les meilleures applications pour garder le contact

Sans parler des options de mouchard qu'offre l'outil permettant aux administrateurs d'enregistrer le contenu de vidéoconférences, de contrôler les connexions au service ou l'assiduité des participants à une telle

vidéoconférence. Enfin, Zoom entretient des relations particulières avec la Chine où se trouve notamment située la société ayant développé l'outil ainsi que les serveurs hébergeant et distribuant les clés de chiffrement du logiciel. Des chercheurs nord-américains ont pu identifier que des données échangées par ses services transitent par la Chine.

Lire aussi Jitsi, le service né en France qui veut vous faire oublier Zoom et Houseparty

Que conseillez-vous aux entreprises qui veulent échanger par visioconférence ?

Frank Valentin : En règle générale, je préfère les outils dont le chiffrement est une priorité, comme Jitsi Meet, logiciel libre, développé par un Français et désormais propriété d'une société américaine, dont le principe repose sur un chiffrement utilisant un protocole fiable, DTLS-SRTP (pour Datagram Transport Layer Security) conçu pour protéger les données privées transitant sur les réseaux de communications. Scaleway, la filiale d'Iliad (Free) a mis au service de l'État ses solutions cloud comprenant une plateforme spéciale de visioconférence fondée sur Jitsi et très performante. Microsoft Teams permet également d'échanger des fichiers, des messages écrits ou du contenu audio de manière fiable et efficace.

La constatation des faits litigieux en ligne est entravée par l'indisponibilité des huissiers de justice.

Que faire si on a été attaqué ? Le signaler à la police ?

Frank Valentin : Pour l'heure, les autorités sont très mobilisées par les questions sanitaires, et notamment les violations des ordonnances prises en application de la loi d'urgence du 23 mars 2020. La commercialisation en ligne de produits de santé irréguliers, la distribution illicite sur des sites Internet douteux de dispositifs médicaux en fraude des décrets de réquisition sont notamment des sujets de préoccupation de la police et du parquet. Les services de police (la Befti à Paris) et de gendarmerie (l'OCLCTIC) sont néanmoins conscients de la multiplication des actes de cybermalveillance à l'encontre des systèmes d'information des entreprises et des particuliers et de la nécessité d'agir en protection. La coopération avec les autorités de police des États d'où proviennent nombre d'attaques est aussi problématique. En temps normal très efficace, elle a pu marquer un coup d'arrêt, notamment avec les États étrangers à l'UE en raison des positions de repli.

D'un point de vue judiciaire, il faut également relever que tous les tribunaux français sont fermés ou tournent au ralenti, se concentrant sur les cas d'extrême urgence et la sécurité physique des personnes. La constatation des faits litigieux en ligne, élément probatoire important et préalable aux poursuites, est en outre entravée par l'indisponibilité des huissiers de justice. La prévention est donc plus que jamais la meilleure alliée de l'entreprise.

Le règlement sur la protection des données personnelles (RGPD) n'est-il pas sous-dimensionné en temps de confinement ?

Frank Valentin : Un certain nombre d'outils ou leurs utilisations ne sont pas tous « RGPD compatibles ». Par exemple, l'explosion des cours scolaires en ligne depuis la mi-mars 2020 a généralisé l'accès de jeunes enfants à Internet dans un contexte de système D généralisé. Et les outils d'accès proposés aux écoliers peuvent à l'évidence constituer des traitements de données personnelles, au sens de la loi française et de la législation européenne. Or, en France, où la « majorité numérique » de l'enfant est de 15 ans, ce traitement n'est licite que si le consentement est donné par le titulaire de l'autorité parentale. Le responsable du traitement, c'est-à-dire l'éditeur de l'outil, doit donc s'efforcer de vérifier qu'un consentement approprié est bien donné, ce qui est loin d'être le cas, en particulier dans l'urgence des premiers jours de la crise sanitaire.

Jean-Guy de Ruffray : Autre problématique : les données de santé des salariés. On peut imaginer que nombre de grands groupes sont amenés à procéder à la collecte massive de données de santé des salariés infectés. Cette collecte exceptionnelle, par temps de pandémie mondiale, des informations qu'on ne collecte pas habituellement, va probablement nécessiter un travail d'assouplissement réglementaire. Le RGPD étant très contraignant, la Cnil devra faire preuve de souplesse pour les besoins de la cause.

À savoir : le site gouvernemental https://www.cybermalveillance.gouv.fr informe les entreprises sur les menaces numériques et leur donne des conseils pour y faire face.