Vivre avec les cyberattaques, le mythe de Sisyphe renouvelé ?

par

Laurent Oudot
Co-fondateur et directeur technique, TEHTRIS

Marie Le Pargneux
Chief Development Officer, TEHTRIS

En bref

Il est des menaces que l'on rêve d'éradiquer et d'autres avec lesquelles il est plus raisonnable d'apprendre à vivre. C'est le cas de la Covid-19. C'est également le cas des cybermenaces. D'ailleurs, les virus informatiques imitent de plus en plus leurs "cousins" biologiques. Les experts opérationnels en cybersécurité luttent au quotidien contre ces attaques en vagues répétées. Parfois, les moyens manquent, le confinement est illusoire et le découragement guette. Pourtant, le lendemain, il faut bien reprendre sa pierre et la rouler tel un Sisyphe moderne qu'il faut sans doute imaginer heureux. Comment les entreprises peuvent-elles s'attacher l'abnégation de tels experts ? Ne devrions-nous pas tous avoir comme obligation minimale d'écouter leurs recommandations et leurs alertes, ne serait-ce que pour les aider à ne pas être submergés ? Ne faudrait-il pas repenser sérieusement notre manière de numériser le monde ?

Compte rendu rédigé par Pascal Lefebvre

L'Association des Amis de l'École de Paris du management organise des débats et en diffuse les comptes rendus, les idées restant de la seule responsabilité de leurs auteurs. Elle peut également diffuser les commentaires que suscitent ces documents.

Séminaire organisé grâce aux parrains de l'École de Paris du management :

Algoé[1] • Chaire Futurs de l'industrie et du travail • Chaire Mines urbaines • Danone • EDF • Else & Bang • ENGIE • Executive Master – École polytechnique • Fabernovel • Groupe BPCE • Groupe OCP • GRTgaz • IdVectoR[2] • IPAG Business School • L'Oréal • La Fabrique de l'industrie • MINES ParisTech • RATP • Syndicat des entreprises de l'économie numérique et des technologies nouvelles[3] • université Mohammed VI Polytechnique • UIMM • Ylios[1]

1. pour le séminaire Vie des affaires / 2. pour le séminaire Management de l'innovation / 3. pour le séminaire Transformations numériques

© École de Paris du management – 60, boulevard Saint-Michel – 75272 Paris Cedex 06
Tél. : 01 42 79 40 80 – e-mail : contact@ecole.org – www.ecole.org

Un changement de paradigme

Marie LE PARGNEUX : L'environnement de la cybersécurité est à la fois fascinant, vertigineux et éminemment complexe. Il nous faut vivre avec. Depuis un an que j'ai intégré l'entreprise TEHTRIS, je suis témoin de l'impact que cet univers a sur nos clients et partenaires, mais aussi sur l'ensemble des collaborateurs, sur notre manière de travailler et de vivre ensemble.

On estime qu'environ 300 000 nouveaux types d'attaques émergent quotidiennement dans le monde. Depuis le début de l'année 2020, on note une augmentation de 667 % des attaques par *phishing*. On s'attend à ce que le marché de la cybersécurité passe de 173 à 270 milliards de dollars d'ici 2026. Les pertes des entreprises, du fait de ces attaques, pourraient atteindre 6 000 milliards de dollars en 2021. Ces chiffres sont colossaux et l'on peine à en prendre la pleine mesure et à en préciser la véracité. Quantité d'études se penchent sur ce sujet et bien que les écarts entre leurs conclusions soient souvent considérables, toutes montrent que le monde a profondément changé du fait de cette cybercriminalité.

Néanmoins, découvrant depuis un an cet univers, ce ne sont pas ces chiffres qui me marquent le plus. Deux faits majeurs, survenus cet été, me paraissent essentiels. Tout d'abord, il y a quelques jours, pour la première fois, la responsabilité d'une cyberattaque dans le décès d'une patiente a été reconnue en Allemagne. L'hôpital où elle était sur le point d'être opérée a été victime d'une attaque imposant son transfert en urgence dans un autre hôpital, ce qui lui a été fatal. Dès lors qu'une vie humaine est mise en péril, on entre dans une toute autre dimension.

Le second fait a été, pour la première fois là aussi, la revendication officielle, par le président Trump, d'une cyberattaque américaine à l'encontre d'un autre pays. Cette revendication montre que la cyberguerre est désormais une réalité, qui se déroule, certes, à l'intérieur des systèmes d'information, mais dont les effets, pour beaucoup encore inconnus, pourront mettre en péril la paix dans nos pays. Cette dimension politique, qui touche à notre humanité et nous fait changer de paradigme, nous amène à avoir une position très humble face à ce monde de la cybersécurité et soulève de multiples questions sur notre résilience.

Tout est piratable

Laurent OUDOT : Imaginons que l'ensemble de nos données, professionnelles ou privées, que nous entendons évidemment préserver, se trouve enclos dans un cercle virtuel. Ce cercle peut aussi bien représenter une personne, une société du CAC40 ou un pays. Qu'importe sa taille, l'objectif du pirate va être soit de s'y introduire pour manipuler les données, soit d'exfiltrer des données qui l'intéressent. Ces attaques vont alors provoquer soit des atteintes à la confidentialité des données, telle une violation du secret défense, soit des atteintes à leur intégrité, comme une modification des listes de médicaments prescrits aux patients d'un hôpital, ou encore des atteintes à leur disponibilité, des données indispensables devenant inaccessibles et provoquant, par exemple, des pannes de réseaux électriques sur un territoire ou l'arrêt des pacemakers d'une marque donnée.

Tous les systèmes peuvent être piratés, en particulier les smartphones et les tablettes. Notre smartphone communique en permanence avec Internet, soit en recevant des mails, des SMS, etc., soit en émettant des informations lors de nos recherches ou de l'envoi de messages. Il donne en permanence la position de son propriétaire. Il devient alors une cible privilégiée. Quant aux ordinateurs, dès lors que l'on en prend le contrôle, on accède à leur caméra et à leur microphone et l'on peut surveiller les personnes à leur insu tout en restant à distance. Les réseaux électriques, les satellites, les équipements militaires, les distributeurs bancaires, les navires, voire même les trains, etc., deviennent tous des cibles potentielles pour des pirates désireux de semer le chaos. L'informatique étant désormais dans toutes les maisons, il est également possible de cibler un système domotique et de prendre la main sur toutes les maisons qui en sont équipées, à travers

la prise de contrôle de leurs alarmes et de leurs ouvertures, où que ce soit dans le monde. Cela pose la question du choix entre des appareils bon marché, made in China, et des systèmes européens, certes plus onéreux, mais répondant à des normes de sécurité strictes. La 5G, les objets connectés et toutes les technologies à venir présenteront évidemment de nouvelles opportunités de piratage.

Pour trouver un vecteur initial, la première flèche qui pénétrera dans le cercle, le pirate va devoir identifier une vulnérabilité, c'est-à-dire, parmi toutes les fonctions d'un logiciel, celle qu'il pourra modifier à son avantage, par exemple en envoyant un mail contenant un lien sur lequel la cible va cliquer. Si quelqu'un trouvait une vulnérabilité inconnue, dite *0-day*[1], dans Windows, il pourrait dès lors bloquer l'usage de ce système d'exploitation sur toute la planète.

Des problèmes de perception de cette nouvelle réalité se posent aux cibles potentielles, quel que soit leur secteur d'activité, qui doivent redéfinir leurs priorités d'action. L'attaque sur site est la dernière mise en oeuvre par les attaquants, car elle est la plus onéreuse et la plus dangeureuse. Ils privilégieront toujours l'attaque à distance alors que les entreprises privilégient la sécurisation physique de leurs locaux, paradoxe qui nuit à leur sécurisation.

Si, par exemple, un pirate veut entrer dans une banque et qu'il ne trouve pas sur Internet des éléments de vulnérabilité le lui permettant, il va devoir s'en rapprocher physiquement, pour brancher dans ses locaux une clé USB ou pour capter un signal Bluetooth. Pour ce pirate, l'idéal est cependant de rester à distance, à quelques milliers de kilomètres de sa cible, en utilisant tous les "rebonds" et tous les systèmes d'anonymisation que permet Internet afin d'éviter que les services de sécurité ne puissent remonter sa piste et trouver sa véritable adresse IP.

Prenons l'exemple de l'usine d'un constructeur automobile qui a investi plusieurs milliards de dollars dans la fabrication de batteries pour ses véhicules électriques. Les cybercriminels ne réussissaient pas à trouver par où pénétrer dans l'entreprise, tant elle était lisse, sans faille dans sa protection. La mafia a chargé une personne, sous couverture évidemment, de recenser les rares entrées et sorties numériques, sans succès. Ne restait que les humains eux-mêmes qui, entrant et sortant en permanence, constituaient ainsi la seule vulnérabilité. Les pirates ont donc approché un salarié via WhatsApp et lui ont proposé 1 million de dollars pour brancher une simple clé USB à l'intérieur de l'une des usines les plus coûteuses du monde. Heureusement, le piratage des données sensibles a été stoppé à temps.

Si les premiers hackers, dans les années 1990, pénétraient des cibles comme la NASA ou le FBI, ils le faisaient essentiellement par défi, par jeu ou pour apprendre, la connaissance des systèmes et du fonctionnement des protocoles étant leur seul objectif. Désormais, c'est l'appât d'un gain rapide et conséquent qui est la principale motivation des pirates. Un jeune informaticien qui conçoit diverses armes, en assemblant ingénieusement des briques logicielles librement disponibles sur Internet, et les revend ensuite sur les réseaux à ceux qui s'en serviront, cybercriminels, terroristes ou simples malveillants, peut devenir très rapidement multimillionnaire. La seule limite est alors éthique. Entre le coût de l'arme, qui peut atteindre 2,5 millions de dollars, celui d'une équipe opérationnelle de hackers et les frais divers, vous pouvez "harponner" tous les CEO et gouvernants de la planète pour moins de 10 millions de dollars et vous garantir un retour sur investissement très profitable.

Pourquoi autant de piratages ?

La question de la sécurité soulève celle des biais cognitifs. Tout le monde se satisfait de disposer d'un antivirus – dont le principe remonte pourtant à des années –, d'un firewall et de mises à jour régulières, et se sent alors en sécurité. Or, cela revient, en 2020, à n'envisager de traverser l'Atlantique qu'en Zeppelin, *dominant design* des années 1920, en ignorant l'existence des avions modernes. Il a fallu des accidents dramatiques pour

1. Une vulnérabilité *0-day* est une vulnérabilité informatique n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu.