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

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

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.

que l'on prenne enfin conscience que la technologie était passée à autre chose. Nous sommes en train de vivre un changement analogue en matière de cybersécurité. Néanmoins, la pression du marketing a créé de telles habitudes dans les entreprises qu'il est difficile de faire admettre à leurs responsables que ces anciens outils ne suffisent plus face aux nouvelles menaces.

Un biais cognitif bien connu, l'effet Dunning-Kruger[2], sous-tend toutes ces résistances au changement. Si un directeur des systèmes d'information, compétent jusque-là, ne sait pas s'entourer de gens qui maîtrisent les évolutions du secteur, ses prises de décision ne seront pas basées sur des faits, mais sur la confiance qu'il accorde aveuglément à l'antivirus qu'il a l'habitude d'utiliser et aux messages marketing qu'il reçoit. Les aspects financiers en jeu sont par ailleurs considérables. La conséquence en est qu'en réalité, énormément de produits ne servent objectivement plus à rien. Ainsi, du fait de la multiplication des attaques et de l'inefficacité de ces systèmes de protection, devenue patente, la confiance accordée à ces derniers s'effrite et le changement de paradigme commence à s'imposer.

C'est pourquoi, depuis huit ans, face à cette recrudescence d'attaques non répertoriées, nous nous efforçons de concevoir des systèmes capables de détecter en temps réel celles qui ne sont désormais plus prévisibles, tâche qu'aucun antivirus ne peut accomplir.

Des enjeux éthiques primordiaux

Marie LE PARGNEUX : Tout cela se vit au sein d'une petite structure de 60 collaborateurs conscients d'œuvrer pour un objectif commun : assurer la cyberpaix dans le monde et la cyber-résilience des entreprises que nous accompagnons. Dans ce cadre, les enjeux humains sont primordiaux et nous imposent une pression constante. Ils sont désormais intrinsèquement liés à la cybersécurité dans un monde durement confronté à la recrudescence des attaques.

Du côté de nos clients, qui sont de grandes organisations, nous notons une intégration de ce nouveau paradigme et un réel bouleversement. Les décisions en matière de cybersécurité y sont désormais prises au niveau de la direction générale et de la direction des systèmes d'information (DSI) et non plus par le seul responsable de la sécurité informatique.

Une vraie prise de conscience a émergé quant aux risques encourus, non seulement financiers, mais aussi humains avec des risques vitaux aujourd'hui avérés. Il en va de même au sein des armées et des États. Aujourd'hui, la réponse en matière de sécurité doit évidemment être technologique, en étant beaucoup plus automatisée et en temps réel, mais aussi et simultanément organisationnelle et humaine, avec une sensibilisation constante des salariés. En effet, des études montrent qu'en matière de *phishing* et en dépit de toutes les précautions existantes, une proportion encore très importante de collaborateurs, particulièrement quand ils sont en télétravail, continuent à cliquer sur les liens proposés par des mails trompeurs – mails désormais plus sophistiqués et rédigés sans fautes d'orthographe.

Nous devons en permanence faire face à de nouvelles attaques de *malwares* (logiciels malveillants) inconnus. Au sein d'une entreprise comme TEHTRIS, la R&D doit donc être au cœur de notre stratégie et de nos préoccupations. En effet, nous devons constamment développer dans l'urgence des outils qui, grâce à l'intelligence artificielle, anticiperont les nouvelles attaques et feront face aux menaces inconnues en temps réel. À cette fin, nous sécurisons simultanément le réseau, le système, ses serveurs et ses postes de travail, ainsi que toute la partie cloud. Cet état de crise permanente, face à l'importance cruciale de certains enjeux, affecte en profondeur les aspects humains d'une entreprise comme la nôtre.

2. Biais cognitif selon lequel les personnes incompétentes ont un déficit dans leurs habiletés métacognitives qui les empêche de comprendre qu'elles n'ont pas la capacité nécessaire dans un domaine. Sans s'en rendre compte, elles ont un excès de confiance qui les pousse à se surestimer.

Enfin, la dimension éthique, totalement intégrée dans la culture de TEHTRIS, nous confronte à l'obligation morale, adossée à un référentiel de valeurs, de prendre en compte la finalité et les conséquences de nos actions. Cela peut bien entendu être source de tensions. En effet, nos collaborateurs, jeunes pour la plupart, peuvent parfois être confrontés à des dilemmes délicats, face à un monde d'une complexité extrême, à une temporalité qui sans cesse les projette en avant. Ils ont choisi de valoriser leurs compétences dans le cadre d'une entreprise ayant une finalité éthique ; ils pourraient le faire dans des environnements moins soucieux d'un bien commun, avec des gains plus rapides.

Notre approche globale s'inscrit non seulement dans une RSE classique, mais aussi dans notre façon de coder, tous nos développements se faisant, par exemple, de telle sorte qu'il ne nous est pas possible d'accéder aux informations critiques et confidentielles des entreprises que nous protégeons. Cela nous impose plus de temps de développement et implique des coûts plus élevés pour nos clients, mais nous considérons que c'est un investissement au service de ce que nous pensons être indispensable dans une démarche de cybersécurité éthique.

Débat

Des systèmes d'exploitation vulnérables

Un intervenant : *La plupart des problèmes actuels viennent du protocole TCP/IP*[3] *qui est derrière Internet et qui ne prend pas en compte les questions de sécurité. Le projet RINA (*Reference Implementation for a National Applications*) est un service mis en ligne par l'Europe, qui souhaite développer son autonomie numérique, pour l'échange confidentiel des dossiers de sécurité sociale entre les institutions compétentes des pays européens. Qu'en pensez-vous ?*

Laurent Oudot : Je ne suis pas spécialiste des aspects techniques du projet RINA et n'ai pas d'information sur sa robustesse, mais il est vrai que le TCP/IP, parmi d'autres protocoles, pose problème, car au fil des années, les chercheurs, du fait de l'intrication des mondes universitaires et militaires, ont empilé des protocoles nouveaux par-dessus des éléments anciens qui ne prenaient pas en compte ces impératifs. Néanmoins, si le réseau est l'un des problèmes, ce n'est pas le principal et beaucoup de systèmes industriels en rencontrent d'autres.

Aujourd'hui, les pirates se focalisent davantage sur les failles des systèmes d'exploitation que sur les réseaux. Grâce aux éléments fournis par Edward Snowden, on sait désormais que les Américains ont complétement tiré parti, depuis des années, des vulnérabilités d'Internet et du protocole TCP/IP pour réaliser des armes informatiques d'un niveau supérieur, comparables, du point de vue de la cybersécurité, aux armes nucléaires.

Par ailleurs, la notion d'autonomie soulève des questions sur l'antagonisme entre le marketing et la science. Il va nous falloir trancher entre l'attirance pour les produits marquetés que la Silicon Valley nous propose et le choix de solutions scientifiques claires et robustes, quoique bien moins séduisantes. Le projet RINA a le grand mérite de montrer aux jeunes générations qu'il faut remettre en question les fondamentaux en se demandant s'il n'est pas possible de faire mieux.

3. *Transmission Control Protocol/Internet Protocol* – protocole représentant l'ensemble des règles de communication sur Internet. Il se base sur la notion d'adressage IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir lui acheminer des paquets de données.

Marie Le Pargneux. : Cette question de la souveraineté semble, depuis peu, de plus en plus présente dans les préoccupations des directions générales et nous avons bon espoir que cette prise de conscience se diffuse à l'avenir.

Int. : *Pour parer une attaque, doit-on seulement être en mesure de la reproduire ou doit-on l'anticiper ? Dans ce cas, comment détecter une menace que l'on ne connaît pas ?*

L. O. : Dès lors que l'on n'est plus en phase de *0-day* et que l'on sait qu'une menace plane sur Internet, l'un des premiers objectifs des *white hats*[4] est de trouver des signatures en analysant et en interprétant le phénomène. Il est alors très intéressant d'avoir un laboratoire dans lequel on puisse reproduire des agressions afin de trouver, parmi les stimuli et les réponses, des éléments discriminants permettant de caractériser de manière certaine une attaque donnée. Dès que vous avez cette signature, il vous est possible d'anticiper les effets de cette attaque sur les cibles visées.

Il y a vingt ans, nous n'étions confrontés qu'à 5 ou 6 outils malveillants par mois, que pouvaient traiter une dizaine d'experts mondiaux. Depuis que nous en avons 300 000 par jour, l'industrialisation des solutions classiques à une telle échelle est devenue trop complexe. Il est désormais nécessaire de déployer une assistance aux capacités humaines grâce à une intelligence artificielle (IA) capable d'observer ces phénomènes avec une approche autre afin de trouver des éléments qui, sinon, seraient indétectables. Sur cette question, l'IA constitue un apport décisif, relevant d'une post-industrialisation, qui permet à des ingénieurs de haut niveau de mieux comprendre les attaques et donc de les contrer.

L'effondrement des géants américains

Int. : *Que font les grands noms de la lutte antivirus face à cette évolution des menaces ?*

M. L. P. : Ces sociétés sont, tout comme nous, lancées dans une course de vitesse. Beaucoup d'attaques récentes se sont produites contre des entreprises pourtant protégées par des antivirus et ont abouti à des destructions de parcs informatiques. Comme les antivirus ne fonctionnent que sur la base de signatures déjà répertoriées dans les bibliothèques de ces sociétés, dès lors que l'on sort de ce cadre, ils deviennent inopérants. Un antivirus reste donc toujours nécessaire pour contrer les menaces identifiées, mais est insuffisant face à celles qui émergent quotidiennement. Ces sociétés ne sont donc pas condamnées et cherchent à se transformer et à monter des EDR[5] pouvant neutraliser en temps réel les menaces – connues ou inconnues –, l'usage d'une IA permettant une contre-attaque en quelques secondes. Dans deux ou trois ans, antivirus classiques et EDR ne formeront vraisemblablement plus qu'un seul et même produit.

Les dirigeants d'entreprise peuvent parfois questionner l'IA. Nous évoquons avec eux ce qu'est le *deep learning*, mais plus l'on va vers ses couches profondes, moins il y a d'"explicabilité". Leur crainte est qu'en laissant la main à la machine, on en perde le contrôle. C'est pourtant ce qui a sauvé nos clients dans d'autres entreprises.

Int. : *Comment faites-vous pour être plus efficaces que les anciens éditeurs d'antivirus et pour compenser les faiblesses des* operating systems *?*

L. O. : Afin de nous assurer que nos éléments soient les plus performants possible, nous restons dans le cadre d'une démarche scientifique. De plus, nous venons du monde de l'offensif et quelque chose dans notre ADN en reste marqué. Dans ce cadre, il m'est arrivé de collaborer avec divers grands pays pour contrer des menaces de très haut niveau, pouvant faire perdre des milliards de dollars à de grandes entités ou déstabiliser des régimes politiques. Notre spécialité était alors l'attaque et la caractérisation des menaces à l'échelle internationale.

Venant de ce monde de l'offensif, la stratégie de TEHTRIS est de chercher à nous approcher au plus près de cette frontière entre l'attaquant et le système d'exploitation, au lieu de nous limiter à produire des logiciels. Nous assistons aujourd'hui à un effondrement financier de nombreux géants américains, tel Symantec/Norton,

4. Les *white hats* sont les défenseurs face à une menace, par opposition aux *black hats* qui sont les attaquants.

5. Les plateformes d'EDR (*Endpoint détection and response*) sont des solutions qui surveillent les terminaux (les ordinateurs connectés au réseau et non le réseau lui-même) afin d'y détecter des activités suspectes.

démantelé et racheté comme quantité d'autres sociétés de la cybersécurité. Ils étaient pourtant passés de l'antivirus classique à l'antivirus *next generation*, mais cela n'a pas suffi à contrecarrer une perte de confiance généralisée envers leurs produits. Pour autant, le couplage avec les EDR ne suffira pas et il faudra descendre encore plus bas dans les couches logicielles, car, quels que soient les outils, il est nécessaire de modifier certains mécanismes des systèmes d'exploitation. C'est ce que nos systèmes vont effectivement faire, mais cela prend du temps, car nous avons d'abord dû être acceptés dans le *Microsoft Virus Initiative*, club fermé qui nous donne le droit d'utiliser un *driver*. Grâce à ce petit élément de très bas niveau dans le noyau du système d'exploitation, nous pouvons modifier le comportement de Windows afin de lui permettre de mieux se défendre.

Int. : *Quel est votre intérêt à former vos clients plutôt qu'à les laisser dans l'incompréhension quant à votre travail ?*

M. L. P. : Au début de cette année, nous avons pris un virage stratégique important. TEHTRIS était jusque-là un fournisseur de services et de technologies. Nous accompagnions alors nos clients sur de la cybersurveillance, de la gouvernance ou de la mise en place de conformité, toutes ces dimensions étant abordées sous l'angle de la sensibilisation ou de la formation. Depuis, nous avons décidé de nous recentrer sur notre cœur de métier, la technologie, là où nous avons la plus forte plus-value, et de nous désengager des actions de formation. Nous avons délégué à des partenaires l'ensemble de ces services adossés à nos technologies.

Les crises dans la crise

Int. : *On a l'impression que TEHTRIS est une cellule de crise permanente, sans pause pour faire baisser la tension. Les traders en Bourse sont dans une configuration analogue et l'on sait que ce sont des gens invivables ! Comment fait-on alors pour gérer le stress ?*

M. L. P. : Chez TEHTRIS, il y a crise et crise. Il y a la crise permanente qui est celle de l'innovation face aux cyberattaques constantes. La question est alors de savoir comment, à notre petite échelle, nous pouvons être contributeurs dans un tel monde. Ainsi, dès le début de la pandémie de la Covid-19, nous avons développé un partenariat avec OVH (entreprise française spécialisée dans l'hébergement de données et les services du *cloud computing*) afin de proposer à l'ensemble des établissements de santé à travers le monde de les protéger gratuitement pendant toute la durée de cette crise. Ils ont effectivement subi énormément d'attaques durant cette période et cela continue. Nous sommes donc en permanence dans une tension dont la finalité ultime serait la cyberpaix dans le monde.

Il y a ensuite les crises dans la crise, par exemple quand on nous appelle à l'aide un vendredi soir, moment préféré des assaillants pour attaquer. Nous lançons alors une mobilisation générale des équipes et de nos partenaires qui vont travailler sans relâche pendant tout le week-end pour essayer de contenir l'assaut et de protéger ce qui, dans le système d'information concerné, n'a pas été touché.

Notre politique RH veille rigoureusement à respecter le cadre réglementaire en matière de repos et de cadre de vie, car il nous faut permettre la déconnexion de nos collaborateurs. Ce n'est pas toujours simple pour l'organisation, car ce sont des personnes passionnées, extrêmement investies dans leur travail, qu'il faut cependant parfois savoir freiner contre leur gré. Pour la plupart, ce sont de jeunes ingénieurs très spécialisés, dotés d'une grande endurance physique et d'une forte résistance au stress, qui ont une capacité de concentration extrême. Le management de ces profils singuliers est donc très spécifique, assez peu affectif bien que nous soyons une petite structure et très orienté vers l'objectif commun tout en gardant un grand respect envers ces fortes individualités.

Int. : *Est-ce obligatoirement un métier de jeune ?*

L. O. : Chez nous, la moyenne d'âge est de 28 ans, comme dans beaucoup d'autres sociétés du numérique. Pour autant, nous ne ressemblons pas à des traders classiques, mais plutôt à des traders haute fréquence, c'est-à-dire à ceux qui fabriquent des algorithmes non pour réaliser des coups, mais pour créer des robots qui, eux, vont réaliser ces coups ! Nous sommes passés dans une autre dimension, celle de l'hyperautomatisation. En contrepartie de cet état de crise permanente, il existe des risques de perte d'attention, auxquels d'autres secteurs d'activité comme l'aviation sont également confrontés et que nous devons apprendre à gérer.

À qui appartiendront les données ?

Int. : *Qu'attendez-vous de l'État concernant les données et quelle est son organisation dans ce domaine ?*

M. L. P. : Aujourd'hui, nos principaux et seuls vrais concurrents sont américains et israéliens, ce qui pose énormément de problèmes de protection des données. En effet, quand une entreprise confie ses données à un Américain, il existe un risque réel qu'elles servent aussi, malgré tous les systèmes de sécurisation, à de l'intelligence économique. Ce que nous attendons de l'État, c'est donc d'agir davantage à une échelle européenne, car nous avons besoin de cohésion pour faire face à ces risques. Je ne parlerai pas des Chinois ; en raison de règlements tels que le RGPD, ils ne sont pas encore en mesure de faire chez nous une réelle percée en matière de business.

Ces dernières années, l'organisation de l'État s'est profondément transformée en faisant évoluer l'Agence pour la sécurité des systèmes d'information (ANSSI), qui contribue efficacement à l'objectif de sensibilisation de toutes les organisations aux questions de cybersécurité, notamment en étant présente sur tout le territoire. C'est particulièrement important pour les PME et les TPE qui, certes, ont toutes un antivirus, mais qui sont peu sensibilisées à la prévention.

L. O. : Dans le plan de relance, le gouvernement a inclus un volet numérique, la cybersécurité étant un enjeu national. L'État français soutient donc des investisseurs privés, qui sont parfois investis dans des domaines proches de ses prérogatives régaliennes. La France, comme beaucoup de pays européens, dispose d'énormément d'ingénieurs de grand talent capables d'inventer des algorithmes, de développer des programmes innovants et de concevoir des théories, mais il semble qu'elle ait moins de capacités à transformer tout cela en succès commerciaux. Une juste dose de régulation peut donc nous aider, mais TEHTRIS cherche avant tout à être au service de l'État. Personnellement, je me méfie de l'excès de centralisation. Nous espérons donc pouvoir rassembler autour de nous, à l'échelle européenne, toutes les forces vives soucieuses de travailler en réseau, afin de créer sur notre continent un espace dans lequel les données ne seront pas uniquement hébergées dans des cloud américains où elles pourront être utilisées en permanence et sans contrôle de notre part.

Int. : *Microsoft ne pourrait-il pas être attaqué en justice pour vice caché puisque, si des gens trouvent des parades, c'est en raison de la défaillance de ses produits ?*

L. O. : Certains, aux États-Unis, y réfléchissent, sans doute pour des raisons monétaires ou politiques, mais aussi pour dénoncer l'hégémonie mondiale des GAFA sur les briques technologiques constitutives de leurs produits. Le contrôle de Microsoft sur ces briques est en effet quasi monopolistique. Je souhaite bon courage à ceux qui se hasarderont dans un tel combat juridique ! Par exemple, un leader mondial de la cybersécurité est engagé dans un procès après s'être rendu compte que, du fait des accords qu'il avait été obligé de passer avec Microsoft pour avoir le droit de produire un antivirus, il lui avait fourni de quoi sortir son propre antivirus concurrent.

Int. : *L'ANSSI a développé un "Linux durci", dénommé CLIP. N'est-ce pas là une voie nationale qui mériterait d'être approfondie alors que le ministère des Armées, à la différence de la gendarmerie nationale, vient de signer avec Microsoft ?*

L. O. : Je crois beaucoup aux systèmes multiniveaux que vous évoquez. C'est pour cette raison que, chez TEHTRIS, la plateforme de cyberdéfense que nous avons créée n'utilise aucun des systèmes proposés sur le marché. Pour cela, nous avons modifié le noyau de Linux afin de faire en sorte que tous les processus soient cloisonnés. J'ai évidemment soutenu CLIP dès ses débuts en tant que représentant du ministère des Finances au sein des sous-commissions du prédécesseur de l'ANSSI.

Int. : *Peut-on sécuriser le cloud ?*

L. O. : L'accélération du mouvement vers le cloud complique considérablement les choses. Y avoir recours suppose un degré de confiance élevé dans la sécurité qu'il offre. Je m'inquiète alors de voir de grandes organisations qui partent dans le cloud pour des raisons souvent plus financières que scientifiques et stratégiques. Nous utilisons, quant à nous, du cloud souverain européen, avec OVH en qui nous avons confiance, mais nous avons

des clients du CAC40 qui mettent toutes leurs données dans des cloud non maîtrisés, dont les serveurs sont désormais localisés au-delà de nos frontières. La sécurisation d'un tel espace sans frontières est un vrai défi.

Int. : *Le problème de la sécurisation ne se pose-t-il pas également avec le développement de la 5G et de l'internet des objets ?*

L. O. : Vous avez parfaitement raison. Les dangers, bien plus que ceux liés aux ondes, sont ceux liés à la sécurité et à la gouvernance des objets connectés. À qui appartiendront les données ? dans quel pays seront-elles stockées ? quelles règles juridiques s'imposeront ? C'est en cela que la sensibilisation de tous sera essentielle.

Int. : *Une attaque qui réussit peut se traduire par un chantage. Que préconisez-vous à ceux de vos clients qui en sont victimes ?*

L. O. : Je suis un ancien opérationnel du ministère de la Défense et, comme pour les prises d'otages, je préconise de ne jamais accepter un chantage. Dès lors que vous cédez, vous êtes étiqueté par les criminels comme étant une poule aux œufs d'or qui, ayant dit oui une fois, le dira une deuxième fois, etc. Il m'est facile de parler ainsi, mais, pour les entreprises qui ne paient pas, le coût est énorme.

M. L. P. : Les entreprises que nous accompagnons à la suite d'un incident perdent parfois des millions d'euros par jour et voient tous leurs systèmes de production soudainement détruits.

L. O. : De par le monde, il y a beaucoup d'entreprises et de services étatiques qui paient des millions d'euros de rançon. Les mafieux gagnent ces sommes de deux façons. D'une part, il y a les gens qui paient dans l'espoir – que rien ne garantit – de récupérer leurs données et de ne plus être victimes à l'avenir. D'autre part, si l'attaque touche, par exemple, un hôpital qui risque de perdre toutes ses données sensibles, choisir de ne pas payer est impossible, car les soignants ont un besoin vital des dossiers médicaux pour sauver leurs patients. Aux États-Unis, énormément de villes ont ainsi payé des sommes énormes, sans les rendre publiques, et des banques asiatiques ont fait de même.

Les équipes mafieuses sont essentiellement basées dans les environs de Moscou et les identités de leurs membres sont parfaitement connues. Quand on regarde la structuration organisationnelle du plus grand groupe criminel, on constate qu'à côté de son "CEO", il a un *Chief Financial Officer* ! L'année dernière, ce groupe a officiellement annoncé 15 milliards de dollars de chiffre d'affaires. Les groupes de pirates sont donc milliardaires, partent en vacances dans des palaces et roulent en voitures de luxe ! Ils sont bien connus et suivis par Interpol qui fait un travail phénoménal en liaison avec les différents services de police dans le monde. En France, à côté de l'ANSSI, le ministère de l'Intérieur fait également un très gros travail de protection des PME, des TPE et des personnes. Dans le cas russe, il est très clair que les criminels bénéficient d'une protection de haut niveau et des considérations diplomatiques vont alors interférer avec les mesures envisagées à leur encontre.

Int. : *Le monde de l'assurance, qui cherche désespérément de nouveaux relais de croissance, se réjouit à l'idée que la cybersécurité devienne un marché mirobolant. Qu'en pensez-vous ?*

M. L. P. : Nous sommes évidemment en contact avec le monde de l'assurance. Les montants des indemnisations servies aux entreprises attaquées sont parfois colossaux et la question que les assureurs posent est alors de savoir ce qui pouvait être protégé et éventuellement ne l'a pas été, et ce qui ne pouvait pas l'être. Cela va imposer aux organisations de mettre en place des systèmes de sécurisation de leur système d'information beaucoup plus performants. Il ne s'agit encore essentiellement que de réaction, pas encore d'anticipation du risque, malgré une timide et récente évolution en ce sens sous la pression des assureurs. La sécurisation du mouvement croissant vers le cloud est également un enjeu colossal.

Les assureurs disent qu'ils rembourseront en cas de problème. C'est là un problème de transfert du risque, total ou partiel, et qui requiert la lecture attentive de toutes les clauses des contrats. Très clairement, la question est de savoir si l'on préfère être réactif, et subir le risque en faisant confiance à l'assurance, ou proactif, en anticipant les menaces et en se protégeant. C'est un choix de société.

Int. : *Existe-t-il une organisation interprofessionnelle qui se préoccupe d'un sujet aussi grave et complexe ?*

L. O. : TEHTRIS fait partie d'une organisation mondiale, AMTSO, qui regroupe des sociétés, toutes ennemies commercialement, mais qui échangent régulièrement entre elles des informations techniques sur les groupes criminels afin de pouvoir les contrer le plus efficacement possible. L'enjeu nous dépasse tous. Le but est de ne pas se faire la guerre, ces groupes en seraient les premiers bénéficiaires. Tout ne se passe pas toujours idéalement dans cette organisation, car les poids lourds du marché sont parfois très réticents à l'émergence de solutions disruptives qui bousculent leur confort.

Il existe également des équipes spécialisées dans la gestion des incidents qui se partagent beaucoup d'informations, le plus important étant de réaliser ce que nous appelons *l'attrition des moyens de l'attaquant*. Ainsi, si un pirate attaque l'un de nos clients, on analyse ses moyens, ses méthodologies et ses informations, que nous communiquons à notre client, afin qu'il les transmette aux autorités de son pays, puis à la communauté professionnelle. Si nous le faisons, c'est afin que tous, nous ayons la signature de cette attaque et qu'elle puisse être utilisée ailleurs contre des attaques similaires. Nous aidons certes nos concurrents, mais l'avantage que nous en tirons est de casser les systèmes offensifs des mafias, confrontées non plus à une seule, mais à de multiples contre-offensives concertées.

Int. : *On a tous à faire des arbitrages entre la vulnérabilité et la fonctionnalité des logiciels. Cédric O, notre secrétaire d'État au Numérique, l'a parfaitement assumé en disant qu'il préférait que l'application StopCovid soit un fiasco plutôt que de voir les Français partager des données personnelles de santé avec Google ou Apple. Quelle est votre opinion sur ce point ?*

L. O. : L'attitude de l'État me semble digne dans la mesure où l'essentiel en la matière est de ne pas prendre de risques. Privilégier la vie privée des citoyens me paraît essentiel et tout-à-fait aligné avec les valeurs de l'Europe. Cela relève simplement du principe de précaution inscrit dans notre Constitution.

Int. : *Au sein des services de renseignement, James Bond est-il mort au bénéfice des "super- pros" du digital ?*

L. O. : Sur ce point, il est intéressant de considérer quel type d'espion a été arrêté ces dernières années, notamment sur le sol européen. Le must de l'espionnage de nos jours, ce sont des équipes opérationnelles organisées, disposant d'un ensemble de compétences variées en fonction d'un objectif donné et qui ont évidemment une dimension cyberdéfense. La France affiche désormais qu'elle s'est organisée en considérant le cyberespace comme un terrain d'affrontement[6]. Elle a largement innové en la matière et fait partie des grands pays qui ont compris que, de la même manière qu'il y a eu une politique de dissuasion nucléaire à une époque, il y a à présent une stratégie de dissuasion en matière de cyberdéfense. Alors, si le James Bond d'aujourd'hui, outre ses capacités physiques lui permettant de survivre en milieu contraint, ses huit langues parlées couramment, son énorme QI et son ignorance de la peur, possède en plus les compétences d'un pirate informatique d'envergure internationale, nul doute que ce sera quelqu'un de redoutable ! Et il doit bien en exister quelques-uns sur la planète !

6. Un commandement de la cyberdéfense, sous l'autorité du chef d'état-major des armées, a été créé en 2017.

Présentation des orateurs

Marie Le Pargneux : diplômée de l'Executive Master de l'École polytechnique, docteur en sciences de gestion, elle a travaillé pendant plus de dix ans avec des dirigeants sur les problématiques de transformations de *business model*, organisationnelle, managériale et technologique. Elle enseigne le comportement organisationnel à l'ESSEC Business School depuis 2009. Elle a intégré TEHTRIS début 2020 en tant que *Chief Development Officer* (CDO).

Laurent Oudot : expert senior international en cybersécurité, il est co-fondateur et directeur technique de la société TEHTRIS. Il a étudié à l'École polytechnique dans le cadre de l'Executive Master. Pendant plus de vingt ans, ses compétences techniques ont été mises à profit au sein d'environnements très sensibles comme le pôle Défense du Commissariat à l'énergie atomique, le ministère de la Défense, l'ONU, etc. Il a participé à de nombreuses commissions, formations et expertises nationales, au sein d'organismes comme l'ANSSI ou pour le Premier ministre.

Diffusion décembre 2020