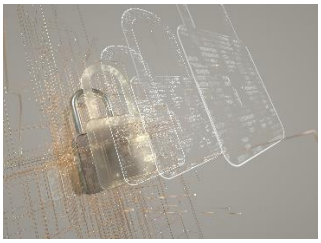
Cybercriminalité et cybersécurité

COLLOQUE 3 AVRIL 2023

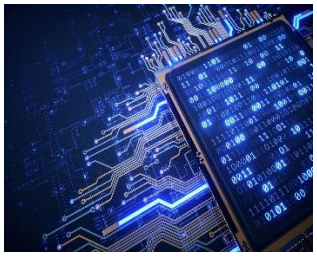
CNECJ
Section autonome de Lyon-Chambéry-Grenoble

Les intervenants

Monsieur Romain DUCROCQ
Substitut général près la Cour d'appel de Lyon



Monsieur Thierry REGOND
Vice-président du Tribunal de commerce de Lyon



Monsieur Thibaud MÉRIEN
Lieutenant de la Gendarmerie nationale
Spécialiste en cybercriminalité

Madame Marianne DELARUE
Déléguée adjointe à la sécurité numérique pour la région Auvergne–Rhône-Alpes
Agence nationale de la sécurité des systèmes d'information (ANSSI)

Maître Olivier MOUSSA
Avocat au Barreau de Lyon
Cabinet SHIFT avocats

Monsieur Philippe LAMBERT
Expert informatique inscrit près la Cour d'appel de Dijon
Spécialiste en cybercriminalité

Introduction au colloque

Pierre BONNET
Président de la section autonome
de Lyon-Chambéry-Grenoble de la CNECJ

La section de Lyon-Chambéry-Grenoble vous souhaite à toutes et à tous la bienvenue à ce colloque, évènement qui ne s'était pas tenu depuis trois ans en raison des temps difficiles que nous avons traversés.

C'est donc avec un grand plaisir que la section vous propose cette année ce colloque concernant **la cybercriminalité et la cybersécurité**, thème d'actualité dans la mesure où il ne s'écoule pas une journée sans que la presse ne se fasse l'écho d'une cyberattaque ciblant une entreprise, une structure ou encore une organisation publique ou privée.

Ainsi et la semaine dernière encore, le site Internet du Parlement français a été bloqué durant toute une journée suite à une attaque par « *déni de services* » par le collectif de hackers pro-russes NoName057.

Le 1er mars, c'était la mairie de Lille qui était visée.

Début janvier 2023, le journal *La Tribune* titrait l'un de ses articles « ***Hôpitaux : la France traverse une véritable tempête cyber*** ». C'est ainsi qu'à Lyon les hôpitaux privés de l'est lyonnais et Jean Mermoz ont été attaqués.

Selon la Commission européenne, une attaque par rançongiciel survient toutes les 11 secondes.

Ainsi et au titre de 2021, le coût de ces attaques à travers le monde a été évalué à 20 milliards d'euros, les revenus de la cybercriminalité représentant un business qui se chiffrerait à 1 500 milliards de dollars selon le Général Christophe Husson, commandant en second de la gendarmerie dans le Cyberespace.

En 2021, Madame Ursula von der Leyen, Présidente de la Commission de l'Union européenne, a affirmé concernant l'état de l'UE que « ***si tout est connecté, tout peut être piraté*** ».

Concernant ce point, la presse relate régulièrement des cyberattaques menées par des États afin d'en déstabiliser d'autres. Ainsi et en 2022, ce sont le Costa-Rica et l'Albanie qui ont été visés. En 2020, il s'agissait de l'Australie et des États-Unis où il est estimé que 18 000 grandes entreprises ou institutions telles que les départements du trésor, du commerce, de l'intérieur, de la santé et de l'énergie ont été attaqués.

Ce ne sont là que quelques exemples.

Devant toutes ces attaques visant États et grandes structures publiques, on pourrait croire que la cybercriminalité ne vise que les grandes organisations. Or cela est loin d'être le cas.

Ainsi, l'ANSSI (Agence Nationale de la Sécurité des Système d'Information) indiquait récemment et concernant l'année 2022 que « ***la menace cybercriminelle et plus spécifiquement celle liée aux rançongiciels se maintient avec un regain d'activité en 2022,*** **[touchant]** ***particulièrement les TPE, PME et ETI*** », soit 40 % des rançongiciels traités ou rapportés à l'ANSSI, les collectivités territoriales représentant quant à elles 23 % et les établissements publics de santé 10 %.

Fin octobre 2022 et à l'occasion du 3ème Forum Sécurité et Résilience, Hugues Foulon, PDG d'Orange Cyberdéfense, estimait que 60 % des entreprises victimes de cyberattaques déposaient le bilan dans les 6 mois.

En outre et en préparant ce colloque, j'ai découvert des données absolument effarantes. Ainsi et par exemple :

- en cas d'attaque, une entreprise met en moyenne 6 mois à détecter une violation de ses données ;
- 43 % des cyberattaques visent les petites entreprises ;

- 91 % des attaques sont lancées par un courriel de phishing (ou hameçonnage).

Étant le 2ème pays d'Europe le plus touché par les rançongiciels, la France a également été l'une des principales cibles mondiales.

Il ressort ainsi que le gain financier, l'espionnage et la déstabilisation restent les principaux objectifs des attaquants.

Devant de telles données, il apparaît donc que la cybersécurité nous concerne tous au quotidien et qu'il n'est plus possible d'estimer que cela n'arrive qu'aux autres.

Dans ces conditions, nos intervenants au colloque de ce jour vous présenteront :

- l'évaluation de cette menace,
- les règles élémentaires de la prévention,
- les conséquences financières de ces cyberattaques pour les entreprises françaises,
- les investigations menées par les services spécialisés,
- et enfin, les dispositifs judiciaires mis en place pour répondre à ces attaques.

Je cède à présent la parole à nos intervenants que je souhaite remercier chaleureusement :

- **Monsieur Romain DUCROCQ**, Substitut général près la Cour d'appel de Lyon ;
- **Monsieur Thierry REGOND**, Vice-président du Tribunal de commerce de Lyon ;
- **Monsieur Thibaud MÉRIEN**, Lieutenant de la Gendarmerie nationale, spécialiste en cybercriminalité ;
- **Madame Marianne DELARUE**, Déléguée adjointe à la sécurité numérique pour la région Auvergne–Rhône-Alpes – Agence nationale de la sécurité des systèmes d'information (ANSSI) ;
- **Maître Olivier MOUSSA**, avocat au Barreau de Lyon, associé du cabinet SHIFT ;
- et enfin **Monsieur Philippe LAMBERT**, expert informatique inscrit près la Cour d'appel de Dijon, grand spécialiste de la cybercriminalité qui sera l'animateur et le modérateur de ce colloque.

Sans plus attendre, je cède la parole à Philippe Lambert.

Un univers connecté

Merci Pierre.

Bonjour à toutes et à tous. Merci d'être présents.

Je commencerai cette approche de la cybersécurité en présentant l'émergence des réseaux et en parallèle celle des attaques informatiques.

Si l'on prend autant en compte la cybersécurité aujourd'hui, cela résulte du fait que nous évoluons dans un univers où l'informatique est dominante. Les notions d'informations automatiques et de données sont omniprésentes dans notre vie, dans notre société. On voit cela avec le réseau Internet, en interconnexion des systèmes d'information. Qu'est-ce qui a mené à tout cela ? C'est la raison informatique, fruit de la volonté humaine de s'unir en réseau.

Avant 2010 et dans le laps de temps qu'il a fallu à Internet pour commencer à émerger, à fleurir, il existait déjà des attaques informatiques. Quand j'étais plus jeune, on appelait cela des BBS[1], c'est-à-dire des systèmes montés sur des Minitels, comme le 36 15 RTEL, qui permettaient aux pirates de toute la France de se connecter et d'échanger : comment

[1] *Bulletin Board System*

pirater un téléphone sur la place publique, comment faire du *phreaking*[2]… ? Il existait donc déjà beaucoup de choses visant à récupérer des données.

Aujourd'hui, cela a énormément évolué. Nous ne sommes plus à l'époque de Kevin Mitnick[3] et autres pirates isolés. Ce sont des groupes sociaux, des personnes avisées, qui utilisent de nouvelles méthodes.

J'invite Madame Delarue à nous parler de cela.

[2] Le phreaking (contraction de « phone » et « freak ») ou piratage téléphonique est un terme décrivant l'activité de personnes étudiant, testant ou exploitant de manière frauduleuse les systèmes téléphoniques

[3] né le 6 août 1963 à Van Nuys en Californie, Kevin Mitnick, surnommé « Le Condor », est un ancien pirate informatique américain devenu depuis les années 2000 consultant en sécurité informatique

1 ANSSI : vue d'ensemble de la cybermenace

Merci. Bonjour à tous.

Je suis déléguée à la sécurité numérique pour la Région Auvergne – Rhône-Alpes pour l'ANSSI.

Aujourd'hui, je vais vous présenter les missions de l'ANSSI. Quel est l'état de la cybermenace ? Qui est principalement visé ? Sans suspense : tout le monde. Ensuite, je vous proposerai quelques recommandations de bonnes pratiques avant de céder la parole à mes collègues.

1.1/ Les missions de l'ANSSI

Tout d'abord, l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) est rattachée au Secrétariat général de la défense et de la sécurité nationale, qui est le bras droit de la Première ministre pour toutes les questions de défense et de sécurité nationale.

Deux missions principales :

- d'une part, l'autorité de sécurité et la prévention ;
- d'autre part, l'autorité de défense.

Dans tous les cas, il s'agit de réduire les impacts d'une attaque cyber.

Pour la partie sécurité et prévention, l'ANSSI met en œuvre, par exemple, des réglementations de SSI[4] pour des secteurs considérés comme ayant une importance vitale pour la France (l'eau, le nucléaire…).

Cela concerne également des labellisations de produits et services. Nous travaillons avec des prestataires et fournisseurs dont le service ou le produit est considéré comme de qualité et pouvant disposer à ce titre de ce label de sécurité. Plus précisément, nous abordons les missions de conseil et d'assistance aux collectivités, aux entreprises, notamment au travers de guides publiés sur le site de l'ANSSI.

Pour la partie défense, l'ANSSI a des missions de supervision et de détection de l'attaque. Elle comprend notamment le CERT-FR[5], centre opérationnel de l'ANSSI, qui peut être contacté 24 h/24 et 7 j/7 pour mener des investigations en cas d'attaque.

Je précise que l'ANSSI ne collecte pas de renseignements, ne réalise pas d'actions offensives et n'est pas le bon interlocuteur pour le dépôt de plainte.

1.2/ L'état de la cybermenace

Est caractérisée comme menace une action composée d'attaquants qui réalisent des objectifs, qui ont une cible et qui pour cela cherchent un chemin d'attaque.

Tout d'abord, quels types de menaces ?

Je vous parlais tout à l'heure de la menace étatique. Cela a déjà été abordé en introduction, mais des États et des gouvernements peuvent mener des attaques contre

[4] Sécurité des Systèmes d'Information
[5] Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques

des gouvernements à des fins d'espionnage ou d'intelligence économique pour des gouvernements et des entreprises stratégiques. Ce type d'espionnage est caractérisé par la durée, l'attaquant essayant de rester le plus longtemps possible en « sous-marin » sur le système d'information ciblé.

On ne va pas forcément s'en rendre compte très vite, contrairement au crime organisé où le but visé est la rentabilité avec une attaque facile à moindre coût. Dans ce contexte, les attaquants vont essayer de scanner les vulnérabilités sur le réseau et de s'introduire par la faille la plus évidente, raison pour laquelle ils ne ciblent pas forcément des entités en particulier. Ils vont là où c'est le plus simple.

À titre d'exemple, on a énormément parlé des rançongiciels. Il s'agit d'un attaquant qui profite d'une vulnérabilité d'un système ou d'un manque de vigilance humaine. Une fois sur le système, il va tenter d'atteindre le plus de privilèges sur le système d'information, comme l'administration du système. Une fois cette tâche accomplie, il va se latéraliser sur tout le système et va aller chercher les données qui l'intéressent et chiffrer tout ou partie des données. Puis il va déposer une note de rançon. Moyennant paiement, il pourra rendre les données. Dans les faits, il apparaît que l'attaquant ne rend pas forcément les données et qu'il ne les rend pas dans leur intégrité. L'ANSSI recommande donc vivement de ne pas payer la rançon. Dans ce contexte et dans la mesure où ces rançongiciels peuvent vraiment avoir des impacts très importants pour le fonctionnement d'une entreprise, il est donc nécessaire de se montrer très vigilant.

Plus anecdotiques, mais on reste aussi vigilant sur ce point : le terrorisme et l'activisme idéologiques. À des fins politiques, les attaquants vont plutôt chercher à saboter le fonctionnement de l'entreprise, notamment dans les secteurs de la banque et du pétrole. Dans ce cas, ils défigureront par exemple le site de l'entreprise en plus du fonctionnement du réseau informatique de celle-ci.

Encore plus anecdotique, mais possible, d'où l'importance de disposer d'une organisation en interne sur « *qui a accès à quoi* » dans le réseau informatique : c'est le « vengeur ». Il s'agit là d'un collaborateur insatisfait, suite à un refus de promotion ou à un licenciement, ayant encore accès au réseau et qui va en profiter pour se venger de son entreprise.

1.3/ Les cibles

Tout le monde peut être visé.

Tout d'abord, il y a les États et les entreprises stratégiques, qui ont été fortement visés ces dernières années. Dans la mesure où ces entités se renforcent progressivement, les attaquants étendent leurs activités aux acteurs privés : les petites et moyennes entreprises, ainsi que les ETI.

Beaucoup d'attaques sont menées de manière indirecte. Profitant d'un prestataire interconnecté mais moins bien protégé, l'attaquant aura un accès au client lui permettant ainsi d'atteindre le système d'information.

La presse parle moins des acteurs privés qui ont peur que cela nuise à leur image. Selon les statistiques de l'ANSSI, le nombre d'entreprises visées est en réalité beaucoup plus élevé. Le nombre de cas référencés ne constitue donc que la partie émergée de l'iceberg.

Entités dont on entend beaucoup parler : les acteurs publics. Hôpitaux, mairies, communes, notamment dans des cas de rançongiciels qui ont eu lieu récemment.

Nous avons tous fait les frais des attaques visant ces acteurs publics. Nous avons été contactés :

- pour récupérer un colis,
- parce que notre vignette Crit'Air n'était pas à jour,
- afin de régler une amende.

Et les attaquants s'adaptent à l'actualité ! À une époque, c'étaient les dons pour l'Ukraine ou « Tous anti-Covid »… Par ce biais, nous recevons de nombreux e-mails comportant des liens malveillants sur lesquels nous avons vite fait de cliquer par manque de vigilance ou simplement parce que l'e-mail était si bien conçu qu'il nous paraît émaner de qui de droit.

Pour souligner mon propos, je citerai le cas du prestataire XEFI, spécialisé en infogérance, qui avait été visé par un rançongiciel et dont les clients, des entreprises et des collectivités, ont pu être atteints par ces attaques. De ce fait, XEFI s'est retrouvé en difficulté financière.

Concernant les individus, il existe beaucoup de tentatives de *phishing*[6], mais également de *smishing*[7] pour les smartphones.

1.4/ L'atteinte des systèmes d'information

Concernant les attaques, comment un attaquant parvient-il à détruire un système d'information ?

Les attaques techniques exploitent une mauvaise configuration d'un système d'information sécurisé ou encore une absence de mise à jour.

Souvent, à réception d'une proposition de mise à jour, nous considérons que nous nous en occuperons plus tard car cela prend du temps et nécessite en outre bien souvent le redémarrage de l'ordinateur. Sauf que ces mises à jour servent à corriger des vulnérabilités qui ont été trouvées par les éditeurs de logiciels et qui sont proposées pour *patcher*[8] et rendre le logiciel à nouveau sécurisé pour les vulnérabilités qui sont connues. Il est donc très important d'appliquer ces mises à jour quand elles sont proposées et de le faire à temps, faute de quoi cela peut avoir de sérieuses conséquences.

Les défauts de configuration présentent également des failles faciles à exploiter pour les attaquants. Par exemple, la mise en place d'un système d'information ou d'une page Internet sans mot de passe ou avec un mot de passe trop faible de type « Soleil 1, 2, 3, 4 ».

Les attaques exploitant le facteur humain. Elles résultent, comme nous l'avons vu, d'un manque de vigilance (clic sur un mauvais e-mail, transfert d'un mauvais e-mail à d'autres personnes en multipliant ainsi les risques), de mots de passe trop faibles…

Les attaques physiques. Elles sont l'œuvre soit d'une personne malveillante, soit d'une personne n'ayant pas connaissance d'avoir été « infectée », qui par exemple vous prête une clé ou vous demande de recharger son téléphone sur votre ordinateur. C'est une

[6] technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance
[7] forme de phishing dans laquelle un attaquant utilise un SMS convaincant pour inciter les destinataires ciblés à cliquer sur un lien et à envoyer à l'attaquant des informations privées ou à télécharger des programmes malveillants sur un smartphone
[8] modifier (un programme…) de façon provisoire pour corriger une erreur en attendant la version suivante

façon d'infecter votre ordinateur, de façon involontaire ou non. Dans ce type d'attaque, on répertorie notamment beaucoup d'histoires de clés USB distribuées sur des salons et dont la finalité n'était pas celle attendue, ayant ainsi eu d'importants impacts.

1.5/ Les bonnes pratiques

Pour 2022, l'ANSSI a relevé :

- un grand nombre d'attaques de PME, de TPE, d'ETI, de collectivités territoriales, d'établissements publics de santé, d'entreprises stratégiques, concluant qu'au final tout le monde pouvait être visé ;
- que 80 % des incidents de sécurité numérique sont liés à des erreurs humaines.

Ainsi, si le terme cybersécurité fait un peu peur et que l'on ne sait pas toujours ce qu'il englobe, il apparaît qu'avec une application de sécurité au sein de son entreprise on peut toutefois déjà se prémunir des risques liés à la cybermenace et ainsi éviter des dommages dont il faut parfois du temps pour se remettre.

Dans ces conditions, l'ANSSI insiste beaucoup sur la sensibilisation. À ce titre, je vous recommande le MOOC[9] de l'ANSSI. Il s'agit d'une plateforme gratuite en ligne proposant plusieurs modules de 10 à 15 minutes qui permettent d'avoir une première sensibilisation sur les risques et l'utilisation des outils informatiques, que ce soit au niveau personnel ou professionnel.

L'ANSSI publie également des guides abordant des sujets techniques et très spécifiques, mais également d'autres plus génériques. Ainsi et pour une entreprise assez structurée en termes informatiques et dont l'effectif comporte au moins une cinquantaine de personnes, nous recommandons le *Guide de l'hygiène informatique* comportant 42 mesures. Ainsi, il est nécessaire que la réponse à la cybermenace soit adaptée à la structure et de connaître impérativement les risques inhérents au fonctionnement de cette structure. Ce guide permet de se poser les premières questions en matière de cybersécurité.

[9] « Massive Open Online Course » que l'on peut traduire par « cours en ligne ouvert et massif »

À l'usage des TPE et PME, l'ANSSI propose le *Guide des bonnes pratiques de l'informatique*, document qui peut également être utilisé à titre individuel. Il comprend un ensemble de recommandations (par exemple : séparer ses usages personnels et professionnels, avoir une politique de mots de passe, etc.) et la manière de les mettre en place.

En définitive et face à la cybermenace, le plus important reste la préparation. Il ne faut pas se demander si on va être attaqué, mais plutôt se demander quand. Avec un maximum d'anticipation, je peux vous assurer qu'il est possible de réduire cette phase de flou qui peut se produire en cas d'attaque et qui est extrêmement traumatisante, à la fois pour les dirigeants et les collaborateurs. Ce plan de préparation peut tenir sur une page recto-verso :

- quel est le plan de communication ?
- qui contacter en interne ?
- sur le plan technique et en externe, qui contacter ?

Je peux vous assurer que cela réduit déjà cette période d'incertitude qui est très impactante.

Je vous remercie et vous laisse mon contact si vous avez des questions, étant précisé que nous sommes deux personnes en région à votre disposition pour vous répondre.

M. Philippe LAMBERT.- Merci Madame Delarue. Pour rebondir sur vos propos, il apparaît en effet qu'il est vital de se préparer à la cybercriminalité en mettant en place des mesures de cybersécurité. Pourquoi cela ?

Dans un livre récent, *« 13 défis de la cybersécurité »* (paru au CNRS), il est mentionné que la cybersécurité est une science récente parce qu'avant on ne pensait pas cybersécurité, on ne pensait pas se faire attaquer et les outils correspondants n'étaient donc pas prêts.

Or et comme l'a dit Madame Delarue, aujourd'hui, il est nécessaire de suivre l'évolution des logiciels dans la mesure où il est possible de tracer des équipements que vous avez dans votre entreprise, des caméras de vidéosurveillance… Ainsi et dans une précédente conférence, j'avais réalisé une démonstration en montrant comment, depuis Internet, il est possible de repérer les caméras dans les entreprises, de rentrer sur le site de la caméra et de modifier son contenu.

Dans ces conditions et devant la mondialisation de l'information, il est nécessaire de disposer de lois en la matière, ce que va évoquer Maître Moussa à qui je cède la parole.

2 Un cadre légal étendu

Bonjour à tous.

Je suis avocat au Barreau de Lyon, spécialisé en propriété intellectuelle et nouvelles technologies.

Madame Delarue, dans votre intervention, vous avez rappelé des choses que j'ai trouvées frappantes et notamment celle-ci : en réalité, chacun est concerné.

Nos clients peuvent avoir des activités industrielles ou de services et le terme « cyber quelque chose » peut leur paraître un peu lointain ou impressionnant. On sait un peu mieux aujourd'hui, et l'actualité nous le rappelle tous les jours, qu'en réalité cette problématique nous concerne tous.

D'ailleurs, je profite de mon intervention pour vous dire que le Barreau de Lyon, particulièrement sensible à ce sujet, comporte une Commission spécialisée consacrée aux nouvelles technologies que j'ai l'honneur de coprésider.

Je me félicite de la présence parmi nous aujourd'hui de Madame la Bâtonnière ainsi que de nombre de mes confrères, marquant ainsi, à l'intention de la Compagnie, que je remercie, l'importance que nous attachons à l'assistance de nos clients sur ces questions.

Je vais vous parler aujourd'hui principalement des prestations de conseil que nous apportons à nos clients qui sont victimes de ce type de faits même si, en tant qu'avocats, nous défendons aussi les mis en cause.

Je laisserai Monsieur l'Avocat Général évoquer la réglementation qui s'applique aux personnes qui commettent ce type de faits et sur ce sujet je me contenterai de vous rapporter une anecdote que j'évoquais avec lui avant notre intervention. Lorsque j'étais jeune avocat, les attaques étaient parfois un peu moins sophistiquées que celles que nous connaissons aujourd'hui. Ainsi, je me souviens d'un appel pour une garde à vue sur un fait de délinquance financière et cyber. J'avais été extrêmement intéressé par cette garde à vue inhabituelle car j'espérais enfin découvrir comment on procédait pour commettre ce type de faits. Ce dossier s'est avéré assez décevant puisqu'il s'agissait du comptable d'une entreprise qui s'était ménagé un accès aux identifiants du compte bancaire de la société et effectuait des virements directement sur son compte personnel. C'est une attaque que Madame Delarue qualifierait sans doute d'humaine. J'avais été extrêmement déçu par la simplicité de cette attaque.

Aujourd'hui, les outils se sont multipliés et les attaques se sont sophistiquées et nous assistons nos clients dans la prévention de ce type d'attaques (2.1). Nous les assistons aussi lorsque l'inévitable se produit et qu'il faut réagir (2.2).

2.1/ Prévenir les atteintes au système d'information

Pourquoi faut-il s'occuper de la cybersécurité ? D'abord parce que c'est l'intérêt de l'entreprise, mais aussi parce que c'est une obligation légale pour la plupart de nos clients et ce en vertu de différentes réglementations.

2.1.1/ Le cadre légal

2.1.1.1/ Concernant les données personnelles

La réglementation que nous connaissons le plus c'est sans doute le RGPD[10], que nous devons respecter lorsque nous traitons des données personnelles. Ce règlement impose aux responsables de traitement, que nous sommes tous, de sécuriser leurs systèmes d'information. C'est l'un des premiers articles du RGPD, qui impose de prévoir un niveau de sécurité adapté.

La Loi Informatique et Libertés de 1978[11] n'a pas disparu et est encore en vigueur. Elle impose elle aussi des obligations à toutes les personnes physiques et morales traitant des données personnelles. Ainsi, lorsqu'on traite des données personnelles, on est soumis à des obligations de sécurisation et de conservation des données dans des conditions permettant d'empêcher :

- les personnes non autorisées d'y accéder,
- l'introduction de données,
- de fausser le système.

C'est donc un premier ensemble de textes qui obligent nos clients à sécuriser leur système. C'est pour la partie données personnelles.

2.1.1.2/ Concernant les données en général

1. Une réglementation existe aujourd'hui pour les données non personnelles, et elle est amenée à se développer.

Il s'agit d'abord d'une directive dite NIS 1[12], transposée en France en 2018, et qui prévoit un certain nombre d'obligations pour les opérateurs de services essentiels : ils

[10] Règlement Général sur la Protection des Données, adopté par le Parlement européen en 2016 et entré en vigueur en 2018
[11] La loi n° 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, plus connue sous le nom de loi informatique et libertés, est une loi française qui réglemente le traitement des données personnelles
[12] Directive network and Information Security dite « directive NIS ». Adoptée par le Parlement européen et le Conseil de l'Union européenne le 6 juillet 2016, et ce après trois ans de négociation. Les États membres avaient jusqu'au 9 mai 2018 pour la transposer dans leur droit national

doivent suivre des règles définies par l'ANSSI et déclarer les incidents. Ils sont susceptibles de subir des contrôles pour vérifier s'ils ont bien mis en œuvre ces règles.

D'autres personnes sont visées : les fournisseurs de service numérique, avec un niveau d'obligations cependant moindre.

Ce sont deux typologies d'acteurs économiques, qui doivent déjà depuis plusieurs années mettre en œuvre un certain nombre de mesures de sécurité.

2. Dès octobre 2024, c'est-à-dire dès demain, cette réglementation sera élargie à un assez grand nombre d'opérateurs économiques par une directive dite NIS 2[13]. Elle s'applique à des entités dites essentielles ou importantes qui opèrent dans des secteurs dits critiques et hautement critiques. L'ensemble de ces opérateurs, qui interviennent dans un grand nombre de secteurs, devront d'abord effectuer une analyse de leurs risques et, face aux risques ainsi identifiés, mettre en œuvre un certain nombre de mesures.

Ce qui est intéressant c'est que ces obligations ne concernent pas seulement les opérateurs ainsi identifiés, dont on pourrait croire qu'ils sont peu nombreux. La directive, et demain sa transposition en droit français, leur imposera de sécuriser toute leur chaîne d'approvisionnement. Ce qui veut dire que leurs prestataires devront eux aussi se mettre au niveau. Je pense que c'est très intéressant car on sait que les attaques ne concernent pas toujours directement les cibles identifiées comme potentiellement pertinentes, mais aussi d'autres maillons de la chaîne par lesquels il est plus facile de s'introduire dans le système. Mécaniquement, les plus petits sont moins sécurisés et restent donc une porte d'entrée. La réglementation européenne a prévu cela et imposera aux donneurs d'ordres de vérifier le niveau de sécurité de l'ensemble de cette chaîne et de leurs sous-traitants.

3. Le Code de la consommation prévoit et prévoira pour une catégorie particulière qui concerne les plateformes l'obligation d'un audit afin de leur décerner un « cyber score ». Vous en entendrez parler en octobre 2023, autant vous dire que là encore c'est demain. Il faut s'y préparer. Les modalités de cet audit ne sont pas encore connues même si l'ANSSI est certainement déjà à l'œuvre concernant ce point. À terme, les plateformes devront donc afficher d'une façon compréhensible pour les consommateurs les règles qu'elles mettent en place pour sécuriser les données de ces derniers ainsi que leur propre fonctionnement.

[13] Votée le par les députés européens le 10 novembre 2022, la directive NIS 2 vise à harmoniser et à renforcer la cybersécurité du marché européen. En France, de nombreuses entreprises et administrations seront soumises à cette nouvelle règlementation

Vous constatez que l'on a là un cadre légal relativement étendu. Dans ces conditions, la cybersécurité ne relève plus seulement de la bonne pratique, mais de plus en plus souvent et pour beaucoup d'acteurs d'une obligation légale sanctionnée assez lourdement en cas d'infraction. Pour le RGPD, cela se compte en millions d'euros. Il existe aussi des sanctions pénales associées, qui sont définies par le Code pénal qui prévoit, même si c'est rarement appliqué, cinq ans d'emprisonnement et 300 000 € d'amende lorsque l'on a traité des données personnelles sans avoir respecté les exigences prévues par la réglementation. Cela nous donne matière collectivement à intervenir auprès de nos clients en prévention.

2.1.2/ Le cadre contractuel

Il est nécessaire de mettre en place un cadre contractuel en interne et en externe, qui permet de déployer ces obligations réglementaires chez le client et auprès de ses prestataires. Dans ce contexte, l'entreprise n'est pas la seule concernée, son personnel doit être engagé dans cette démarche.

2.1.2.1/ Le cadre contractuel interne à l'entreprise : règlement intérieur, charte informatique

Ainsi, il convient d'inciter les entreprises à mettre en place des chartes informatiques. Le terme de charte est trompeur, car il paraît peu contraignant. Et de fait, pour que cet outil soit efficace, il faut donner à cette charte force obligatoire :

- en l'intégrant au règlement intérieur ;
- en la faisant voter par les instances représentatives du personnel ;
- d'une manière ou d'une autre, en l'intégrant aux contrats de travail.

En outre, il est impératif que les obligations résultant de cette charte ne restent pas lettre morte et qu'elles soient appliquées au sein de l'entreprise.

La charte informatique en elle-même n'est pas un document mystérieux. Elle a vocation à reprendre à peu près tout ce que vous avez dit, Madame Delarue, c'est-à-dire des obligations d'hygiène informatique. À cet égard, les documents de l'ANSSI sont une très bonne base de travail. On peut citer :

- les obligations de loyauté,
- les obligations de confidentialité,

- l'obligation d'utiliser les outils de sécurisation que l'employeur met à disposition de ses salariés.

Dans le même registre, il n'est pas recommandé de se connecter à Internet n'importe où. Je ne sais pas qui est connecté au réseau wifi[14] de l'hôtel qui nous accueille en ce moment-même sans VPN[15]. Ce serait intéressant que nous levions la main les uns et les autres. On n'utilise pas non plus les clés USB que l'on distribue dans les salons.

Avec le confinement et l'essor du télétravail que nous avons tous connu, il est devenu impératif de gérer de façon plus précise ce mode de travail. Dans ce contexte, la question de ce que l'on appelle encore le BYOD[16], à savoir l'utilisation de terminaux personnels pour accéder au réseau de l'entreprise, doit être encadrée.

Il est enfin nécessaire d'informer les salariés que l'employeur se dote de moyens de contrôle. En effet, pour pouvoir sanctionner les salariés qui ne respectent pas ces obligations, il est impératif que l'employeur ait prévenu les salariés qu'ils sont surveillés, faute de quoi toute preuve recueillie par l'employeur serait inexploitable.

2.1.2.2/ Le cadre contractuel externe à l'entreprise

Je ne reviens pas en détail sur le fait que ces obligations doivent également être étendues aux tiers et aux prestataires de l'entreprise, aux fournisseurs, aux sous-traitants et aux stagiaires, qui ne sont pas soumis au règlement intérieur et qui n'ont pas de contrat de travail, notamment aux doctorants intervenant dans le cadre de recherches. Toutes ces personnes gravitant dans la sphère de l'entreprise sans en faire partie sont autant de « portes d'entrée » exploitables pour attaquer l'entreprise, raison pour laquelle il est nécessaire que cette dernière se montre vigilante sur les obligations qu'elle peut leur imposer ainsi que sur les moyens de contrôle qu'elle peut avoir sur leurs activités.

[14] Le (ou la) Wi-Fi, aussi orthographié wifi, est un ensemble de protocoles de communication sans fil régis par les normes du groupe IEEE 802.11 (ISO/CEI 8802-11). Un réseau Wi-Fi permet de relier par ondes radio plusieurs appareils informatiques (ordinateur, routeur, smartphone, modem Internet, etc.)

[15] Un Réseau privé virtuel (Virtual Private Network ou VPN en anglais) est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics

[16] Bring Your Own Device

2.1.2.3/ Un contrat d'assurance spécifique

Dans le cadre légal et contractuel dans lequel nous intervenons, il faut aussi se préparer au moment où nous allons intervenir en cas de sinistre. Cela passe par deux choses : la souscription d'un contrat d'assurance (sans attendre, comme c'est souvent le cas, d'avoir subi un premier sinistre) et la définition d'un plan d'action pour agir au moment du sinistre.

Le contrat d'assurance du risque cyber est encore une rareté. On connaît effectivement des contrats dédiés mis en place par quelques assureurs qui, à ma connaissance, ne se précipitent pas pour envahir le marché parce que le risque est, d'une part, difficile à identifier et, d'autre part, croissant, ce qui ne plaît pas forcément aux assureurs.

En revanche et dans plus en plus de contrats classiques apparaissent des clauses d'exclusion. Il faut donc être très vigilant sur ce risque et tenter de l'assurer par des contrats dédiés.

Ce ne sont pas des contrats que l'on peut conclure à la légère. Les assureurs ne les acceptent qu'à condition de respecter un certain nombre de prérequis, notamment :

- s'engager à mettre en place les règles de sécurité dont nous avons déjà parlé ;
- s'engager sur la licéité des logiciels utilisés par l'entreprise : preuve de l'obtention des licences correspondantes, mises à jour régulières ;
- disposer de procédures en cas d'attaque.

Si l'entreprise répond à ces prérequis, deux types de risques peuvent être couverts en cas d'intrusion dans votre système :

- votre système comporte une faille qui permet à un attaquant de s'introduire pour causer un préjudice à un tiers : il s'agit d'un risque de responsabilité civile que vous pouvez couvrir par le contrat d'assurance ;
- la continuité d'exploitation de l'entreprise est remise en cause en cas de rançongiciel : il s'agit d'un préjudice pour lequel l'assureur peut vous indemniser.

Je dois dire qu'il faut profiter de ce type de contrat tant qu'il existe dans la mesure où, les risques liés à la cybermenace se déployant, les assureurs ont tendance à se replier ou à limiter la couverture sur ce marché.

2.2/ Traiter les atteintes au système d'information

Une fois que l'entreprise respecte le cadre légal, met en place des politiques contractuelles en interne et en externe et a souscrit un contrat d'assurance, on peut considérer que tout a été fait pour prévenir le risque d'une attaque.

Dans ces conditions, en cas d'attaque, notre intervention en tant qu'avocat en est facilitée. Notre rôle auprès de nos clients se divise alors en trois temps.

Dans un premier temps, qui est traditionnel dans nos interventions, il s'agit de préserver la preuve de l'attaque et de l'intrusion. Il est donc nécessaire :

- de recourir à un huissier de justice spécialisé en la matière ;
- de tenter de prendre très rapidement une photographie de l'ensemble du système d'information pour permettre le succès des investigations ultérieures, dans la mesure où l'attaque n'a pas forcément eu lieu à l'endroit où elle est recherchée.

Dans un deuxième temps, il faut également déposer plainte, d'abord parce que c'est une saine pratique et puis parce que, d'ici trois semaines, la loi nous imposera, si nous souhaitons pouvoir percevoir l'indemnité prévue par un contrat d'assurance, d'avoir déposé plainte dans les 72 heures à partir du moment où on a connaissance de l'attaque.

Dans un troisième temps, le RGPD vous impose dans un certain nombre de cas de notifier l'atteinte au traitement de données personnelles à la CNIL[17], là encore dans un délai très réduit et, un peu plus tard, de communiquer aux personnes concernées le fait que leurs données ont été atteintes.

* * * * *

Comme vous le constatez, à partir du moment où l'attaque se produit et où vous en avez connaissance, vous avez très peu de temps pour faire énormément de choses – et je ne parle pas ici de la nécessité d'assurer la continuité de l'exploitation.

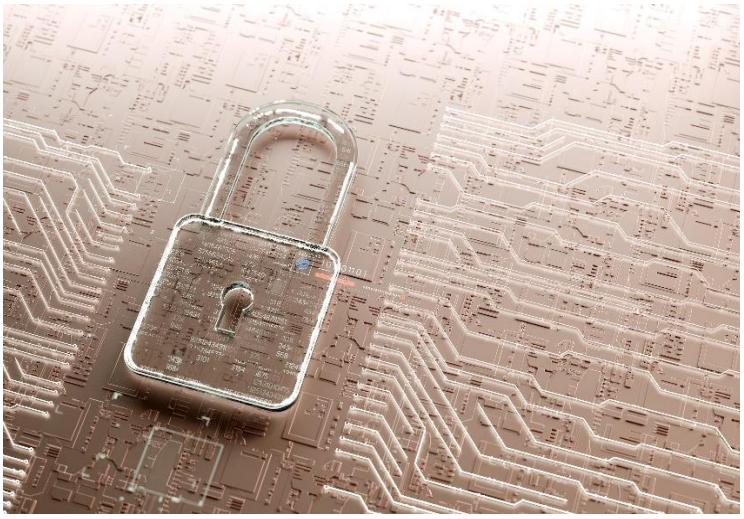
[17] Commission nationale de l'informatique et des libertés

Même en étant bien préparé, on ne sait pas quand l'attaque va se produire et quel sera le risque qui va se réaliser. Dans ces conditions, si rien n'est mis en place en amont, on peut se retrouver dans des situations très difficiles.

Le mot-clé est donc d'anticiper.

M. Philippe LAMBERT.- Merci Maître. Nous avons vu qu'il y a tout un aspect légal des procédures à mettre en place pour l'étude de l'impact, qui est repris aussi dans le cadre du RGPD. Mais il existe aussi toute une institution judiciaire et là je vais m'adresser à Monsieur le Substitut général, Monsieur Ducrocq, pour évoquer tout ce qui a été mis en place.

3 L’aspect de la criminalité



Merci beaucoup.

Je me présente, je suis Substitut général. Je vais évoquer l’aspect cybercriminalité. J’ai axé mon intervention sur certains aspects de la cybercriminalité qui, je pense, vous intéressent le plus en tant que TPE, PME et experts-comptables.

3.1/ Deux grandes catégories d’impacts

Sur l’évaluation des menaces, j’ai d’abord voulu expliquer ce qu’est la cybercriminalité au niveau judiciaire. Au niveau pénal, il existe deux grandes catégories :

- soit des infractions commises à l’aide de l’outil informatique. C’est le cas des escroqueries au changement de RIB. On va changer un RIB légitime d’un de vos clients ou de vos prestataires en un RIB illégitime ;
- soit un ciblage de la technologie, en plus de s’appuyer sur la technologie numérique. C’est ce qui a déjà été indiqué par l’ANSSI. C’est le cas des atteintes au STAD[18] et des rançongiciels que l’on appelle en réalité par l’anglicisme *« ransomwares »*.

À cela répondent, à mon sens, trois types d’infractions pour les entreprises, qui vous concernent tous en réalité.

[18] système de traitement automatisé de données

3.2/ Pour trois types d'infractions

Le traditionnel FOVI, les faux ordres de virements. Un faux éditeur de logiciels, de comptabilité ou un responsable informatique, va prendre le contrôle de votre poste de travail ou de votre poste informatique pour en extraire des fonds ou effectuer des mouvements bancaires non désirés.

Pour exemple, l'escroquerie au « faux président » : un faux président d'une société va indiquer que c'est urgent et qu'il faut effectuer un virement.

Le rançongiciel. Je ne vais pas le détailler. L'ANSSI l'a bien expliqué. Vous n'avez plus accès à votre logiciel SAGE de comptabilité en ligne.

Les fuites de données : en réalité, ce type de menaces vous concerne peu. Vous pouvez vous concentrer sur le FOVI et le rançongiciel puisque les fuites de données, c'est-à-dire la peur de perdre vos données personnelles, représentent en l'état 8 % de la menace. En comparaison, les FOVI et les rançongiciels représentent chacun aux alentours de 40 % des « parts de marché ».

3.3/ L'intérêt pour les délinquants

Pour les délinquants :

- c'est rentable et facile. Le chiffre clé c'est 5 dollars le kit de piratage de données sur le darknet[19]. C'est très facile pour l'adolescent ou l'étudiant de se procurer ce type d'outils ;
- une réputation d'impunité internationale parce que justement ce type de délinquance se considère internationale, même si en réalité nous avons aussi des délinquants au niveau national.

[19] Un darknet est un réseau superposé (ou réseau overlay) qui utilise des protocoles spécifiques intégrant des fonctions d'anonymat

3.4/ L'impact sur l'économie

Tout d'abord, précisons que ce n'est plus une honte d'avoir fait l'expérience d'une cyberattaque puisque 90 % des entreprises en France le disent, sachant que 43 % de ces attaques ciblaient des PME en 2020.

Cependant, ces attaques ont un impact réel sur l'économie. Pour s'en faire une idée, il suffit de citer les chiffres astronomiques des pertes :

- 720 M€ selon la Fédération des comptes de France,
- 8 M€ en coûts moyens par entreprise en 2018.

Concernant ces pertes, j'insisterai sur l'attaque au « faux président » que j'ai évoquée précédemment car, si elle représente seulement 7 % des infractions, elle s'élève en revanche à 43 % des préjudices, ce qui est extrêmement important.

Enfin, j'ajouterai que les PME et TPE sont particulièrement sensibles aux rançongiciels puisqu'elles représentent 70 % des attaques.

Très rapidement brossée, l'analyse judiciaire qui est faite de ces menaces : c'est un contentieux très technique, de masse, protéiforme à l'international.

3.5/ Les réponses aux attaques

Deux types de réponses : à la fois la prévention et la répression.

Concernant la prévention, très schématiquement, je l'ai axée sur cinq points de vigilance :

- les deux premiers : la vigilance des agences, comme l'ont dit Maître Moussa et l'ANSSI, c'est mettre en place des process de vérification. Je ne vais pas insister. Investir dans la cybersécurité privée. Vous avez la CNIL, au point de vue administratif, des amendes entre 400 000 € et 500 000 € sur des défauts de respect lorsque vous avez à gérer un STAD vous-même. Le défaut de sécurisation, ce sont des amendes administratives, mais aussi des sanctions pénales : 5 ans d'emprisonnement et 300 000 € d'amende ;
- troisième point : le *recall* bancaire. C'est un système très variable en fonction des banques et des changes. Vous avez fait un virement bancaire illégitime au profit d'un

escroc. L'un des premiers réflexes que vous devez avoir, à mon sens, est d'appeler votre banque pour demander que les fonds reviennent chez vous. C'est le *recall* bancaire. C'est très variable. Concernant des dispositifs français, ce n'est pas possible, mais concernant l'international il faut compter un délai compris entre 4 et 14 jours ;

- quatrième point : préparer l'attaque. En fonction de votre niveau de sensibilité, c'est contacter et connaître les références cyberpolice et gendarmerie. En fait, il s'agit d'un réseau de policiers et de gendarmes qui sont référencés. Il existe depuis 2018 et vous pouvez disposer de l'identité des personnes le constituant ;
- cinquième et dernier point de vigilance, qui n'en est quasiment plus un : la réactivité en cas d'attaque. Il faut déposer plainte très vite puisque le seul constat d'huissier ne suffit pas car il s'agit avant tout d'un aspect judiciaire dans la mesure où vous êtes victime d'une infraction. Vous pouvez déposer plainte en tant que société et personne morale, tout de suite, avec un responsable informatique ce qui est fortement préconisé, en tout cas avec une personne qui gère l'informatique de votre société afin de pouvoir aiguiller les enquêteurs et/ou signaler les faits.

Concernant la répression, pour pouvoir investiguer, il est nécessaire de disposer de beaucoup d'informations au niveau judiciaire, et ce afin de procéder à des recoupements concernant les délinquants qui sévissent sur Internet.

Un exemple, pour mémoire, car il ne concerne que les particuliers en nom propre : la plateforme THESEE, créée en mars 2022, qui fonctionne très bien avec cependant 85 000 plaintes et signalements.

Dans ces conditions, je rappelle cette nouvelle disposition du Code des assurances qui vous contraint à déposer plainte dans un délai de 72 heures à compter de la connaissance de l'attaque. Si, lors des investigations, l'assureur apprend que vous aviez connaissance de cette attaque et que vous n'avez pas agi dans le délai prescrit, cela vous exposera à des difficultés dans le remboursement des sommes perdues.

L'aspect répression, à mon sens, est assez simple. Contrairement à l'idée reçue du sentiment d'impunité, la justice et surtout les services d'enquête se sont adaptés à cette nouvelle modalité de délinquance.

3.6/ Des moyens de preuve et de saisie des avoirs criminels

La cyberpatrouille : vous avez de plus en plus de services d'enquête, de gendarmerie, de police et de douanes, qui patrouillent, qui recherchent et qui récupèrent des informations sur Internet, le darknet et les avatars du Web.

Les enquêtes sous pseudonyme sont possibles. L'enquêteur ne va pas dire qui il est réellement et investiguer.

La saisie d'avoirs criminels : si vous n'avez pas pu récupérer votre argent, il est possible que l'enquêteur saisisse l'argent des délinquants. Il existe une politique offensive de saisie des avoirs criminels des délinquants, notamment des cyberdélinquants. Cela est de plus en plus répandu.

Un point important : l'expertise judiciaire numérique. En termes probatoires, beaucoup de progrès sont faits. En effet, le numérique laisse des traces de mieux en mieux et de plus en plus identifiées.

3.7/ Juridictions : les différents niveaux

Au niveau judiciaire, la réponse aux attaques est graduée.

À mon sens, et c'est en fait ce qu'indique le plan de stratégie nationale élaboré en 2020, tout ce qui est de faible intensité, des cyberattaques liées à des erreurs humaines à des failles de sécurité de mise à jour, avec un jeune qui viendrait pirater votre système sans connaissance particulière en la matière, devrait faire l'objet d'une cybersécurité des particuliers et entreprises afin que ces cas tendent à disparaître.

Au-dessus de cela, sont mis en place des enquêteurs qui se sont spécialisés au niveau départemental, sûreté et brigades de recherche, pour tout ce qui est de moyenne intensité, type escroquerie par Internet.

Deux éléments qui vous concernent en tant que PME et TPE, très peu à titre individuel, mais en réalité vous pouvez être victimes d'attaques de grande envergure. Ce sont les attaques en haut du spectre et très haut du spectre qui sont par exemple des attaques au STAD.

Dans ces cas, deux grandes juridictions :

1/ la JIRS[20] avec tout ce qui est international, préjudice élevé et technicité d'attaques.

Les services d'enquête spécialisés sur lesquels les JIRS s'appuient sont la police judiciaire et la section de recherche. Le cas échéant, je laisserai Monsieur Mérien détailler ce point dans son intervention ;

2/ au niveau national et international, le très haut du spectre, c'est la JUNALCO[21] section J3, à Paris, qui dirige les investigations concernant par exemple :

- les attaques ayant pour cible les opérateurs d'importance vitale,
- les cyberattaques d'hôpitaux,
- les déphasages de sites Internet nationaux très spécialisés et très sensibles.

Dans ce contexte, les enquêtes sont menées par des services très spécialisés : DGSI[22], C3N[23] et offices centraux. Tout le monde agit dans le but de réprimer ces agissements.

3.8/ Les sanctions

Sur l'aspect purement légal, la loi évolue en permanence. Je ne vais citer que la loi toute récente du 24 janvier 2023[24] dont je reprendrai ici les points importants :

- aggravation des peines relatives aux atteintes au STAD qui passent de 7 à 10 ans. C'est le maximum en termes de délit contre l'État, les hôpitaux… Dans la mesure où ce sont ces attaques qui vous concernent le plus, il faut tenter au maximum de s'en prémunir en sécurisant ses systèmes et données le mieux possible ;
- les saisies d'actifs numériques : c'est un peu mon fil rouge. Les services d'enquête peuvent récupérer votre argent plus facilement avec cette nouvelle loi, d'où l'intérêt de déposer plainte le plus rapidement possible.

Les sanctions deviennent également de plus en plus internationales, puisqu'il existe des délinquants russophones, chinois… Cette délinquance n'ayant pas de frontières, il est

[20] Juridiction Interrégionale Spécialisée
[21] Juridiction nationale chargée de la lutte contre la criminalité organisée
[22] Direction générale de la Sécurité intérieure
[23] Centre de lutte contre les criminalités numériques
[24] Loi du 24 janvier 2023 d'orientation et de programmation du ministère de l'Intérieur

devenu nécessaire de disposer d'outils probatoires internationaux, tels que les Conventions de Budapest[25] (2ème protocole), qui sont en train d'être signées et d'être mises en place avec des plateformes idoines.

3.9/ Pour conclure

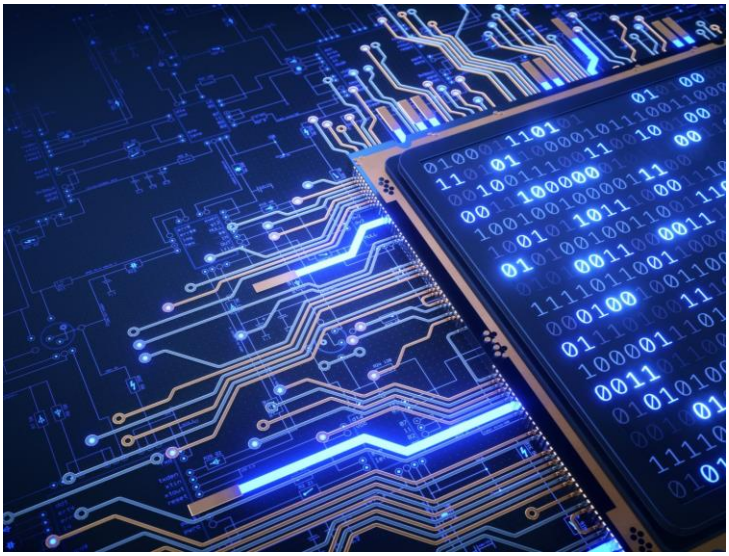
En synthèse, mon message se résume donc en trois points clés :

- investir dans un système d'alarme informatique, comme vous pouvez investir dans votre habitation. Ceci doit devenir une pratique commune ;
- signaler immédiatement à la justice les faits délictueux en déposant plainte. Prévoir c'est bien, signaler c'est encore mieux ;
- malgré la réputation d'impunité que l'on peut donner à ce type de délinquance, la justice est bien là et réprime la cybercriminalité.

M. Philippe LAMBERT.- Merci Monsieur le Substitut général. Je vais maintenant m'adresser à Monsieur Mérien, concernant la partie « terrain », c'est-à-dire la gendarmerie qui assiste la justice.

[25] Convention du Conseil de l'Europe sur la cybercriminalité : il s'agissait du premier accord international au monde visant à lutter contre les activités criminelles en ligne – Budapest, 23.XI.2001

4 Les différentes formes de la cybercriminalité



Bonjour à tous.

Je suis lieutenant et militaire de la gendarmerie. Je suis affecté à la section de recherche de Lyon qui travaille principalement avec la JIRS et la JUNALCO. J'occupe un poste de commandement dans une division spécialisée en délinquance cyber et en délinquance financière.

Je souhaite vous présenter les différentes thématiques qui existent principalement dans le cyber. Cela a déjà été abordé. Il y a les rançongiciels, les FOVI, le *jackpotting*, le *skimming*, malheureusement, beaucoup de pédopornographie et énormément d'escroquerie en bande organisée.

Cela a été présenté tout à l'heure par l'ANSSI. Il existe différents niveaux d'attaques avec différentes motivations. Nous sommes tous concernés. Du moment que l'on existe, on offre une surface d'attaque à des attaquants. La question n'est pas de savoir si on va être attaqué, mais quand et il faut s'y préparer.

C'est un peu comme une image d'Épinal :

- le matin, on se lave les dents avant de sortir ;
- on ne sort pas pieds nus quand le goudron est brûlant.

En résumé, le volet préparation et le volet prévention sont avant tout des réflexes qu'il faut appliquer à la cybersécurité.

Je commencerai par les deux principales thématiques à retenir : le *ransomware* et le FOVI, cas dans lesquels vous êtes les plus touchés.

4.1/ Le ransomware

Comme cela a déjà été dit, il est nécessaire de déposer rapidement plainte. J'insiste sur ce point car il est vraiment essentiel. Cela permet d'avoir une réponse juridique rapide, d'effectuer les demandes de *recall* et de récupérer l'argent en cryptoactifs, et ce particulièrement dans le cas des *ransomwares*. Concernant ces derniers, nous demandons aux victimes de ne pas payer la rançon car, si à réception de la rançon vous obtiendrez une clé de déchiffrement, rien ne certifie qu'elle pourra servir à déchiffrer l'intégralité de vos données. Cela pourrait donc vous inciter à payer une nouvelle rançon avec pour seul résultat de recevoir une partie seulement de la clé de déchiffrement. Ce n'est pas du tout intéressant pour vous.

En revanche, si vous vous êtes préparé, si vous avez des solutions de *back-up*, si vous avez de quoi remettre votre système informatique en place, dans ce cas, payer la rançon ne présente aucun intérêt puisque vous pouvez très rapidement remettre votre système informatique en place.

Déposer plainte le plus rapidement possible c'est bien, déposer une plainte avec des éléments de preuve c'est essentiel pour nous, et ce afin de pouvoir réagir également très rapidement à l'événement.

Pour les PME comme pour n'importe quelle entreprise, il est très important de disposer de « fiches réflexes » afin de disposer d'éléments clés à nous fournir et qui nous permettront de traiter le dossier.

Pour nous, ce qui est important, c'est cette préservation des éléments de preuve. Nous allons chercher :

- à obtenir la chronologie des événements réseau,
- à connaître l'architecture de votre réseau informatique,

- à obtenir un échantillon des données qui ont été chiffrées pour pouvoir attribuer un rançongiciel et définir sous quel rançongiciel vous avez été attaqué.

Nous vous demanderons également :

- les fichiers de journalisation,
- des informations sur votre réseau, vos pare-feux, vos routeurs, vos systèmes de protection.

Plus nous aurons d'informations à analyser, plus nous aurons de chance de remonter l'attaque et potentiellement d'attribuer cette attaque à qui de droit.

Nous chercherons également à obtenir les données relatives au paiement. Je ne vous le souhaite pas, mais lorsque vous aurez été piraté par un rançongiciel, il y aura une demande de rançon, qui est faite en cryptomonnaies. Il nous faut donc ces informations afin d'être en mesure de retracer les flux.

Très rapidement, nous procédons aux auditions :

- celle de la personne qui a constaté en premier l'attaque,
- celle du responsable de la sécurité des systèmes d'information,

et ce pour disposer de deux auditions de témoins lors du dépôt de plainte.

Au niveau des services enquêteurs, nous analyserons la souche afin d'attribuer très rapidement le rançongiciel à un service spécialisé. En effet, chaque section de recherche et chaque unité de police judiciaire spécialisée s'est vu attribuer plusieurs familles de rançongiciels afin de travailler spécifiquement dessus.

Après avoir analysé l'intégralité des fichiers de journalisation à notre disposition, nous tenterons d'identifier et d'attribuer les différentes adresses IP et ainsi de remonter au mieux, avec l'aide des enquêteurs spécialisés, les flux financiers cryptoactifs et donc aux portefeuilles et aux personnes qui détiennent ces portefeuilles de cryptoactifs.

4.2/ Les FOVI

Les FOVI (les faux ordres de virement) sont bien plus répandus que nous le pensons. À la section de recherche, ils représentent plus de 30 % de notre portefeuille d'enquêtes. Ils sont surtout réalisés par l'ingénierie sociale (le *social engineering*) où le vecteur de l'attaque sera l'humain.

Comme déjà évoqué, une personne externe à la société va se faire passer pour une personne très importante et demander au comptable de réaliser un virement dans la plus grande discrétion à la demande du PDG sur un RIB untel, et le tout en utilisant des techniques pour usurper une adresse mail et donc au final cacher son identité. Des virements vont être réalisés, la plupart du temps pour des sommes astronomiques. Plusieurs millions d'euros sont ainsi détournés par ce type attaque.

C'est impressionnant et l'impact n'est pas accusé par la seule société. Il est également ressenti par les collaborateurs de l'entreprise. Devant l'ampleur des pertes générées par ces attaques, des comptables ou des secrétaires peuvent tomber en dépression, voire commettre l'irréparable. En effet, des licenciements ont lieu et qui dit licenciements dit familles détruites car plus en mesure d'assumer les charges familiales. Il existe donc un réel impact humain derrière ces attaques.

Sur ce type d'attaque, l'urgence sera d'effectuer immédiatement une demande de *recall* comme le signalait Monsieur le Substitut général. Plus tôt la demande sera faite, plus vous pourrez récupérer votre argent. C'est le premier réflexe à avoir en cas de FOVI, lorsque vous vous en rendez compte. Il faut contacter votre banque et absolument réaliser ce *recall*.

Très rapidement, il est également nécessaire de réaliser un dépôt de plainte auprès d'un service de police ou de gendarmerie, en fonction de votre zone de domiciliation ou de la zone des faits.

Afin de nous permettre de mener au mieux nos investigations, il est vital de se présenter avec un maximum d'informations :

- la façon dont vous avez été contacté (par mail ou par téléphone) ;

- si c'est par mail, nous apporter tous les enregistrements concernant ces mails afin que nous puissions mener des investigations cyber et remonter à la source de ces mails ;
- si c'est par téléphone, nous donner le numéro de téléphone et le maximum d'informations sur la personne qui vous a contacté. Avait-elle un accent ? Comment s'exprimait-elle ?
- les numéros des comptes bancaires qui ont été utilisés, les différents RIB, les différents comptes qui ont été touchés afin de disposer des dates des différents virements effectués. Généralement, ce sont plusieurs virements effectués à coup de 100 000 ou 500 000 €. Le but est de remonter jusqu'à ce que l'on appelle des « mules », un premier niveau d'auteurs, les premiers comptes rebonds de ces flux financiers. Une fois ces premières « mules » atteintes, nous sommes ensuite capables de remonter aux différents niveaux et d'attribuer l'attaque, en tout cas, aux donneurs d'ordres de l'attaque.

Mais d'autres cyberattaques existent et prennent de l'ampleur : le *jackpotting* et le *skimming*.

4.3/ Le jackpotting

Le *jackpotting* va toucher principalement les banques et les distributeurs automatiques de billets. Des pirates informatiques vont produire des briques-logicielles et les vendre à des groupes de pirates informatiques, d'escrocs en bandes organisées qui vont se rendre ensuite sur différents territoires européens.

Au chalumeau ou à la disqueuse, ils vont découper rapidement le DAB[26], se brancher sur ce dernier, exécuter une commande et *« jackpot »*. Pour eux, c'est la récupération d'un maximum de billets si l'attaque réussit.

[26] distributeur automatique de billets

4.4/ Le skimming

Une autre attaque tend à devenir de plus en plus commune : le *skimming.* Il s'agit d'un type d'attaque physique dans laquelle l'attaquant se positionne devant un distributeur automatique de billets ou devant une pompe à essence en y installant une fausse façade dotée d'un lecteur de piste magnétique et/ou d'une caméra. Ainsi, il récupère l'intégralité de vos données bancaires pendant que vous passez votre carte (informations figurant sur les pistes magnétiques et code de votre carte).

Suite à cela, plusieurs possibilités s'offrent au pirate : vendre vos données sur le *darknet* ou les utiliser directement à son avantage (pour régler le péage par exemple).

Ce qui prime, c'est donc toujours la vigilance. Sur ce volet prévention, il faut avoir conscience de l'omniprésence des cyberattaques et du risque qui existe. Nous sommes tous sujets à ces risques-là et il faut s'en prémunir à travers la prévention en ayant une bonne hygiène informatique et SSI. En outre, il est nécessaire de réagir rapidement concernant le volet judiciaire.

M. Philippe LAMBERT.- Merci. Effectivement, cela m'évoque deux ou trois choses. Le *social engineering*, également appelé OSINT[27]. On va aller chercher une information sur le net, vos informations. Pour moi, qui suis expert en justice, j'adore fouiller dans les téléphones, dans les disques durs des attaquants et des agresseurs, pour identifier pourquoi ils ont visé une victime et pas une autre.

Monsieur le Substitut général, vous évoquiez les rançongiciels, à savoir un virus la plupart du temps non ciblé.

Aujourd'hui, grâce à l'OSINT, nous arrivons à retirer l'information. Pour savoir comment se défendre contre nos attaquants, il convient donc d'apprendre à être comme eux. Nous investissons donc la société en lui faisant subir des tests d'intrusion, qui ne sont pas, comme vous l'avez mentionné Madame Delarue, une discipline de l'ANSSI. Ainsi, nous vérifierons la vulnérabilité de l'entreprise. Il existe également la possibilité de mettre en place des systèmes d'audit en intelligence artificielle – j'y reviendrai – pour prévenir ces menaces.

[27] Open-Source Intelligence

Je m’adresse à vous Monsieur Regond, en tant que chef d’entreprise et vice-président du Tribunal de commerce : comment voyez-vous la chose ?

5 La cybercriminalité vue par les chefs d'entreprises

Merci.

Je vais vous donner un angle de chef d'entreprise, qui va compléter ce qui a été dit jusqu'à maintenant, peut-être d'une façon un peu plus dramatique, parce que le chef d'entreprise va subir directement, sur son entreprise, et donc sur la pérennité de sa structure, ces risques-là.

J'ai un profil un peu particulier. Je ne suis pas un expert en cybersécurité, mais j'ai une entreprise qui travaille dans le domaine de la défense depuis plus de 20 ans. Je suis fondateur et vice-président d'un cluster appelé EDEN, qui regroupe une bonne partie des entreprises de la BITD[28] de la Région.

5.1/ Cyberdépendants

Nous sommes un peu tombés dans la cybersécurité dès le début, mais avec une approche très particulière, à tel point qu'à un moment donné l'approche extrême consistait à dire : « *vous avez un serveur, vous vous déconnectez d'Internet* ». Or, vous avez une machine pour aller sur ce serveur.

[28] Base Industrielle et Technologique de Défense

Forcément, au début cela peut fonctionner, mais très rapidement c'est complètement incompatible avec le développement d'une société et d'une société internationale.

De toute façon, nous sommes tous obligés maintenant de faire avec les outils que l'on nous propose. Ces outils sont d'une extrême efficacité, mais celle-ci engendre également un risque extrême qui doit être intégré.

Notre problématique réside dans le fait que nous n'avons pas forcément conscience du risque. Petit avantage : nous sommes majoritairement des *boomer*s, c'est-à-dire que nous avons assisté à l'évolution du numérique dans nos entreprises et nos activités. Le fait de voir ces évolutions nous donne peut-être un peu plus de recul par rapport aux jeunes qui sont nés là-dedans (dans les années 2000) et pour qui le numérique fait partie de la vie. Je le teste tous les jours, car j'ai deux filles qui sont concernées. La distance n'existe pas réellement. Parfois, l'esprit critique peut être un peu défaillant.

En tout état de cause, même nous, si nous avons conscience de certaines choses, il faut comprendre que notre survie passe par la nécessité d'avoir réellement conscience de ce que l'on fait. La problématique, nous le constatons, est la composante humaine. Le vrai risque ce n'est pas la machine en tant que telle, mais ce qui se passe entre le fauteuil et le clavier. C'est vrai que le risque repose essentiellement sur nous en tant qu'être humain.

J'ai une anecdote. Nous avons beaucoup de jeunes stagiaires en entreprise et ce matin j'ai fait une sensibilisation, notamment à l'utilisation de leur matériel personnel et à l'utilisation de nos matériels qui donnent accès à l'entreprise, un accès compartimenté. En fait, le matin même, à 1h30 du matin, j'ai reçu un e-mail d'un des stagiaires. Il était très bien fait, à l'adresse de son école, dans lequel il m'invitait à cliquer sur un lien. Cela était un peu louche, car c'était un lien *TikTok*. Évidemment, je n'ai pas cliqué. Quand le stagiaire est arrivé, je lui ai demandé si c'était un mail qu'il m'avait adressé, mais évidemment il m'a répondu non.

Cela va quand même très loin, car globalement nous pouvons nous demander s'il s'agit d'une tentative de *phishing* ou pas. Le risque dans le flot de nos activités est de cliquer. Il ne faut jamais cliquer quand on a un doute. C'est le vrai sujet. Du point de vue du quotidien, dans toutes nos activités, dès que quelque chose nous paraît anormal ou qu'une adresse e-mail ne nous semble pas conforme, il faut être attentif aux détails et ne pas tomber dans les pièges (par exemple, ajout d'une lettre). Même si l'e-mail est

extrêmement bien fait et que la plupart du temps les logos correspondent exactement, il faut être extrêmement attentif.

Je ne vais pas répéter tout ce qui a été dit d'une manière beaucoup plus parfaite que ce que je pourrais énoncer. En fait, nous sommes cyberdépendants. Globalement, nous ne pouvons plus avoir d'activités aussi bien à titre personnel qu'au niveau de nos entreprises sans le Net et sans nos systèmes d'information.

5.2/ La conservation des datas

La plupart du temps, ces systèmes-là ont un impact sur notre mode de fonctionnement. Si on n'a plus d'énergie, on n'a plus de Net et on ne fait plus rien. D'où la problématique liée à la conservation de nos datas et surtout à la remise en route de nos activités. Ce qui nous intéresse, en qualité de chef d'entreprise, c'est avant tout la continuité de l'exploitation. Elle passe par un certain nombre de choses, qui sont quand même très importantes au niveau de l'entreprise : la sauvegarde de nos données, une sauvegarde intelligente. En fait, le risque n'est pas qu'informatique. Il y a le risque d'incendie ou de vol. On doit avoir une sauvegarde qui doit être faite intelligemment au sein de notre site.

Éventuellement, des sauvegardes croisées entre différents sites ou une sauvegarde *via* un cloud sécurisé et validé par un centre serveur référencé. Nous en avons dans la Région.

Ce sont juste des principes de base et il faut être hyper humble par rapport à la mise en place de nos systèmes de sécurité informatique et ne pas hésiter à les remettre en question très souvent.

Nous avons la chance en Région d'avoir une structure appelée l'Espace Numérique Entreprise, qui est grandement supportée par la Région et qui donne accès à des possibilités de conseil et d'audit pour partie financées par la Région. Il ne faut pas hésiter à utiliser ces dispositifs qui permettent de faire très régulièrement un audit de situation de notre système d'information, voir si ce que l'on a fait est correct, si on prend des risques, et faire très fréquemment des mises à niveau.

Dans le domaine de la défense, nous avons la chance d'être suivis à la fois par la DGSI[29] et la DRSD[30]. Cela aide un peu. On fait des rappels/sensibilisations très régulièrement, tous les deux mois, en fonction des entrées de nos salariés. Ce sont des choses qui ont une valeur extrêmement importante. Mais il faut faire attention, car le naturel revient très vite et la facilité d'utilisation peut faire oublier le risque que l'on peut prendre.

5.3/ La partie dynamique de la menace

Concernant la partie dynamique de la menace, pour résumer ce qui a été fait, nous avons toujours constaté depuis très longtemps qu'il y a trois éléments : la motivation, la facilité d'accès et le sentiment d'impunité.

Le sentiment d'impunité : dans la mesure où la menace est internationale, on a ce sentiment d'impunité permanent. La communication sur les sanctions au niveau national est essentielle et importante. Il faut sanctionner, mais il faut communiquer sur la sanction. On le fait dans le cadre du cluster EDEN. Il est extrêmement important de savoir que derrière, à chaque agression, il y a potentiellement une sanction.

La motivation : nous l'avons énoncée tout à l'heure. Nous n'allons pas revenir dessus. Les motivations peuvent être d'ordre lucratif, de vengeance, etc.

La problématique de la facilité d'accès : c'est là où nous avons un rôle à jouer. Si nous laissons les portes ouvertes, c'est sûr qu'un jour on se fera voler, vidanger les données, etc. Il faut donc rester extrêmement vigilant.

Par rapport à ces éléments-là, il faut savoir qu'au Tribunal de commerce nous avons eu à connaître, et on connaît très régulièrement, des difficultés d'entreprises liées à ces agressions. Soit de la captation de datas, avec des dénis de service, soit un blocage pur et simple de sites Internet. Dans la mesure où beaucoup de sociétés sont dépendantes de leur site Internet, elles peuvent se retrouver en défaut de vente, d'une façon extrêmement rapide.

[29] Direction générale de la Sécurité intérieure
[30] Direction du renseignement et de la sécurité de la Défense

En outre, on a aussi beaucoup de sociétés dont le site Internet est activement lié à leur ERP[31]. Ce chaînage fait que la société peut se retrouver dans une situation de blocage total de son activité : impossibilité de recevoir ses commandes, de les préparer, de lancer des ordres de production et de livrer.

5.4/ Entreprise : que faire suite à une attaque

Premier point bien sûr, signaler très rapidement les faits. Comme déjà indiqué, il est vital de porter plainte le plus rapidement possible. 48 heures c'est vite passé.

Deuxième point, lorsque cela a un impact sur l'activité et sa pérennité, il ne faut pas hésiter à prendre rendez-vous auprès du Président du Tribunal de commerce.

Nous avons différentes possibilités en fonction de la gravité de la situation et de l'impact de cette agression sur la trésorerie de l'entreprise, notamment en regardant si la société prend un risque en termes de pérennité. En outre et au départ, mieux vaut rester extrêmement discret, voire secret, sur ce qui s'est passé parce que la première atteinte en matière commerciale est une atteinte à l'image et à la réputation.

Si la situation n'est pas trop grave, nous pouvons tout à fait ouvrir un mandat ad hoc ou une conciliation de façon à prendre le temps d'analyser, de mettre en place des mesures correctives, récupérer des données, afin que la reprise d'activité puisse être mise en place tout en négociant des délais avec les partenaires de l'entreprise. Cela permet en parallèle de traiter un certain nombre de problématiques et de demander des délais afin de sortir efficacement de ce mauvais pas.

Parfois il est déjà trop tard. Il y a deux ans nous avons eu un cas où l'impact a été tel sur une entreprise, qui par ailleurs était déjà un peu affaiblie, que le Tribunal de commerce a été obligé d'ouvrir une procédure de sauvegarde. Cependant cela n'est possible que si la structure n'est pas en état de cessation des paiements. Une procédure de redressement judiciaire permet également d'avoir un peu plus de temps et de trouver des solutions. Ces deux procédures restent malheureusement un peu plus lourdes.

[31] Un ERP (Enterprise Resource Planning) est un système de gestion intégré qui regroupe plusieurs applications pour gérer les activités opérationnelles et administratives d'une entreprise

5.5/ La data : enjeu de souveraineté

L'impact d'une attaque n'est pas neutre. Le mot-clé par rapport à cela est la rapidité de la réaction. Il faut réagir le plus rapidement possible. Je dirais presque dans l'heure, car la priorité absolue est de sauvegarder son entreprise, essayer de récupérer ses données, ce qui n'est pas évident car, face à un *ransomware*, on est tenté de payer. Or, la plupart du temps, payer ne mène à rien. Il vaut donc mieux éviter de payer et plutôt compter sur ce qui est mis en place. D'où l'importance fondamentale de ces systèmes de sauvegarde, des procédures de protection et de restauration des données en interne afin de pouvoir relancer son activité.

Au sein de notre entreprise, nous avons des systèmes de protection croisés entre différents sites. En cas de disparition totale de nos datas sur un site, nous sommes capables dans l'heure de continuer sur la base de ce qui existe sur un autre site. Or, nous pouvons tous nous organiser de cette façon. C'est juste fondamental et essentiel.

Les assurances vont être de plus en plus vigilantes sur ces aspects-là. Si on n'a pas mis en place ces mesures minimales, cela deviendra une cause de non-couverture d'assurance. Je suis dans le domaine de l'aéronautique et, depuis quelques années, dans certaines professions, nous avons mis en place un protocole appelé AIR Cyber qui permet, un peu en anticipation par rapport à la législation européenne, de valider que dans toute la chaîne, du sous-traitant de dernier rang jusqu'au donneur d'ordre, toutes les mesures en termes de cybersécurité sont mises en place. Il y a vraiment des choses à faire. La rapidité, là encore, est le mot-clé.

Il y a une autre chose : ne pas oublier les principes de base de la résistance. On ne va pas trop en parler, mais parfois les approches sont insuffisantes. C'est un peu mon « dada », mais c'est important. La data est devenue un enjeu de souveraineté. Or, nous avons quand même de vrais soucis en Europe, et en France en particulier, par rapport à cela parce que nous avons perdu la guerre de la data. Nous devenons dépendants de la donnée et nous avons parfois du mal à réagir face à cette problématique.

Un exemple : le CLOUD Act américain[32]. La législation aux États-Unis permet au global, de façon assez simple, à n'importe quel procureur américain de solliciter la transmission

[32] Entré en vigueur le 3 octobre 2022, le Cloud Act va officiellement permettre aux États-Unis et au Royaume-Uni de « *lutter contre les crimes graves, notamment le terrorisme, la maltraitance des enfants et la cybercriminalité* »

d'informations de toute société où qu'elle se trouve sur la planète pour autant qu'une société américaine ait un intérêt capitalistique dans la société détentrice de la data. C'est quand même gravissime dans la mesure où les États-Unis se trouvent donc en position quasiment dominante en termes de logiciels, ce qui impacte beaucoup de choses.

Une petite anecdote. Nous utilisons un logiciel de modélisation numérique de flux très fréquemment utilisé dans l'aéronautique et qui est excellent. Ce logiciel, ni français ni européen, a été développé en Grande-Bretagne et a été racheté par une société américaine quasiment en situation de monopole. Or, la démarche commerciale qui a été mise en place par les Américains est très bonne, consistant à le fournir gratuitement à tous les chercheurs de toutes les universités sur la planète. Les personnes qui travaillent dans la modélisation doivent savoir de quoi je parle. Ce logiciel, dont le nom commence par un A, est en fait un vrai mouchard.

Nous avons découvert ce logiciel de manière accidentelle. En effet, un jeune docteur travaillant dans notre structure l'utilisait dans le cadre de son doctorat et l'a « malencontreusement » installé sur l'une de nos machines. Étant très légaliste et en parallèle, j'ai acheté ce logiciel 125 000 € pour une licence pluriannuelle, avec 25 000 € de maintenance annuelle. Or, j'ai reçu une lettre de cette structure par le lawyer américain, qui m'indiquait qu'ils avaient détecté l'utilisation d'un logiciel non déclaré.

Allant un peu plus loin, nous nous sommes aperçus que non seulement ils avaient la capacité de savoir quand la licence avait été utilisée, mais comment elle avait été utilisée et quelles datas avaient été fournies. Ils avaient donc connaissance de l'intégralité des datas. À chaque fois que nous réalisons un calcul, y compris sur un logiciel que nous avions payé, toutes les datas étaient récupérées par cette structure.

C'est un peu le contre-exemple : *« Quand c'est gratuit, c'est toi le produit »*. Là, c'est très payant, mais c'est quand même toi le produit. Il faut en être conscient. Il y a plein de choses à faire par rapport à cela, mais il faut être conscient de cette problématique.

Malheureusement, elle touche beaucoup de sociétés. Nous sommes réellement dans une guerre de la data internationale entre deux blocs principaux : les Américains et le reste du monde. En ce moment, le reste du monde, ce sont les Russes et les Chinois. Nous, les Européens, nous avons quasiment perdu cette guerre.

Face à cela, dans la mesure où il existe des intérêts américains sur des structures françaises, y compris des structures que l'on connaît tous ici, nous prenons un risque de fuite de datas. C'est quasiment imparable, si ce n'est qu'il faut le savoir. Quand on possède des données très sensibles, il faut éviter par exemple d'utiliser *WhatsApp*. C'est une question de choix. Mais pour avoir le choix il faut en avoir conscience.

Pour les Chinois c'est pareil, notamment avec *TikTok*. Ce matin, j'ai un peu réprimandé tout le monde, notamment les jeunes stagiaires qui arrivent chez nous, car l'utilisation de *TikTok* est quasiment automatique avec des photos. Or, chez nous, il est interdit de prendre des photos. Il faut avoir conscience de cette réalité-là, car, malheureusement, nous ne sommes pas dans un monde de « Bisounours ». Nous sommes potentiellement en guerre numérique depuis plusieurs années. Sans être trop négatif ou anxiogène, je pense que le fait d'avoir conscience de cela nous permet de lutter de manière efficace, au-delà d'ailleurs de ce que l'on peut faire très clairement au Tribunal de commerce. C'est aussi notre rôle d'insister là-dessus.

Après, avec Avisa Partners, ce qui s'est passé est très compliqué. C'est en cours. Regardez dans la presse ce que l'on en dit. C'est assez intéressant. Là, on dépasse un peu la cybersécurité en tant que telle. On est sur la problématique de l'intelligence économique où nous avons pris pas mal de retard ces dernières années, mais avec des personnes comme Alain Juillet[33] on a beaucoup évolué.

Voilà ce que je voulais dire à ce stade. Merci.

[33] Alain Juillet, président du Club des directeurs de sécurité des entreprises, fut directeur du renseignement de la DGSE entre 2002 et 2003, puis responsable de la cellule intelligence économique à Matignon jusqu'en 2009

6 Débat

M. Philippe LAMBERT.- Merci Monsieur Regond.

Pour ma part, pour ouvrir le débat, je vais évoquer des anecdotes par rapport à ce que vous avez mentionné.

Ma première expertise est en fait un cas d'urgence d'une société qui fabriquait des meubles. Elle avait un souci avec les robots de l'usine : ils ne faisaient plus d'assemblage, ils jouaient au *frisbee* avec une plaque de meuble. En allant visiter le bureau de l'informaticien, qui avait été licencié, j'ai constaté qu'il n'y avait plus de sauvegarde, que son ordinateur était crypté et que les robots avaient été déprogrammés.

Effectivement, l'expertise a été très vite puisque l'identification de la personne a été rapidement réalisée.

Autre anecdote. Vous parlez, Monsieur le Substitut général, d'attaques *via* Internet. J'ai une double casquette, je suis aussi enseignant en cybercriminalité et en cybersécurité. Je forme les cybercriminels de demain, mais plutôt dans la partie défense. Je leur ai dit un jour que j'allais leur montrer ce qu'ils n'entendaient pas. En fait, ce qui me fait sourire c'est lorsque sur LinkedIn des gens disent : *« Regardez, il a laissé son ordinateur ouvert dans le train. Il a laissé son téléphone. On pourrait lui prendre et capturer ses données »*. Je vais vous montrer que l'on peut écouter votre écran et lire ce qu'il y a dessus. C'est aussi simple que cela.

Par exemple, quand nous avons préparé notre conférence, je parlais d'une société « X » qui travaillait avec la société de mon frère et qui fabriquait des exosquelettes à destination des personnes paralysées afin de leur permettre de marcher. En fait, cette société était observée par un autre État qui voulait s'emparer des exosquelettes pour renforcer les armures militaires de ses soldats. Ainsi, il serait possible d'injecter un antalgique aux soldats qui pourraient ensuite rentrer à la base grâce au GPS intégré dans l'exosquelette. Ce sont des plans de recherche. X n'existe plus. Vous pouvez la chercher sur Internet puisqu'elle a été reprise par le ministère de la Défense.

Maintenant, je pose la question ouverte : quelles sont aujourd'hui les recherches qui sont réalisées dans le domaine de l'IA ? Quelles sont les nouveautés ? Nous avons parlé de la France qui est un peu en retard. Mais il faut informer et aussi se tester par rapport à tout cela. Où en est-on par rapport à ces évolutions ? Est-ce suivi ? Y a-t-il des réalisations à faire ? Des concepts sont-ils mis en place ? J'ouvre le débat.

M. Thierry REGOND.- La problématique est que l'on a toujours un temps de retard et qu'on l'aura de plus en plus. Ce que l'on va observer ne sera pas forcément la réalité. La problématique est que l'on peut tout à fait avoir du recul et un œil critique, mais on risque d'être surpris par la sophistication des futures attaques : vraie voix du chef d'entreprise, vraies intonations, voire même une vidéo le représentant lui-même. C'est quelque chose qui peut devenir dramatique. C'est très compliqué de lutter contre cela.

Nous y avons déjà réfléchi chez nous et on peut lutter contre cela par des procédures. Nous avons eu deux tentatives de détournement en passant par notre standardiste. On a notamment des procédures de paiement qui sont obligatoires. Comme en matière nucléaire pour l'Armée, on passe par une procédure qui ne peut pas être modifiée. Au global, cela nous a sauvé deux fois de suite.

Je pense que l'avenir est aux procédures qu'il faut mettre en place, dans un premier temps . Mais ensuite, il faudra être vigilant car les procédures pourront éventuellement être détournées. C'est l'option que nous avons décidé de mettre sur la table récemment.

M. Philippe LAMBERT.- Merci Monsieur Regond. Maître Moussa, on évoquait tout à l'heure des idées.

Me Olivier MOUSSA.- Vous avez indiqué que les algorithmes sont entraînés sur des *datasets*[34].

Une des attaques difficiles à déjouer et à laquelle on assiste désormais ne consiste pas à s'en prendre directement à l'entreprise qui met au point l'algorithme, mais à essayer de corrompre le jeu de données sur lequel l'algorithme va être entraîné.

C'est assez radical, à partir du moment où vous corrompez la donnée, nécessairement elle va infecter le fonctionnement. Ce type d'attaque en est à ses débuts.

Pour aller sur un aspect plus réglementaire, il y a en effet une source de responsabilité. C'est l'autre volet : les dégâts causés par l'IA. Sans aller trop dans le détail, car ce serait fastidieux, un règlement a été mis en place pour essayer de réglementer en scindant différents types d'IA. D'autres réglementations concernaient les plateformes qui mettent en œuvre des algorithmes tous utilisateurs. Les plus grandes d'entre elles seront soumises à des obligations, comme la transparence et notamment celle concernant les algorithmes sur les critères de recommandations.

Une réglementation qui sera nécessairement multiforme face à ce que vous décriviez, Monsieur le Président, à savoir le caractère également multiforme de l'utilisation des outils. Je crains que l'on se dirige vers une réglementation qui consistera à avoir des outils dédiés : à chaque outil sa réglementation.

Cependant, lorsqu'il s'agit de philosophie commune, nous constatons que nos clients rechignent à la mettre en œuvre, comme dans le cas du RGPD. Pourtant, en tant que conseil, nous pensions que c'était l'occasion de s'occuper de ces sujets et qu'en s'occupant des données personnelles nous pourrions également aborder les questions de sécurité et de l'habitude de considérer qu'il s'agit d'un sujet en soi. Commencer à s'en occuper, c'est comme aller chez le dentiste, quand on commence à se brosser les dents, on évite beaucoup de problèmes. Donc, aborder la question, c'est faire un grand pas vers la sécurité.

[34] Les datasets (ou jeux de données) sont couramment utilisés en machine learning. Ils regroupent un ensemble de données cohérentes qui peuvent se présenter sous différents formats (textes, chiffres, images, vidéos etc.)

M. Philippe LAMBERT.- Merci Maître. Vous parliez du RGPD. Or, à l'heure actuelle, il a été constaté que si l'on accepte aisément les conditions de ce RGPD, dans les faits on ne les lit même pas. C'est l'automatisme du cliquage comme disaient les chercheurs du CNRS. Il y a donc là un enjeu sur l'avenir du RGPD.

En tant que DPO[35], je lisais avec un grand intérêt que la donnée est sécurisée, mais qu'elle peut être utilisée anonymement. Si on ne la définit pas, on arrive à l'utiliser pour faire une prédiction, comme Madame Irma dans sa boule de cristal, de ce que vous allez acheter demain et de ce que vous allez faire.

J'ai répondu cette nuit à un formulaire de l'IESF[36]. Des questions m'ont été posées et je me suis aperçu qu'en y répondant, si cet institut effectuait un recoupement de ces questions, il saurait qui je suis. Bien sûr, j'ai accepté les conditions du RGPD, mais avec un peu de jugeote on constate aisément que ces données peuvent être utilisées.

Dans le cadre de cette remontée d'informations, effectivement, Google est un service gratuit. Cependant, comme vous l'avez mentionné, la gratuité n'existant pas, les concepteurs de ce moteur de recherche ont fait des données une monnaie d'échange. Cette valorisation de la donnée est ce que l'on appelle le « second marché ». Il existe cependant des opérateurs dits du « troisième marché », comme Google, Facebook et autres plateformes, qui vont échanger ces données contre du numéraire. Pierre, vous évoquiez le domaine médical. Effectivement, il existe maintenant des plateformes spécialisées dans la donnée médicale. J'ai cherché également sur *Family Search* qui était mon ancestral grand-père de la cinquième génération de la dynastie. Je ne l'ai pas trouvé. En revanche, il s'est avéré que grâce aux données de l'ADN, on arrive aujourd'hui à prédéfinir que je peux avoir du cholestérol, si ce n'est déjà fait, d'ici quelques années.

L'enjeu réside aujourd'hui dans cette masse d'informations qui ne cesse de s'accroître. Or, ce qui m'inquiète c'est de savoir si la jeunesse qui utilise aujourd'hui tous les produits informatiques est consciente de ce qui se cache derrière eux. Quand j'enseigne, je me dis qu'ils font cela avec leur ordinateur, leur téléphone, et je suis relativement surpris. Dans les juridictions, constatez-vous cette insouciance du jeune d'aujourd'hui qui utilise la donnée ou le sujet informatique comme s'il était impunément protégé derrière son écran ?

[35] Délégué à la protection des données : personne chargée de la protection des données personnelles au sein d'une organisation.
[36] Institut des Ingénieurs et Scientifiques de France

M. Thibaud MÉRIEN.- Effectivement, on se rend compte qu'il y a ce sentiment d'impunité et que les jeunes sont très peu au fait du partage d'informations. Pour cela, il suffit de constater ce qui se passe sur les réseaux sociaux : multitude d'informations laissées au vu et au su de tous, autant de portes ouvertes au cyberharcèlement, voire pire. J'ai eu l'occasion de faire des enquêtes sous pseudonyme (ESP) et on se rend compte que très vite, sur n'importe quel forum, on peut être abordé par un pédophile et obtenir un rendez-vous très rapidement. Effectivement, nous traitons donc beaucoup de dossiers dans lesquels les jeunes n'ont pas conscience à quel point ils s'exposent quand ils sont sur Internet.

Comme vous et pendant mon doctorat, j'ai eu l'occasion d'être professeur à l'École navale, école associée à la Marine nationale. Bien qu'ils soient officiers, qu'ils aient fait des Prépas et qu'ils aient passé des concours particulièrement compliqués, les aspirants utilisaient constamment leur téléphone pour prendre des photos, pour filmer ou encore échanger des données, données qui relevaient parfois d'un caractère militaire.

Or, l'informatique et tout ce que nous transmettons à travers ces photos laisse des empreintes, ne serait-ce que d'utiliser son navigateur. Il existe d'ailleurs un site appelé « À maille unique », qui permet d'identifier si votre navigateur laisse une empreinte unique, à l'image de notre ADN. En fonction de la version du navigateur, de la machine, de tout ce que vous avez sur votre ordinateur, on est capable de définir une empreinte unique qui vous identifie.

Vous parliez tout à l'heure des sites pour définir qui sont vos ancêtres, etc. Quand on laisse des traces d'ADN, on peut maintenant les utiliser avec les Américains pour obtenir des résultats sur des personnes. L'informatique laisse des traces partout et les jeunes n'en ont pas conscience.

M. Romain DUCROCQ.- Justement, c'est aussi cela l'intérêt au niveau pénal. C'est un outil informatique à double tranchant. Pour la victime, cela l'expose pleinement, mais vous avez aussi des cas, non moins populaires, d'auteurs qui se servent de ces réseaux-là et qui permettent l'identification. Très concrètement, le conseil qui peut être donné est de diffuser le moins possible des informations personnelles en tant qu'honnête citoyen et que les délinquants continuent de faire ce qu'ils font avec l'outil informatique.

Effectivement, lorsque l'on voit des photos sur les sites Internet, on évoque des messageries instantanées, prétendûment totalement cryptées. En réalité et comme chacun le sait, cela est totalement faux, les délinquants trouvant toujours une « porte d'entrée ».

Un exemple assez connu : même les messageries instantanées ont un historique, qui est consultable par Internet et assez facilement identifiable. Ce qui est intéressant concernant cette technologie, c'est cette certaine insouciance des jeunes dans l'utilisation de ces outils qui, dans le même temps, peuvent servir aux délinquants.

M. Thibaud MÉRIEN.- Pour illustrer les échanges et les traces qu'on laisse sur Internet, en travaillant pour la Marine nationale à l'époque, je me suis intéressé aux informations que l'on pouvait tirer de la simple lecture d'une bande patronymique d'un militaire qui comportait l'écusson d'un sous-marin.

À partir de là, je regarde son profil *Facebook*, sur lequel on peut voir ses amis. La majorité des profils sont publics, sauf qu'aucune information n'est postée sur le fait qu'ils soient militaires et sur le fait qu'ils embarquent sur des sous-marins. Cependant, à certains moments, ils vont poster sur *Facebook* ou pas du tout. À partir de là, il est donc possible de déduire, par exemple, à quel moment un sous-marin avec ces personnes-là est en mer, si elles appartiennent à l'équipe bleue ou à l'équipe rouge. Il est également possible d'obtenir des informations concernant leur femme, leur famille, et d'avoir un moyen de pression sur le militaire par le biais de sa femme ou de ses enfants pour extorquer des informations.

Tout ce que vous laissez sur Internet laisse des traces et peut avoir un impact sur votre sécurité, sur celles de vos enfants, sur votre emploi. Tout laisse des traces. La majorité des attaques par FOVI se fait avec une grosse phase de *social engineering* en amont. Et avec cette phase d'OSINT, on est capable de connaître toute la vie d'une personne et de l'approcher par certains leviers très puissants pour pouvoir obtenir les informations que l'on souhaite et mener à bien par la suite l'attaque informatique. La première faille est donc, à mon sens, l'humain.

M. Romain DUCROCQ.- Concernant les *ransomwares*, vous avez indiqué qu'il ne fallait pas payer la rançon, mais il y a un autre critère qui n'est pas forcément abordé : vous, vous avez le sentiment d'être débarrassé. En fait, vous n'êtes pas du tout débarrassé du virus et votre ordinateur peut servir pour d'autres attaques. Vous-même, vous pouvez être approché et embêté parce que votre ordinateur va servir pour commettre d'autres infractions. Il va servir de miroir, de tampon, pour faire des attaques de plus en plus importantes. Vous allez vous-même être embêté. Vous allez aussi nourrir les différents réseaux mafieux. Il ne faut surtout pas payer la rançon pour cette raison-là. Votre logiciel continuera d'exister.

M. Philippe LAMBERT.- Je tiens à souligner que moi aussi j'ai eu affaire à l'ANSSI, qui avait fait un très bel audit de sécurité pour une municipalité qui voulait se prémunir d'une attaque. Effectivement, en France, on a la chance d'avoir des organes d'État, qui ont des experts : la gendarmerie, la justice. Je suis juge et partie puisque je suis expert de justice. On a des entités dépendantes et indépendantes, qui vont mener à bien les conseils. Je vous conseille le MOOC SecNumAcadémie de l'ANSSI, qui est très bien. Je le conseille aussi à mes élèves. Il est très rationnel.

Maintenant, je vais vous passer le micro pour les questions à nos intervenants. N'hésitez pas. Ils sont là pour vous répondre.

7 Questions / réponses

M. Jean-Paul GRANADOS, expert de justice.- Vous dites de ne pas payer, mais comment faire quand on ne possède pas de sauvegarde ? Comment sort-on de cette situation ?

M. Romain DUCROCQ.- Le but de cette conférence est d'avoir des moyens de prévention. En fait, quand vous payez, vous avez une solution totalement précaire. Certes, vous récupérez un certain nombre de vos données pendant un certain temps, mais derrière, l'attaque reviendra et vous ne serez pas débarrassé. Vous allez avoir la satisfaction d'avoir payé 800 € pour être tranquille. En général, ce n'est pas très cher au départ, puis après cela va augmenter.

M. GRANADOS.- Je pars du principe que l'on ne paye pas. L'entreprise va tourner. Comment faut-il réagir ?

M. Romain DUCROCQ.- Il y a d'autres solutions. Pour la cybersécurité, il existe des sociétés privées qui peuvent vous aider à récupérer la donnée, mais c'est un autre domaine d'expertise.

Mme Marianne DELARUE.- Quelques solutions existent. Souvent une attaque survient un samedi à minuit, la veille de Noël, quand il y a moins de personnes dans l'entreprise. Si on découvre le lundi matin qu'un poste a été infecté, la première recommandation est de demander à tout le monde de ne pas allumer son ordinateur. On laisse quand même tourner le poste infecté, mais on n'y touche pas. Cela va permettre l'investigation. On déconnecte toutes les machines qui n'étaient pas identifiées comme connectées à cette partie-là. Il faut les déconnecter pour les laisser saines.

Ce sont les premières mesures. Ensuite, il faut faire appel à un prestataire informatique. Dans certains cas, ils arrivent à récupérer les données. Des sociétés sont spécialisées dans la récupération de données. Je ne peux pas les citer, car elles ne sont pas labellisées par l'ANSSI, mais elles existent. Parfois, ce n'est pas l'intégralité des données qui sont infectées, mais seulement une partie.

M. Olivier FAVELIN, Juge chargé du contrôle des expertise au Tribunal de commerce de Grenoble.- Une remarque et une ou deux questions. La première remarque est de ne pas oublier dans les mesures de prévention de tester les sauvegardes. On a déjà constaté que le système d'exploitation avait changé entre la dernière sauvegarde et la nouvelle et que l'on n'arrivait plus à la remonter.

Première question : vous insistez sur le fait qu'il faut déposer plainte dans les 72 heures. Quel est l'intérêt de faire ce dépôt de plainte ? J'aimerais vous entendre à nouveau à ce sujet. Est-ce pour se protéger d'une éventuelle amende ? Est-ce pour les assurances ?

Deuxième question : vous nous dites intervenir, mais quel est votre interfaçage avec les assureurs et leurs prestataires dès lors que l'on arrive à souscrire des contrats ? Il y a encore quelques compagnies qui sont prêtes à souscrire et à prendre ce risque-là ?

M. Thibaud MÉRIEN.- Effectivement, on vous demande d'intervenir rapidement. Il y a certes un volet assurances, mais ce qui va vous intéresser dans un premier temps c'est le volet financier. C'est une bonne chose effectivement, mais si vous voulez des résultats derrière il faut que le dépôt de plainte soit rapide pour éviter une suppression des données. Pas mal de virus se suppriment d'eux-mêmes au bout d'un certain temps. Une fois que l'argent est parti, au bout de ces 48 heures, il est beaucoup plus difficile de faire le *recall*. Quand l'argent a déjà effectué trois ou quatre rebonds, on ne peut plus le récupérer. D'où la rapidité. Le dépôt de plainte est essentiel.

Récemment, sur un dossier, nous avons réussi à récupérer une très forte somme d'argent. Si la personne n'avait pas déposé plainte, on n'aurait pas pu rentrer dans le cadre d'une procédure pénale et reprendre cet argent.

Nous sommes obligés d'être dans le cadre d'une enquête pour pouvoir récupérer vos fonds. Plus vous laissez traîner, plus les fonds seront déjà partis et nous ne pourrons plus récupérer votre argent.

M. FAVELIN.- La deuxième partie : à partir du moment où on arrive à souscrire un contrat, dans le contrat d'assurance, il y a toujours une partie intervention et un prestataire qui est mis à disposition pour débloquer, si ce n'est pas les services de la compagnie. Comment interfacez-vous avec ces services-là ? On met en avant le fait que ces compagnies prennent la main sur le système, mais comment travaillez-vous avec elles ?

M. Romain DUCROCQ.- Vous évoquez peut-être les personnes qui interviennent pour rétablir rapidement le fonctionnement du système ?

M. FAVELIN.- Oui. Ce ne sont pas forcément les prestataires actuels de l'entreprise qui a été hackée. Il y a d'autres prestataires extérieurs.

M. Thibaud MÉRIEN.- Bien sûr. On travaille avec eux parce que nous récupérons beaucoup d'informations. Les experts de justice ont des outils qui permettent d'extraire très rapidement des informations. S'ils peuvent le faire à notre place, pour nous c'est du temps gagné sur la phase d'enquête. En tant que force de l'ordre, on n'interviendra pas du tout sur le volet assurances.

M. Romain DUCROCQ.- Sur l'aspect plainte, en réalité, il y a plusieurs leviers, en termes purement stratégiques qui vous concernent moins. Il faut avoir des informations. Si vous ne déposez pas plainte, les services d'enquête et de prévention n'auront pas l'information. Quand vous vous faites pirater et que vous subissez un rançongiciel, il y a une signature assez typique. Cela permet après, par recoupement, de déclencher d'autres enquêtes et de trouver d'autres victimes. C'est un point plus macro.

Personnellement, pour vous, il y a deux leviers. La loi vous oblige de plus en plus à déposer plainte, sinon vous n'êtes pas indemnisés. Des banques subordonnent le *recall* au dépôt de plainte.

Dernier point, lorsque vous allez déposer plainte le plus précocement possible, vous allez maximiser deux choses : premièrement, récupérer votre argent. Deuxièmement, et cela peut avoir un intérêt, identifier l'auteur.

M. Philippe LAMBERT.- Effectivement, de la même manière que le pirate collecte des informations pour identifier sa victime ou l'attaquer, les services judiciaires ont besoin d'informations pour identifier l'attaquant. Plus il y aura d'informations, plus on identifiera des profils comportementaux d'attaquants qui nous permettront d'arrêter la menace. C'est une réalité. Si on ne dépose pas plainte et que l'on se débrouille seul, cette information est manquante.

Maître Luc CHAUPLANNAZ, avocat au Barreau de Lyon.- C'est une question extrêmement pratique : que ce soit une entreprise ou un particulier qui subit une cyberattaque, à quel service de police, commissariat ou gendarmerie faut-il s'adresser ? Y a-t-il des services spécialisés dans la métropole de Lyon ou le commissariat du siège de l'entreprise ou du domicile est-il seul compétent ?

M. Thibaud MÉRIEN.- Il faut avoir porté plainte le plus rapidement possible, que ce soit dans un commissariat de police ou une brigade de gendarmerie. Des canevas d'audition sont déjà prédéfinis pour que votre plainte soit prise le plus rapidement possible, avec le maximum d'informations.

Ensuite, les premières évaluations vont être effectuées. Plus le dossier sera complexe, plus il va monter auprès de services spécialisés. Les *ransomwares* sont des thématiques appelées des ASTAD[37]. Elles sont considérées comme très complexes, étant un enjeu majeur. Même s'il n'y a pas de préjudice et que c'est l'ordinateur d'un particulier qui est touché, ces dossiers-là seront systématiquement remontés à notre section de recherche pour avoir le maximum d'informations. Plus les pirates vont réaliser d'attaques, plus ils vont laisser de traces et plus nous serons capables de comprendre leur manœuvre et leur fonctionnement et plus nous pourrons remonter à eux.

[37] Atteintes aux Systèmes de Traitement Automatisé de Données

Peu importe où vous irez porter plainte, la notion de guichet unique a été évoquée tout à l'heure, les personnes sont obligées de prendre votre plainte. Ensuite, elle est attribuée en fonction des premiers éléments à un service spécialisé selon la complexité de l'attaque.

Me Marie-Josèphe LAURENT, Bâtonnier du Barreau de Lyon.- Je confirme que déposer plainte est très efficace dans certains cas. Nous l'avons fait avec un client. Les services de police ou de gendarmerie qui se sont occupés du dossier ont bloqué une partie des fonds sur la banque.

Maintenant la procédure pénale est en cours. Je crois que les « malfaiteurs » sont partis et ont pris leurs jambes à leur cou. Comment faire pour faire débloquer les fonds au profit de mon client s'il n'y a pas de procédure pénale ? Ce serait merveilleux si je pouvais récupérer les 150 000 € sur les 200 000 € qui ont été détournés.

M. Thibaud MÉRIEN.- Les fonds ont été bloqués sur un compte de l'AGRASC ?

Me LAURENT.- Justement, je ne sais pas où est passé l'argent. Il a été bloqué sur le compte bancaire sur lequel mon client a envoyé les fonds par erreur. Ces fonds se trouvent dans une banque X, qui est tout à fait connue. Je sais que les 150 000 € sont bloqués. Il me semble que la procédure pénale est en train de suivre son cours. Ce dossier est suivi à Valence. Je ne suis pas sûre que cela puisse maintenant avancer beaucoup. Non pas que j'en fasse le grief aux services de Valence, mais je pense que les attaquants se sont évaporés dans la nature. Ce dossier risque de durer un certain temps. J'aimerais bien récupérer les 150 000 € pour mon client, qui lui font cruellement défaut.

M. Thibaud MÉRIEN.- J'imagine et je comprends tout à fait que les 150 000 € représentent une certaine somme pour votre client. Il y a deux choses.

Dans un premier temps, les comptes peuvent être gelés. L'argent est bloqué sur un compte et plus aucun mouvement bancaire ni aucune transaction ne peuvent être faits.

Il y a aussi le *recall*, dont on parlait tout à l'heure. À ce moment-là, la transaction est systématiquement annulée. Là, la transaction ayant été réalisée et le premier compte rebond ayant été identifié, les fonds sont d'abord gelés pour ensuite être rapatriés une fois que l'on considère que la transaction est bien frauduleuse.

Je pense que quelques investigations sont encore à réaliser dans le cadre de l'enquête, que je ne connais pas du tout, pour pouvoir confirmer également la manœuvre frauduleuse et rapatrier les fonds sur le compte de la victime. Les demandes de *recall* sont souvent faites sur des comptes de l'AGRASC, qui gèrent les avoirs criminels pour qu'ils puissent être remis à la victime.

Me LAURENT.- Excusez-moi, car je donne l'impression d'avoir une consultation individuelle, mais comment puis-je savoir que l'argent de la banque X est parti à l'AGRASC ?

M. Romain DUCROCQ.- Cela vous est normalement notifié. Il y a deux cas de saisie. Le premier est une saisie bancaire, type *recall*, où la personne a informé sa banque. La seconde est plus complexe, lorsque l'on a une procédure pénale en cours avec une procédure de saisie et nécessité d'identifier l'origine des fonds. Le cas échéant la procédure est engagée pour obtenir la récupération des fonds.

Me LAURENT.- Je suis avocate.

M. Romain DUCROCQ.- Donc vous connaissez. Il y a les deux systèmes. Il faut voir à quel titre vous avez été saisie.

Me LAURENT.- Je vais poursuivre mon enquête.

Mme Cathy SCHMERBER, Première vice-présidente du Tribunal administratif de Lyon.- Une question beaucoup moins pratique. Je crois que la cybercriminalité n'a pas vraiment de frontière. Le Conseil de l'Europe s'en souciait déjà il y a 15 ou 20 ans. Où en est la coopération internationale aussi bien en prévention qu'en répression. Est-ce que l'on avance ?

M. Romain DUCROCQ.- Je suis passé un peu rapidement. En réalité, il y a la coopération européenne et internationale qui est en projet et la convention de Budapest. Ce sont des chantiers. Contrairement à ce qui est indiqué dans le deuxième protocole, les Américains récupèrent beaucoup d'éléments et de preuves. De notre côté, c'est plus compliqué. C'est une coopération Europe – États-Unis.

Au niveau du système européen, on a plusieurs mécanismes. Le plus important et le plus connu est e-Evidence[38], qui vise à fluidifier et à accélérer les procédures de coopération internationales.

C'est un sujet. Son évolution est récente. Cela existe et se fait. Les derniers travaux en la matière : le but est d'arriver, en fonction de l'importance de la demande et de la sensibilité du dossier, à une réponse en 72 heures en cas d'urgence.

Me Thierry DUMOULIN, avocat au barreau de Lyon.- Pour apporter un complément à l'inquiétude de mon confrère Chauplannaz, je rappelle que l'article 15 du Code de procédure pénale fait obligation à tout service de police ou de gendarmerie, même incompétent territorialement, de recevoir la plainte de toute personne qui se présente. Si vous êtes victime d'une cyberattaque, même si vous êtes dans l'Ain à Jujurieux, vous pouvez vous présenter à la brigade de gendarmerie. Voilà de manière très pratique, les possibilités qui vous sont offertes.

M. Philippe LAMBERT.- Merci. Une dernière question ?

M. GRANADOS.- Je rebondis sur ce qui a été dit sur les banques. Personnellement, j'ai été victime d'une attaque.

Dans les faits, plusieurs virements avaient été réalisés sur un compte en France. Le banquier a trouvé cela anormal et a alerté les autres banquiers, dont le nôtre, qui nous a appelés afin de nous prévenir qu'un virement frauduleux de 10 000 € avait été émis depuis notre compte et qu'il fallait porter plainte.

C'est ainsi que nous avons pu récupérer au bout d'un mois et demi 9 600 € sur les 10 000 €, notre propre banque nous ayant versé les 400 € complémentaires dans le cadre de notre assurance.

Les banques ont donc un rôle très important à jouer dans ce domaine.

[38] Le règlement relatif aux preuves électroniques (*e-Evidence*) vise à faciliter les enquêtes criminelles transfrontalières en mettant en place un mécanisme de coopération permettant aux forces de police européennes d'obtenir des preuves stockées sous forme électronique par un fournisseur de services tel qu'un service de messagerie ou de courrier électronique basé dans un autre État membre de l'UE (Accord du 29/11/2022)

M. Thibaud MÉRIEN.- Effectivement, cela va dépendre de votre banque. Elle est censée analyser certaines transactions et certains flux. Comme je le disais pour les FOVI, le premier réflexe est de contacter immédiatement votre banque afin d'effectuer le *recall*.

Le *recall* est à l'initiative de la banque. La transaction se faisant en plusieurs temps, même au bout d'un ou deux jours, la transaction va être initiée, mais les fonds ne seront pas systématiquement envoyés. C'est sûrement ce type de procédure.

Il y a l'autre cas où les fonds sont déjà sur le compte de l'escroc. Ils sont gelés et ils vont être rapatriés *via* la procédure judiciaire sur le compte de l'AGRASC pour les récupérer ensuite. Les banques jouent évidemment un rôle essentiel dans la récupération des fonds. C'est pourquoi il faut avoir une réactivité immédiate et de bonnes relations avec son banquier afin qu'il vous contacte rapidement.

M. Philippe LAMBERT.- Merci. Je reviens sur la coopération internationale. À travers mon profil d'expert de justice, j'ai été formé par un institut français qui cache derrière lui un institut de renseignement américain, notamment pour la formation et l'expression de données numériques sur les téléphones.

Très récemment, on a parlé de cybercriminalité. Aujourd'hui, notre ami Google a mis en place un système de repérages par rapport au champ lexical utilisé par le profilage des criminels. Quand un mot est saisi plusieurs fois, il alerte le renseignement américain, qui alerte l'État français, qui alerte la Région. Ensuite, on saisit les forces judiciaires, notamment la gendarmerie ou un expert de justice, comme moi.

J'en ai fini. Je repasse le micro à Pierre.

Un dernier mot pour clôturer ce colloque

M. Pierre BONNET.-

Je voulais remercier l'ensemble de nos intervenants pour la qualité de leurs interventions.

Je terminerai ce colloque en me faisant le témoin de la manipulation opérée par Philippe au cours de son intervention puisque c'était mon ordinateur qui était ciblé. Philippe m'avait demandé d'écrire quelque chose sur mon ordinateur, évidemment sans qu'il voit ce que j'avais saisi. Or, grâce à son logiciel, il a pu savoir ce que j'avais « pianoté » sur mon clavier alors qu'il se trouvait à l'autre bout de la pièce. Maintenant, à chaque fois que je prends le train et que quelqu'un est assis à côté de moi, j'ai toujours un petit sourire, me disant que la personne qui est juste derrière nous possède peut-être le même logiciel que Philippe et regarde tout ce que nous rédigeons !

Je vous remercie tous chaleureusement et vous propose de nous retrouver pour le cocktail au niveau du restaurant.

Merci à tous de votre attention !

(Applaudissements).

Pour aller plus loin

Documents et sites à consulter

Site de l'ANSSI (https://www.ssi.gouv.fr/) :

- Panorama de la cybermenace 2022
- Guide des bonnes pratiques de l'informatique
- La cybersécurité pour le TPE/PME en 12 questions

Autres références :

- https://www.gendarmerie.interieur.gouv.fr/gendinfo/dossiers/la-menace-cyber
- https://www.gendarmerie.interieur.gouv.fr/onists/ressources-documentaires/veille-technologique/la-cybercriminalite-organisee
- « La convention de Budapest et ses protocoles » – Conseil de l'Europe https://www.coe.int/fr/web/cybercrime/the-budapest-convention
- « Cybersécurité: le Parlement adopte une nouvelle loi pour renforcer la résilience à l'échelle européenne » https://www.europarl.europa.eu/news/fr/press-room/20221107IPR49608/cybersecurite-une-nouvelle-loi-pour-renforcer-la-resilience-europeenne
- « Cyberstratégie, l'art de la guerre numérique », Bertrand Boyer, ed. Numis
- SecNumacadémie (secnumacademie.gouv.fr)