CYBERATTAQUES >
Les TPE-PME : les oubliées de la cybersécurité

DOSSIER > France Num, nouvelle initiative nationale d'assistance aux TPE-PME

DROIT > Secret des affaires : un outil de protection numérique

REVUE
de la gendarmerie nationale

REVUE TRIMESTRIELLE / AVRIL 2019 / N° 264 / PRIX 6 EUROS

La sécurité économique des TPE et des PME
dans un environnement numérique

retour sur images NUMÉRO 263

© concept of leaky software, par the_lightwriter

PROTECTION DE LA VIE PRIVÉE DÈS LA CONCEPTION

La révolution industrielle de l'économie numérique, l'émergence du réseau social comme mode de communication et l'interconnexion généralisée des objets induisent de nouvelles pratiques relationnelles et économiques. Celles-ci génèrent également des activités illégales dont les auteurs démontrent un haut niveau de technicité. La protection des données personnelles et la sécurité « by design » sont maintenant des sujets centraux. Les acteurs des traitements doivent tenir compte des impératifs de sécurité dès la conception d'un produit et pour tout son cycle de vie.

RETROUVEZ À PARTIR DE LA PAGE 52 DE CE NUMÉRO DEUX INITIATIVES NATIONALES (FRANCE NUM ET CYBERMALVEILLANCE.GOUV.FR) FORMALISÉES PAR DES PLATEFORMES D'ASSISTANCE AUX VICTIMES, NOTAMMENT LES TPE ET PME. PARTENARIALES, INTUITIVES ET METTANT EN ŒUVRE UN RÉSEAU D'EXPERTS CERTIFIÉS, ELLES S'INSCRIVENT PRAGMATIQUEMENT DANS UN SPECTRE DE PRÉVENTION, D'INFORMATION ET DE SENSIBILISATION.

© France num

Répondre aux demandes du marché, entretenir une relation clientèle, avoir une grande réactivité aux évolutions technologiques engloutit l'essentiel des ressources humaines et matérielles des TPE et des PME. La numérisation des échanges mondialisés, la mise en réseau des protocoles commerciaux, l'émergence des objets connectés ont fragilisé les entreprises en mettant leurs valeurs patrimoniales et mobilières à la portée des cybercriminels. Autant les grandes entreprises, fortes de leur puissance financière et de la disponibilité d'experts, ont globalement saisi les enjeux de la cybersécurité, autant les TPE-PME peinent culturellement à mobiliser des moyens et à mettre en place des mesures préventives visant à protéger leurs valeurs : données, brevets, processus industriels qui assoient leur destin économique.

Les acteurs économiques et les pouvoirs publics ont pris conscience de cette faiblesse structurelle qui touche des entreprises qui forment une part importante du marché du travail et de la richesse de la nation. Les CCI, les ordres professionnels, l'ANSII mais également des initiatives nationales (France Num, Acyma) concourent à guider les entreprises vers une sécurité acceptable. La Gendarmerie nationale, forte de son maillage territorial et de son réseau d'experts en intelligence économique et en nouvelles technologies, participe à cet effort de sécurisation du tissu commercial et humain formé par les TPE et PME.

COL(ER) Philippe Durand,
rédacteur en chef

SOMMAIRE

NUMÉRO 264

PME ET CYBERATTAQUES

DOSSIER

DROIT

DOSSIER

UN ACCOMPAGNEMENT
face à la menace

PME ET CYBERATTAQUES

© Fotolia_122388647_Subscription_XL

LE RISQUE DE PERDRE LES VALEURS SUBSTANTIELLES DE L'ENTREPRISE

Accélératrices du développement national, les 3,1 millions de TPE-PME sont en retard en matière de transformation digitale alors que trois quarts d'entre elles ont déjà subi une attaque virale. L'inadéquation entre le risque ressenti par les dirigeants d'entreprise recélant des expertises et la fréquence des cyberattaques montre une acculturation insuffisante. Des personnels inexpérimentés, des stockages non sécurisés de données sensibles attestent de cette impréparation.

La prise de conscience des dirigeants et la formation de leurs collaborateurs, la promotion d'outils accessibles conjugués à l'utilisation de formations en ligne de l'ANSII sont une première étape pour assainir l'environnement numérique de ces petites entreprises. On peut y ajouter le choix de solutions Web totalement respectueuses de la vie privée et le soutien procuré par des plateformes gouvernementales et nationales.

TPE-PME : les oubliées de la cybersécurité

Par François Cazals

Les TPE-PME représentent un potentiel essentiel pour la France. Leur contribution humaine, économique, sociale et leur dynamisme en font de véritables accélérateurs du développement national. Sont-elles suffisamment armées pour relever les défis de la cybersécurité, qui représentent aujourd'hui un enjeu crucial pour leur pérennité ?

Après quelques définitions initiales, nous verrons le poids stratégique de ces entreprises pour notre pays. Dans un second temps, nous évaluerons la situation, les enjeux et les défis de la cybersécurité des TPE-PME. Finalement, nous proposerons quelques pistes pour élaborer une véritable stratégie Cyber, adaptée à leur taille et à leurs spécificités.

FRANÇOIS CAZALS

Professeur adjoint HEC Paris
Lieutenant-colonel Réserve citoyenne de la gendarmerie

Les TPE-PME : des atouts capitaux pour la France

Commençons par définir les concepts de TPE et PME. Les TPE sont des entreprises ayant moins de 10 salariés et un chiffre d'affaires annuel ou un bilan total inférieur à 2 millions d'euros. Depuis la loi n° 2008-776 du 4 août 2008 de modernisation de l'économie, les TPE sont renommées microentreprises (attention, toutefois, à ne pas confondre avec le régime fiscal de la micro-entreprise qui est le nom donné à l'auto-entreprise) [1]. Les PME, quant à elles, sont des entreprises qui occupent moins de 250 personnes, et qui ont un chiffre d'affaires annuel inférieur à 50 millions d'euros ou un total de bilan n'excédant pas 43 millions d'euros[2].

(1) https://www.l-expert-comptable.com/a/51980-qu-est-ce-qu-une-tpe-tres-petite-entreprise-ou-microentreprise.html

(2) https://www.insee.fr/fr/metadonnees/definition/c1962

Les 3,1 millions de TPE-PME représentent l'immense majorité des entreprises, en

France (99,8 %). Elles réalisent 1 300 milliards d'euros de chiffre d'affaires annuel (36 % du total français) et 44 % de la valeur ajoutée du tissu productif français. 360 000 (11,7 % du total) sont des entreprises exportatrices. Par ailleurs, elles pèsent pour 49 % de l'emploi salarié en France, même si 55 % d'entre-elles n'emploient aucun salarié (entreprises individuelles) [3].

(3) INSEE, Les Entreprises en France 2014 (données 2011) et Etude Ipsos pour Randstad (données 2016).

Néanmoins, elles sont en retard en matière de transformation digitale. Selon l'indice DESI (Digital Economy and Society Index) 2017 publié par la Commission européenne, les TPE et PME de l'hexagone se positionnent seulement à la 16e place du classement européen, même si 76 % d'entre-elles ont un site Web et 74 % assurent une présence sur les réseaux sociaux[4].

(4) https://www.francenum.gouv.fr/comprendre-le-numerique/20-chiffres-cles-sur-la-presence-sur-internet-des-tpe-pme-en-2018

Dans ce panorama, la cybersécurité représente évidemment un enjeu crucial de développement.

Cybersécurité des TPE-PME : le défi de la taille

Avant d'aller plus loin, définissons rapidement les principaux concepts de la cybersécurité. Voici la définition officielle donnée par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) : « État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.[5] »

(5) https://www.ssi.gouv.fr/entreprise/glossaire/c/

(6) https://www.market-inspector.fr/blog/2017/06/cybersecurite-et-pme

Faisons un rapide bilan de la résilience des TPE-PME à ces risques Cyber[6] : celui-ci fait apparaître une situation plutôt inquiétante. Ainsi, 74 % des TPE-PME ont déjà pâti d'une cyberattaque. Le type d'attaques les plus subies par les entreprises reste la demande de rançon (Ransomware), à 80 %. Viennent ensuite les attaques par déni de service (40 %), les attaques virales généralisées (36 %) et la fraude externe (29 %). Paradoxalement, 83 % d'entre-elles se sentent peu ou pas exposées aux risques Cyber ! Ce décalage de perception montre le risque encouru.

Et pourtant, l'enjeu économique est très significatif, puisqu'il est évalué, en moyenne, à 242 000 euros, ce qui représente près de 50 % du chiffre d'affaires de la TPE moyenne, ce qui est considérable. Au-delà des conséquences financières, la réputation des entreprises est évidemment

© Elite hacker entering a room in turquoise par beebright

La problématique fondamentale est l'inadéquation entre le risque ressenti par les dirigeants quant aux valeurs de leur entreprise et la fréquence de cyberattaques frappant les petites et moyennes structures notamment celles qui recèlent des expertises techniques ou des bases de données personnelles.

affectée par un sinistre Cyber. Ainsi, 50 % des français sont prêts à poursuivre en justice les entreprises pour négligence sur leurs données personnelles. Les nouvelles règlementations européennes (RGPD[7]) renforcent, par ailleurs, les responsabilités des entreprises sur le sujet.

(7) RGPD - https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes

Les causes de cet état des lieux inquiétant s'expliquent assez logiquement par des problématiques de taille, de moyens et de maturité organisationnelle. 5 à 10 % du budget global de l'entreprise devrait être alloué à la cybersécurité. C'est en tout cas l'estimation de Guillaume Poupard, directeur de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Il précise : « Oui, la sécurité a un coût, mais ce n'est pas grand-chose comparé au prix à payer lorsqu'on est victime d'une attaque informatique » [8]. Il est clair qu'il s'agit d'un effort difficilement accessible pour de petites structures, singulièrement les TPE. L'autre enjeu principal est humain, assez logiquement. Ainsi, 1 TPE-PME sur 3 confie la cybersécurité à des employés inexpérimentés. Dans le même registre, 16 % des TPE et PME laissent leur personnel stocker des informations client personnelles identifiables sur leurs propres appareils, qu'ils utilisent pour le travail[9]. Que le mobile soit financier (73 % des attaques selon le baromètre Verizon) ou l'espionnage (21 %), l'attaquant exploite la faiblesse du maillon humain dans le

(8) https://experiences.microsoft.fr/business/confiance-numerique-business/cybersecurite-chiffres-cles/

(9) https://itsocial.fr/enjeux/securite-dsi/

dispositif : la cybersécurité, c'est 20 % de technologie, 80 % de management[10].

(10) https://www.lesechos.fr/pme-regions/

Quelques pistes nous semblent réalistes pour réduire cette grande vulnérabilité Cyber des TPE-PME et renforcer leur potentiel numérique.

Renforcer la cybersécurité et concevoir une stratégie numérique des TPE-PME

Trois enjeux se dégagent pour assurer la sécurité et le développement numérique des TPE-PME.

Le premier enjeu est celui de la prise de conscience des dirigeants et de la formation des collaborateurs. Aujourd'hui, il n'est plus possible pour une entreprise, quelle que soit sa taille, de négliger la dimension numérique de son organisation. Les relations avec les services de l'État et les organismes sociaux lui imposent déjà des interactions essentiellement virtualisées (déclarations fiscales et sociales en ligne, par exemple). Par ailleurs, la visibilité sur Internet est aujourd'hui capitale pour se faire connaître. Le concept ZMOT (*Zero Moment of Truth*, le moment zéro de vérité[11]), développé par Google, postule que la recherche d'information dans un processus décisionnel commence essentiellement sur le Web. Il convient donc d'imaginer et de concevoir une véritable stratégie numérique intégrant une dimension offensive, pour se développer et défensive, de cybersécurité. Une réflexion et des outils théoriques accessibles à des petites structures permettent aujourd'hui d'aborder cet enjeu[12]. La formation des collaborateurs constitue également un défi important. De manière générale, l'effort de formation est assez faible dans les TPE-PME. Si 48 % des salariés ont suivi une formation en 2015, cette proportion s'échelonne de 25 % dans les plus petites à 63 % dans les plus grandes[13]. Le manque de disponibilité et le coût des formations expliquent facilement cette situation. Néanmoins, des solutions innovantes permettent aujourd'hui de surmonter ces difficultés. L'état met à disposition une formation en ligne sur la cybersécurité : le MOOC[14] de l'ANSSI[15]. Cette formation de 16 heures est certifiante et gratuite. D'autres formations en ligne gratuites permettent d'approfondir des aspects spécifiques de la cybersécurité, notamment au plan des risques juridiques[16].

(11) https://www.thinkwithgoogle.com/marketing-resources/micro-moments/zero-moment-truth/

(12) Stratégies digitales : la méthode des 6C (Cazals, De Boeck, mai 2018).

(13) https://www.cpformation.com/formation-tpe/

(14) L'acronyme MOOC signifie « Massive Open Online Course » que l'on peut traduire par « cours en ligne ouvert et massif » : https://moocs.unige.ch/presentation/

(15) https://secnumacademie.gouv.fr/

(16) https://www.my-mooc.com/fr/mooc/maitrisez-les-risques-juridiques-lies-au-numerique/

L'enjeu technologique est évidemment réel. Au-delà des dimensions élémentaires de la cybersécurité (logiciels de protection, pratiques de sauvegardes, sécurisation des postes de travail, …), la migration des systèmes d'information vers le Cloud permet

un renforcement significatif de la cybersécurité. Si les grands leaders mondiaux sont américains (Amazon/AWS, Microsoft/Azure, …), des solutions françaises permettent de garantir une souveraineté des données sur le territoire national (OVH, Orange, …). Ajoutons qu'il est aujourd'hui possible de choisir des solutions Web totalement respectueuses de la vie privée et qui permettent d'avoir accès à toutes les fonctionnalités Internet de base. Le moteur de recherche français QWANT se développe significativement sur cette promesse[17].

(17) https://www.qwant.com/?l=fr

(18) https://framasoft.org/fr/

Dans la même veine, le projet FRAMASOFT[18] propose 32 services numériques libres et sécurisés.

Le troisième enjeu est public : celui de la sécurité nationale des données. Cybermalveillance.gouv.fr est le programme gouvernemental assumant un rôle de sensibilisation, de prévention et de soutien en matière de sécurité du numérique auprès des particuliers, des entreprises ou des collectivités territoriales. La plateforme en ligne du dispositif est là pour accompagner les victimes d'une cybermalveillance : établissement d'un diagnostic précis de la situation, mise en relation avec les spécialistes et organismes compétents proches des victimes et mise à disposition d'outils et de publications dispensant de nombreux conseils pratiques. La gendarmerie nationale s'est évidemment engagée résolument, ces dernières années, dans la lutte contre ces nouvelles formes de criminalité, en rapport notamment avec l'utilisation de l'Internet. Cette nouvelle typologie de crimes et de délits a conduit à mettre en place aux niveaux central et territorial des formations et des moyens spécifiques[19].

(19) https://www.gendarmerie.interieur.gouv.fr/Zooms/Cybercriminalite

Conclusion

La transformation numérique de la société touche évidemment les TPE-PME. Celles-ci doivent intégrer de nouveaux enjeux : saisir les opportunités technologiques pour se développer et se prémunir de risques nouveaux. Cette reconfiguration passera par la prise de conscience des dirigeants et un effort de formation important des salariés. Dans ce contexte, l'appui de l'État sera déterminant. La gendarmerie nationale, quant à elle, va certainement devoir intégrer une nouvelle mission : à la sécurité des personnes et des biens, il faudra ajouter la sécurité des données.

L'AUTEUR

François Cazals est professeur adjoint à HEC Paris. Spécialiste des stratégies numériques et de la valorisation des données (Big Data, Data Science, intelligence artificielle), il dirige également un cabinet de conseil en stratégie. Il a rédigé de nombreux ouvrages et articles, en particulier « Stratégies digitales : la méthode des 6C » (De Boeck, mai 2018, 2e édition).
Il est également lieutenant-colonel (réserve citoyenne) de gendarmerie, affecté au cabinet du directeur général.

PME ET CYBERATTAQUES

© wutzkoh pour AdobeStock_138582698

UNE TRANSITION TECHNOLOGIQUE DÉLICATE

Réactives, flexibles, compétitives tout en mobilisant des ressources humaines réduites, les TPE-PME vivent le passage d'une sécurité informatique centralisée et gérée par des spécialistes à des systèmes ouverts mise en œuvre par les utilisateurs qui ne maîtrisent pas nécessairement le fondement des technologies déployées. Cette transition d'une sécurité informatique à une cybersécurité passe par la définition d'un risque, de coûts et d'un niveau de protection acceptables…

Cela nécessite de considérer l'organisation de l'entreprise et d'y instaurer une conscience collective des cybermenaces et des mesures de prévention à inclure dans ses protocoles internes.

De la Sécurité Informatique

à la Cyber-Sécurité, les TPE et PME ont-elles mal appréhendé ce changement de paradigme ?

Par Didier Spella

L'époque où les cyberattaques étaient le lot de quelques PME malchanceuses est bel et bien révolue. Très rentables pour les cybercriminels car plus faciles à attaquer que les grands groupes, elles sont devenues une cible de choix. Au cours des 12 derniers mois, 21 % ont été victimes d'une cyberattaque. Si le coût de celles-ci dépasse rarement les 10 000 €, il peut arriver dans de très rares cas que l'entreprise victime ne s'en relève pas, notamment quand l'affaire devient publique. (01/02/2019 – Damien Bancal).

DIDIER SPELLA

Mirat Di Neride
Excelia Group
La Rochelle

Une « belle commande… »

Encore un de ces matins ensoleillés qui font le charme de cette région. Il est temps de se rendre sur les parcs à huîtres car la marée n'attend pas. Ce matin, René, ostréiculteur, a une grosse commande à expédier.

Hier soir, il a reçu par mail de son commanditaire habituel une demande un peu particulière, mais bon, il lui a répondu qu'il ferait tout son possible pour l'honorer.

Au retour des parcs, la mise en cagette des 2 tonnes d'huîtres ne prend que quelques heures et le livreur est déjà prêt à faire la route jusqu'en Espagne. Cette fois ci, le lieu de livraison a changé, mais bon, Ce sont des choses qui arrivent.

La journée se poursuit, il reste à envoyer la facture…

Deux jours plus tard, le jeudi, nouvelle commande de son commanditaire. René en profite pour l'appeler…

« Alors, cette commande de mardi ? Ça vous a plu ? »

« Quelle commande ? Je ne vous ai rien commandé depuis 3 semaines ?

« Mais si, votre message de lundi, les 2 tonnes d'huîtres ? »

« Je ne vous ai jamais envoyé de message lundi, j'étais au Maroc depuis samedi. Je suis rentré mardi soir. J'ai même mis des photos sur ma page Facebook »

René commence à réaliser qu'il vient de se faire escroquer…

Quelqu'un s'est fait passer pour son commanditaire. En reprenant l'adresse mail de sa commande, il s'aperçoit alors qu'elle est légèrement différente…

Encore une usurpation d'identité…
Le cyber criminel a observé les échanges de cet entrepreneur, a surveillé le commanditaire…

Nous sommes devant un cas assez classique de délit commis sur une petite entreprise. On aurait pu aussi chiffrer les données sur son ordinateur et lui demander une rançon…

Le contexte

Qu'il s'agisse des Petites et Moyennes Entreprises (PME) ou des Très Petites Entreprises (TPE), leur caractéristique commune est la centralisation de la gestion de la société. Elles en font un véritable atout de compétitivité car avec des ressources humaines réduites, ces sociétés sont beaucoup plus réactives et flexibles que des structures appartenant à des grands groupes.

Pour contextualiser réellement les TPE et les PME, il convient de les définir. Pour cela, nous nous inspirerons des définitions parues dans « Économie Magazine ».

Une distinction technique

Souvent on a tendance à confondre la TPE et la PME. Pourtant ces deux notions sont vraiment différentes. Mais commençons par la Très Petite Entreprise. Il est d'usage de qualifier de TPE toutes les structures dotées de la personnalité morale, dont le nombre maximal de salariés est inférieur à dix. Par ailleurs, le chiffre d'affaires annuel ou le total du bilan réalisé par ces TPE ne doit pas dépasser le plafond de deux millions d'euros.

Cette forme de société est dans la grande majorité des cas une entreprise individuelle, c'est-à-dire sans salariés. On l'appelle alors également « micro-entreprise ». Elle correspond là aux besoins des travailleurs non-salariés tels que les artisans, les commerçants ou les professions libérales. Ainsi, comme le démarrage de ce type d'entreprise n'exige pas beaucoup de ressources, tant humaines que financières, les TPE constituent l'essentiel des créations d'entreprises en France. En effet, selon les statistiques, près de 93 % des sociétés créées en France sont des

micro-entreprises. La particularité réservée aux micro-entreprises concerne leur régime fiscal qui est spécifique.

En comparaison avec la TPE, la PME se démarque par sa taille. À ce jour, il n'y a pas de définition précise pour ce qui est de ces types d'entreprises. Celle de la recommandation européenne n° 96/280/CE du 3 avril 1996 modifiée par la recommandation n° 2003/361/CE du 6 mai 2003 semble s'imposer. Ces textes organisent une classification des entreprises en fonction de deux données conjuguées : leur taille et leur chiffre d'affaires.

Sont donc définies comme petites entreprises, les sociétés dont l'effectif se situe entre dix et cinquante salariés et dont le chiffre d'affaires et le bilan total n'excèdent pas dix millions d'euros par an.

Entre cinquante et un et deux cent cinquante salariés, on peut définir les « moyennes entreprises » dont le chiffre d'affaires sera inférieur à cinquante millions d'euros et le bilan total annuel à quarante-trois millions d'euros.

Au-delà de deux cent cinquante salariés, on parlera alors de « grande entreprise ».

Quelques chiffres…

Selon une étude de PWC, pour moins d'un tiers des entreprises françaises la cyber-sécurité est un enjeu aujourd'hui. *A contrario*, deux tiers considèrent que le risque d'une cyber-menace dans leur entreprise n'est pas important. Il en ressort, c'est peut-être le plus grave, que 2 entreprises sur 10 se sentent tout à fait capables de gérer une cyber attaque. Pour compléter ce tableau, moins d'une entreprise sur 5 a véritablement mis en œuvre des mesures de protection possibles. Enfin, 95 % des entreprises ne comptent pas engager une personne dédiée à la cyber-sécurité dans les 12 prochains mois.

Quel sont ces cybers risques ?

Les cybers risques sont de deux ordres :

– des risques directs sur l'environnement technique des Technologies de l'information et de la communication (TICs),
– des risques plus « classiques » qui concernent des environnements utilisant les TICs.

On voit bien alors que la problématique ne peut pas se résumer à un renforcement des TICs.

L'espace numérique

Il faut d'abord définir ce que recouvre l'espace numérique. Nous en donnerons cette définition : ensemble des paradigmes qui sont utilisés afin de fournir le service que l'on attend d'une machine numérique. Ces paradigmes, à partir desquels l'espace numérique s'est développé, sont au nombre de quatre :

Le premier est celui de l'électricité, au sens « ions » positifs et négatifs, et de toutes

les propriétés qui en découlent : transport d'énergie, mais aussi électromagnétisme, ondes radios, rayonnement, etc…

Le deuxième est le paradigme de toute machine numérique qui reprend tout ou partie de l'architecture type définie par von Neumann.
Le troisième concerne la communication. Il peut être schématisé de la manière suivante : la transmission d'un message nécessite un émetteur et un récepteur qui codent et décodent le message transmis au moyen d'un canal de transmission.
Le quatrième est la donnée dont nous reprendrons les 3 propriétés : disponibilité, confidentialité et intégrité.

De la Sécurité Informatique…

À la création du monde numérique, nous sommes en présence de machines numériques imposantes qui nécessitent un positionnement dans des lieux dédiés. Elles sont chères, ainsi que tous les périphériques qui s'y rattachent. Elles sont administrées par des personnels qualifiés et nécessitent une surveillance permanente. Leurs accès logiques sont réduits faute de potentiels d'accès et d'un débit très limité. Il en ressort que seules les fonctions pouvant être numérisées sont développées et traitées sur ces machines, à la ressource limitée.

Nous sommes alors en présence de centres informatiques, véritables « bunkers » physiques, qui vont offrir surtout une protection électrique en termes de disponibilité. Un personnel nombreux et qualifié y est employé. Les utilisateurs du système sont au mieux connectés en filaire pour traiter quelques informations. Au pire, ils lancent des traitements qui leur sont restitués sous forme de documents imprimés (listings). Aucune ressource de traitement n'est délocalisée. Les protocoles réseaux sont rigides et complexes, mais facilement traçables. Les débits sont limités. La grande priorité en termes de données est surtout la disponibilité.

Nous sommes sur un environnement technique, lourd, nécessitant des ressources importantes et spécialisées. En fait, un monde assez fermé dont les utilisateurs « attachés » à un centre de traitement doivent en respecter les règles et les contraintes.

Nos quatre paradigmes apparaissent alors comme des **piliers**. Nous sommes vraiment dans une sécurité physique et technique, qu'utilise **un monde technique, mis en œuvre par des spécialistes**.

Pour les TPE et PME, l'investissement numérique est rare et spécifique. Les machines doivent être installées par des prestataires confirmés. L'ensemble de la gestion du système est confié à un spécialiste pour les structures assez importantes ou totalement sous-traité à un prestataire de service.

…À la cyber-sécurité

Une définition de la Cyber-sécurité

La cyber-sécurité (selon l'ANSSI) est l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cyber-sécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

Les évolutions

Au cours des 20 dernières années, les 4 paradigmes ont subi des évolutions.

– L'électricité a vu ses propriétés développées et utilisées, notamment en termes de consommation d'énergie, en matière d'électromagnétisme, de rayonnement et sur ses propriétés d'ondulation…

– La machine de von Neumann, a pu être réduite, miniaturisée et renforcée. Elle rentre dans des machines très petites, transportables et portatives. Elles sont plus robustes et ne nécessitent pas des environnements régulés. En outre, les systèmes peuvent être préconfigurés sur la machine. Leurs coûts deviennent de plus en plus réduits. Distribuées dans des commerces « grand public », elles peuvent être mises en œuvre par des non spécialistes.

– Les communications ont subi des évolutions phénoménales, en termes de support, dont les débits s'accroissent et les protocoles sont plus simples. L'ensemble combiné permet alors des diffusions « nuageuses » rendant obsolètes toutes formes de câbles. Nous n'avons plus besoin d'une compétence réseau pour mettre en œuvre ces communications.

– En ce qui concerne la donnée, si sa disponibilité est assurée par des médias de plus en plus performants, miniaturisés et peu chers, sa confidentialité semble assez simple à assurer. En fait son intégrité devient le nouvel enjeu de la sécurité.

Il ressort de ces évolutions une vulgarisation complète de cette technologie numérique qui apparaît alors simple et bon marché. Nous pouvons tout numériser, donc tout est numérisé. Le pouvoir qui était sur le système informatique se déplace des experts et des spécialistes vers les utilisateurs finaux qui n'ont plus besoin de connaître ces technologies.

Toute la gestion du monde numérique est dévolue à l'utilisateur final. Les technologies ont évolué pour lui permettre cette gestion mais elles ouvrent autant de voies à des activités frauduleuses autour de ce monde numérique. Exit les bunkers sécurisés où se positionnaient les machines de

© State in which the conference using the electronic tablet By Monet

Passées d'un système centralisé, sécurisé dans un environnement de spécialistes, à un système ouvert en réseau, où l'utilisateur commun use de logiciels variés dans une interconnexion générale, les entreprises doivent définir un champ de risques et façonner un ensemble de mesures acceptables, tant au niveau des coûts que des mœurs de l'entreprise, pour y faire face.

traitement. Exit les protocoles qui permettaient de suivre le cheminement des trames. Nous sommes dans un monde technologique ouvert, mis en œuvre par des utilisateurs.

Confrontés à l'évolution de ces paradigmes, nous pouvons comprendre le désarroi des chefs d'entreprises de TPE et PME. Les 4 piliers du numérique leur sont devenus les 4 cavaliers de l'apocalypse.

Comment passer de la sécurité informatique à la cyber-sécurité

Après ce lourd constat, il est temps d'identifier quelques axes d'évolutions afin d'amener les chefs d'entreprises à mieux les appréhender.

Il est donc nécessaire d'aborder le problème de la Cyber-sécurité, non pas comme un problème technique mais comme un problème sociétal.

Le chef d'entreprise doit donc s'en emparer, en y associant le responsable informatique pour celles qui en ont un, et/ou leurs prestataires pour les autres. Ils sont des acteurs incontournables de cette démarche. Cependant, ce ne sont pas les seuls qui doivent être associés.

Des objectifs acceptables – le risque

Il revient dans un premier temps au chef d'entreprise de recenser l'intégralité de ses ***risques***. Concernant tous les domaines de l'entreprise, cette démarche

nécessitera une analyse fine. En fonction de celle-ci, le dirigeant d'une entreprise devra commencer par améliorer sa sûreté puis sa sécurité, afin de réduire l'ensemble des risques initialement identifiés. Il pourra même transférer une partie de ces risques auprès d'un assureur spécialisé dans le domaine concerné. ***Son risque devient alors acceptable.***

Des objectifs acceptables – le coût

Toutes les solutions que le chef d'entreprise devra mettre en œuvre auront un coût pour son entreprise. Il devra comparer ces coûts à ceux qu'entraînerait un sinistre, dû aux risques évalués lors de l'analyse. Cette démarche fait que le ***coût devient alors acceptable***.

Une mise en œuvre…

Au-delà des solutions techniques qui seront construites et mises en œuvre par les spécialistes du domaine (et là nous retrouvons en partie notre sécurité informatique), il faudra revoir l'organisation de l'entreprise. Tous les composants numériques pouvant être personnels ou professionnels, ainsi que leurs usages et leur cadre d'utilisation, présentent alors le risque de ne plus être protégés par les équipements techniques mis en œuvre dans l'environnement professionnel. Il faudra donc revoir les règles d'usage de tous ces composants « numériques ». Il sera nécessaire d'éduquer les collaborateurs afin de développer au sein de l'entreprise une ***conscience collective***.

Tout cela montre bien l'ensemble des problèmes que rencontrent nos TPE et PME. Tournées vers une productivité indispensable à leur survie, elles ont recours à une technologie qui a évolué sur des axes divergents. Cela leur impose une réflexion qui ne relève pas seulement d'un aspect technologique mais aussi d'un aspect sociétal.

Notre sensibilisation doit porter sur ces aspects afin d'amener les chefs d'entreprise à mieux appréhender leur approche vis-à-vis de la cyber-sécurité.

L'AUTEUR

Ancien officier supérieur de l'Armée de l'Air, co-fondateur de Charente-Maritime Cyber Sécurité, colloque qui s'est déroulé pour la première fois les 17 & 18 octobre 2018, à La Rochelle, Didier SPELLA a vu évoluer les différents concepts qui régissent aujourd'hui le cybermonde. Ses connaissances en sécurité tant analogiques que numériques, son expérience d'analyse de risques et ses expertises, auprès d'une compagnie américaine, lui ont permis de se positionner en tant qu'expert en définition de stratégie de sécurité. Confronté aux attaques cyber de plus en plus importantes et intrusives dans nos modes de vie, il a récemment été à l'initiative de ce colloque dans lequel ont été abordés les risques encourus par la population en général et plus particulièrement les responsables de TPE et PME. Le thème développé était : « tous attaqués, tous complices ».

PME ET CYBERATTAQUES

© Fotolia Red 50770

UNE ATTAQUE DES OUTILS DE PRODUCTION POUR OBTENIR UN EFFET DÉVASTATEUR SUR L'ENVIRONNEMENT D'UNE ENTREPRISE

Une cyberattaque sur des outils de production, qu'elle soit commise par un groupe privé ou un état, peut avoir un effet dévastateur sur une ressource humaine et sur l'environnement.

L'intrusion est possible du fait d'automates, de SCADAS non sécurisés dès leur conception et d'un déploiement territorial, national et international, susceptible de permettre de délivrer au client une prestation de service en adéquation avec la demande du marché local.

La transition énergétique s'accompagnera d'une interconnexion des processus, de l'affinement des techniques de télé-maintenance et de supervision. Elles sont indispensables pour assurer un pilotage précis et réactif des automates et logiciels qui concourent à la disponibilité des services mais constituent des sources de vulnérabilités.

Cyberattaques :
peut-on craindre des conséquences sur l'intégrité physique des personnes ?

Par Sylvain Chaumette

Certaines TPE/PME[1] exploitent des installations mettant en œuvre des matières dangereuses. Ces installations disposent pour la plupart de systèmes automatisés de contrôle qui peuvent être connectés à différents dispositifs de commande ou de supervision souvent reliés directement ou indirectement au réseau extérieur de l'entreprise. Une prise de contrôle à distance de ces installations par des cyber-attaquants pourrait leur permettre de provoquer des phénomènes physiques dangereux pour les personnels, les utilisateurs ou les riverains tels que des explosions, incendies ou rejets toxiques.

(1) Notamment, 94% du tissu des entreprises de la chimie en France est constitué de TPE / PME (source site internet https://www.francechimie.fr/Positions-Expertises/Economie-competitivite/TPE-PME-ETI).

SYLVAIN CHAUMETTE

Responsable du pôle Analyse et Gestion Intégrées des Risques accidentels. INERIS

Les transformations en cours dans l'industrie (numérisation et standardisation des technologies du contrôle commande, transition énergétique, industrie 4.0) ainsi que la montée des actes de terrorisme tendent à augmenter la vraisemblance de cyberattaques visant à provoquer des conséquences humaines.

Quelles conséquences d'une cyberattaque ?

Pour bon nombre de personnes, les cyberattaques consistent en des actes de malveillance visant la destruction ou le vol de données avec des objectifs d'espionnage, de manipulation, financiers ou d'atteinte à l'image par exemple.

L'impact sur l'outil de production est

rarement cité comme une conséquence potentielle d'une cyberattaque. Pourtant, plusieurs d'entre-elles ont eu ces dernières années des effets directs ou indirects sur les installations industrielles, les plus médiatisées étant celles liées à un arrêt de production généré par une cyberattaque tel que le *blackout* électrique en Ukraine de Décembre 2015[2].

(2) Référence : Fiches Incident Cyber SI Industriels – CLUSIF – GT SCADA (lien internet : https://clusif.fr/publications/fiches-incidents-cyber-industriels-2017/)

L'impact sur l'outil de production qui pourrait générer des effets dommageables sur l'intégrité physique des hommes ou sur l'environnement naturel n'est quant à lui quasiment jamais pensé. Pour autant, bon nombre d'entreprises disposent d'installations qui stockent, utilisent ou produisent des produits dangereux (gaz naturel, propane, butane, ammoniac, acides, bases, etc…) pouvant être à l'origine d'explosions, d'incendies et/ou de rejets d'effluents toxiques en cas de dysfonctionnements. La corruption des systèmes de contrôle de ces installations (modifications de mesures ou de seuils de régulation, envoi de commandes via la supervision, désactivation de fonction de sécurité) peut aboutir aux mêmes phénomènes dangereux.

Quel historique ?

Plusieurs cyberattaques ayant pour finalité de provoquer des dégâts matériels ou humains ont été recensées[3] par le passé. À noter que pour certaines d'entre elles, la prise en main sur le système informatique a été précédée d'une intrusion in situ et que pour d'autres, l'attaque vient de l'intérieur (personnel ou sous-traitant). À titre d'illustration, certaines sont brièvement décrites dans les paragraphes suivants.

(3) Référence : Fiches Incident Cyber SI Industriels – CLUSIF – GT SCADA (lien internet : https://clusif.fr/publications/fiches-incidents-cyber-industriels-2017/).

En 2000, un ancien employé de la société, ayant installé le SCADA[4] d'une centrale de traitement des eaux usée en Australie, s'est vengé suite à un refus de la société gérant la centrale de l'embaucher. Il a volé un équipement radio de son employeur et a envoyé des commandes au SCADA générant le déversement dans la nature de 800 m3 d'eaux usées.

(4) Logiciels destinés au contrôle de processus et à la collecte de données en temps réel auprès de sites distants, en vue de contrôler des équipements et des conditions d'exploitation.

En 2008, des attaquants ont exploité la vulnérabilité des caméras de surveillance installées le long du pipeline de Baku-Tbilisi-Ceyhan en Turquie pour accéder au serveur de gestion des alarmes et des moyens de communication. Puis, ils se sont rendus physiquement à une station de pompage et ont généré, par l'intermédiaire du système de contrôle local, une montée en pression dans le pipeline qui a

entraîné une explosion.

En 2011, un ver informatique très complexe (Stuxnet) a endommagé 100 centrifugeuses du site d'enrichissement d'uranium de Natanz (Iran) en modifiant leur vitesse de rotation pour atteindre une fréquence de résonance. Ce virus exploitait 4 failles de windows et du système de contrôle de Siemens qui étaient inconnues avant cette attaque (« Zero Day »).

En 2013, des attaquants se sont introduits dans une station d'eau potable en Géorgie (USA) et ont, via le système de supervision, modifié les réglages des taux de fluor et de chlore injectés dans l'eau, la rendant impropre à la consommation et privant ainsi 400 personnes d'eau potable.

En 2014, des hackers ont pris les commandes des systèmes de contrôle d'une aciérie située en Allemagne via les logiciels de gestion et le réseau bureautique pénétrés par une campagne de mails infectés (variante du phishing). Ils ont fait dériver la température du haut fourneau et ont inhibé les fonctions automatiques de sécurité sur température haute, ce qui a causé de gros dégâts à l'infrastructure.

Ces exemples illustrent la diversité des types d'attaquants et des moyens humains, techniques et financiers mis en œuvre pour réaliser ces attaques.

Quel est le contexte actuel ?

Les entreprises connaissent actuellement de nombreuses évolutions de toutes formes, dont certaines sont très dépendantes de leurs secteurs d'activités, qui les rendent plus vulnérables à une cyber-attaque.

De façon globale, on assiste au déploiement massif d'objets connectés (et notamment l'internet des objets) et l'on s'attend à un déploiement d'installations de production plus petites (pour certaines installations reproductibles à grande échelle), plus proches des consommateurs (voire chez lui) qui, pour beaucoup d'entre elles, seront surveillées et pilotées à distances et toutes connectées au réseau internet.

L'un des exemples les plus parlants est sans nul doute celui de la transition énergétique[5] où sera disséminée au sein des territoires toute une panoplie d'installations de production, de stockage et de distribution d'énergie. Ce déploiement s'accompagnera donc d'une interconnexion forte et de la nécessité de piloter finement l'ensemble de ces moyens pour assurer la disponibilité de l'énergie quelles ques soient les demandes.

(5) Site internet Commission de régulation de l'énergie (lien : http://www.smartgrids-cre.fr/index.php?p=gestion-donnees-cyber-securite).

Enfin, les systèmes électroniques et logiciels liés à la sécurité des personnes

et de l'environnement (automates de contrôle commande, automates de sécurité, réseaux de communications industriels) présents sur les sites industriels sont des systèmes de plus en plus ouverts et connectés avec l'extérieur. Ils réalisent des fonctionnalités avancées (télé-maintenance, supervision à distance…) et utilisent des technologies issues des systèmes d'information (réseaux sans fils, PC de bureau, routeurs) les rendant vulnérables aux cyberattaques.

© 176330467 Smart factory and wireless communication network. Abstract mixed media par metamorworks

La variété des objets connectés, conjuguée à l'interconnexion des processus de pilotage et de maintenance ainsi qu'à une standardisation des logiciels de contrôle, crée une vulnérabilité de sites sensibles en aveuglant ou en trompant les décideurs sur la réalité des processus en cours.

En parallèle, les attaquants, aux motivations diverses et aux moyens plus ou moins importants, ayant les compétences pour attaquer les systèmes industriels, sont de plus en plus nombreux.

Ainsi, l'entreprise de sécurité Kaspersky a détecté des attaques sur 41 % des ordinateurs intégrés à des SCADA qu'elle protège au 1er semestre 2018 contre 37,75 % au second semestre 2017 et 36,61 % au premier semestre 2017[6].

(6) Source : https://ics-cert.kaspersky.com/reports/2018/09/06/threat-landscape-for-industrial-automation-systems-h1-2018/

Quel risque ?

L'attaque d'une installation dangereuse, dans le but de générer des dommages physiques, n'a d'intérêt a priori que si le site est sensible (en termes d'image par exemple), que si l'environnement de l'installation attaquée est sensible (forts enjeux dans l'environnement immédiat du site en termes de population, de cours d'eau etc.) ou que l'attaque peut toucher en même temps de nombreuses installations de même type.

Ainsi, des installations plus petites, bien que potentiellement moins dangereuses que leurs ainés et se rapprochant des enjeux humains (mix énergétique au cœur des villes), deviennent plus vulnérables aux cyber-attaques car elles sont connectées en réseau et potentiellement clônées en beaucoup d'exemplaires ou utilisant des équipements identiques et connectés, entraînent à terme pour un attaquant des cibles privilégiées.

La détermination et les moyens mis en œuvre par les attaquants dépend de l'importance des conséquences qu'ils es comptent obtenir. L'ANSSI[7] estime que des organisations étatiques font actuellement du pré-positionnement stratégique : elles s'introduisent dans les réseaux industriels pour être capable de déclencher des attaques massives en cas de crise géopolitique. Des organisations terroristes chercheraient plutôt de manière opportuniste des sites vulnérables provoquant des effets visibles, des réseaux criminels cherchent à démontrer leur capacité à réaliser ces attaques pour vendre leurs services. Dans ce contexte, les exploitants de PME/TPE, acteurs qui n'ont ni les moyens ni l'expertise des grands groupes qui mettaient en œuvre les grosses installations, peuvent être des cibles d'attaque privilégiées.

(7) Conférence d'ouverture du FIC 2019.

Quoi faire pour prévenir ce risque ?

Pour prévenir ce risque, il est nécessaire en premier lieu d'étudier la possibilité qu'une cyber-attaque puisse engendrer des phénomènes dangereux pour l'homme et l'environnement par l'intermédiaire notamment des systèmes d'information et des SCADA. Il faut donc intégrer dans l'analyse des risques l'impact d'une cyber-attaque sur les installations physiques.

En deuxième lieu, il s'agit d'en évaluer la gravité, c'est-à-dire les conséquences éventuelles de ces attaques sur les biens, les personnes et l'environnement (estimation des rayons d'effets d'une explosion par exemple).

En troisième lieu, la vraisemblance de chaque scénario doit être étudiée sur la base notamment de la vulnérabilité des systèmes (systèmes informatiques, contrôle commande, interfaces avec les installations : capteurs et actionneurs), des installations et de leur environnement.

Enfin des mesures doivent être mise en place, si besoin, en fonction de la gravité et de la vraisemblance des scénarios d'attaques identifiés. Ces mesures peuvent, voire doivent, selon les cas, être une combinaison de mesures prises au niveau des systèmes d'information (conception d'une architecture plus facile à défendre, gestion des intervenants, protection par antivirus, pare-feu, etc.), de mesures physiques, humaines et/ou organisationnelles prises au niveau des installations physiques elles-mêmes (mise en place de barrières de sécurité physiques non connectées par exemple) ainsi que des mesures de détection et de traitement des incidents.

Les approches d'analyse des risques issues de la cybersécurité doivent ainsi être combinées à celles adoptées pour la maîtrise des risques accidentels, centrées sur les installations physiques et les phénomènes dangereux qu'elles peuvent générer.

Cette analyse des risques devrait être réalisée de façon globale en intégrant et en s'assurant de sa cohérence avec la prévention des risques d'intrusion et des risques accidentels intrinsèques à l'exploitation des installations.

Pour mettre en place ces différentes analyses et mesures, bon nombre des TPE / PME concernées devront être accompagnées par des prestataires externes dont il faudra s'assurer de la compétence.

Conclusion

Les cyber-attaques peuvent être, par la prise de contrôle d'équipements ou d'installations dangereuses, à l'origine de phénomènes dangereux ayant des effets dommageables sur le personnel, les riverains ou l'environnement. Pour raison de sécurité, il est nécessaire que ces conséquences soient prises en compte et que des mesures pertinentes soient mises en œuvre pour limiter les conséquences de telles attaques.

Au-delà de l'impact direct sur les personnes, une mauvaise prise en considération des cyber-attaques sur des équipements dangereux intégrés à des filières en cours de déploiement, avec des effets sur les personnes ou sur

l'environnement, pourrait avoir un impact très négatif sur ce processus. On peut penser notamment au déploiement actuel de la filière hydrogène en France[8] et le comparer à celui de la filière véhicule GPL qui s'est arrêté du fait de l'explosion d'un réservoir GPL dans un véhicule.

(8) Plan de déploiement de l'hydrogène pour la transition énergétique – MTES (source :https://www.ecologique-solidaire.gouv.fr/sites/default/files/Plan_deploiement_hydrogene.pdf).

L'AUTEUR

Sylvain Chaumette est expert en sécurité industrielle et responsable du pôle Analyse et Gestion Intégrées des Risques accidentels au sein de l'INERIS. Il a participé à la publication de nombreux guides qui font références dans le domaine de la prévention des risques industriels majeurs.

PME ET CYBERATTAQUES

LE CONSEILLER NUMÉRIQUE DE LA CCI EST AU CARREFOUR DES COMPÉTENCES

Par sa fonction, le conseiller numérique d'une CCI a une connaissance du maillage commercial et industriel de son département. Grâce aux documentations qui sont à sa disposition, à ses contacts avec ses collègues de la CCI et avec les responsables des entreprises, il peut évaluer la sensibilité de leurs activités et leur poids dans l'économie locale.

Ses visites sur site et ses entretiens avec les personnels des TPE ou des PME faciliteront sa perception des vulnérabilités de l'entreprise qu'elles soient humaines ou organisationnelles. Il trouvera alors l'essence de sa fonction dans le conseil et la capacité d'orienter les décideurs vers des organes institutionnels ou des professionnels détenant une réelle expertise de la sécurité économique. Fondamentalement, il s'agira de protéger les valeurs patrimoniales de l'entreprise en distinguant les priorités et en contenant les mesures dans un coût et une pratique professionnelle acceptables.

Conseiller numérique
au sein d'une CCI : une fonction émergente au regard d'une situation complexe

Par Jacques Tek

Propos recueillis par le rédacteur en chef de la Revue : Monsieur Jacques Tek, Conseiller numérique de la CCI d'un grand département de la région d'Ile de France, nous fait part de son expérience récente de conseil auprès des TPE et PME en matière de sécurité numérique.

La revue : pourriez-vous nous rappeler les fondamentaux de l'action d'une CCI ?

Jacques Tek : les Chambres de Commerce et d'Industrie (CCI) ont pour mission d'accompagner les entreprises présentes au sein de leur territoire, de la création d'entreprise, puisque les Conseillers CCI accompagnent et conseillent les créateurs d'entreprise, jusqu'à la transmission en passant par toutes les phases de croissance et de développement (innovation, international, développement durable, intelligence économique, développement commercial, financement et numérique).

JACQUES TEK

Conseiller numérique CCI de Seine et Marne

La revue : comment est née la fonction de Conseiller numérique au sein de la CCI ?

Jacques Tek : une réflexion régionale avec l'ensemble des CCI Paris Ile-de-France a été menée entre 2013 et 2016 sur l'apport du numérique au développement des entreprises. Elle prenait en compte la conscience d'une réelle « fracture numérique » au sein des TPE / PME de la région. Le résultat a été la mise place du programme régional « Les Digiteurs », accompagné d'un financement européen FEDER[1], visant doter chaque CCI de la région Paris Ile-de-France de Conseillers numériques.

(1) Le fonds européen de développement régional ou FEDER est un des fonds structurels qui visent à renforcer la cohésion économique et sociale au sein de l'union européenne en corrigeant les déséquilibres régionaux.

J'ai pris mes fonctions au sein de la CCI Seine-et-Marne, dans ce cadre, en mars 2017. Mon rôle a été immédiatement compris au sein de la CCI et surtout auprès des entreprises du territoire.

La revue : comment avez-vous progressivement investi les différents aspects de votre nouvelle mission ?

Jacques Tek : la première phase consiste à aller à la rencontre des entreprises de Seine-et-Marne (secteurs industries et services - les secteurs commerces et tourismes étant gérés par un autre service). Les contacts se font par sollicitation directe et par l'intermédiaire de l'ensemble des canaux de communication : publication sur le site internet de la Chambre, sur les réseaux sociaux, parutions d'articles dans des magazines et évènements organisés à la CCI.

Je réalise des diagnostics numériques auprès des dirigeants au sein de leur entreprise. Ces rendez-vous me permettent mieux comprendre le fonctionnement de l'entreprise, connaître ses ressources et son organisation me permettant ainsi d'identifier les axes qui peuvent être améliorés et/ou optimisés grâce au numérique : visibilité et communication avec le site web, la présence sur les réseaux sociaux, outils de planification des ressources de l'entreprise (ERP) et les logiciels relation client (CRM). La sauvegarde des données et donc l'aspect Cybersécurité est devenu est un axe très important : j'essaie de réaliser un travail de sensibilisation auprès du dirigeant sur les risques en formulant également des recommandations (sauvegardes des données en externe en mode Cloud, gestion des mots de passe, sensibilisation du personnel aux bonnes pratiques).

© Fotolia_79058628_Subscription_XXL

Un audit bien construit dans une relation de confiance permet de comprendre les flux organisationnels d'une entreprise et de saisir ses vulnérabilités dans le domaine numérique. C'est le premier pas d'une acculturation à la cybersécurité.

La revue : quels sont les freins de cette acculturation à la sécurité économique ?

Jacques Tek : la première cause est une absence de culture et de sensibilisation à la « sécurité informatique » et à la « protection des données ». J'estime qu'environ 10 % des entreprises ont perçu le risque cyber pour leurs activités et ont commencé à l'intégrer dans leurs processus de sauvegarde et de sensibilisation des risques auprès des collaborateurs. Pour les autres, la sensibilisation est infime et la conscience du risque est nulle.

La deuxième cause est relative au mode de croissance de ces entreprises. Passées d'un poste informatique à des petits

réseaux internes, le plus souvent avec sans ressource spécifique à l'informatique, ces entreprises en croissance ont construit leurs réseaux et leurs communications de manière « artisanale ». Elles ont souvent laissé des prestataires leur dicter, faute d'un discours interne cohérent, des solutions. J'ai pu noter une carence manifeste en matière de gestion des données et des sauvegardes. Il n'est pas rare que les sauvegardes de l'entreprise soient réalisées sur une clé USB ou un disque dur externe puis ramené le vendredi soir à son domicile par le dirigeant…

C'est une des raisons pour lesquelles j'accorde une place plus importante lors de mes entretiens sur la sécurité des données et que je m'efforce d'expliquer la notion de données sensibles et le caractère impératif des sauvegardes externes périodiques. Je conseille des solutions cloud françaises afin d'éviter que les données sauvegardées dans des data center ne soient régies par des législations étrangères. En effet, paradoxalement, certains chefs d'entreprises pensent que la délocalisation de leurs données sur un site externe à leur entreprise les prive de leur maîtrise et voient cela comme un danger. Ils préfèrent en conséquence des sauvegardes de proximité.

La revue : utilisez-vous pour fortifier vos analyses et vos communications les données de l'ANSII ou de plateformes gouvernementales ou nationales ?
Jacques Tek : Ma première priorité a été d'effectuer un premier tour d'horizon que j'ai réalisé au travers de l'audit et le conseil d'une cinquantaine d'entreprises du département.

J'ai exploré les publications de l'ANSII et la plate-forme cybermalveillance.gouv.fr. J'avais rencontré Jérôme Notin, son dirigeant, lors d'un colloque. J'en ai tiré un catalogue de références de bonnes pratiques que je compte délivrer aux dirigeants et cadres de TPE et PME par lettres électroniques, lors d'évènements et des réunions professionnelles. Je pense qu'il faut s'appuyer sur les ordres professionnels qui par leur connaissances « métier » ont une réelle prévalence en matière d'attention et de prescriptions pour instiller des pratiques d'hygiène informatique.

Du fait de ma position, je ne puis directement indiquer des prestataires de services aux entreprises. Cependant, je peux guider les décideurs vers des structures référencées par l'ANSII ou les plateformes nationales. France Num va dans ce sens.

L'AUTEUR

Jacques TEK est diplômé d'un MASTER Communautés virtuelles et management de l'intelligence collective via les réseaux numériques à l'Université de Limoges et d'une Licence en Marketing Digital à l'Université de Marne-la-Vallée.

Spécialisé et passionné par le digital, il est Conseiller numérique à la CCI Seine-et-Marne depuis Mars 2017.

PME ET CYBERATTAQUES

© Fotolia 45750cd Subscription

UNE MAITRISE DE L'ENVIRONNEMENT DE L'ENTREPRISE PAR UNE INTELLIGENCE STRATÉGIQUE

Chaque organisation ou entreprise agit au sein d'un territoire géographique ou virtuel en liaison avec des réseaux d'acteurs. Elle se doit de cartographier les opérateurs clés et les informations utiles afin de formaliser une démarche concrète d'*Intelligence Stratégique Localisée* qui ne néglige pas les interconnexions entre les secteurs économiques et sociaux.

La définition d'une stratégie des réseaux réside dans une approche définissant la vulnérabilité et la vigilance d'une organisation. Celle-ci repose sur une motivation des personnels pour gérer un reporting régulier de l'information utile et pour mettre en valeur des signaux faibles qui sont souvent les premiers éléments d'une menace ou d'une opportunité pour l'entreprise. Ces process de veille intègrent une approche de *Vision Périphérique* qui dépasse les métiers essentiels de l'entreprise pour saisir les nouveaux flux informationnels et technologiques qui peuvent rapidement modifier l'environnement d'une entreprise et mettre en danger son activité.

L'intelligence stratégique
localisée au service du territoire

Par Patrice Schoch

Certaines organisations présentent une vision étriquée et très focale de leur stratégie. Cette attitude conduit généralement à ne pas se préoccuper de signaux faibles ou de réseaux pourtant pertinents, pouvant permettre la détection d'opportunités ou de menaces dans leurs environnements. Le Relevant Network présente un intérêt novateur dans le domaine de la gestion des réseaux pour définir les plus pertinents à développer pour atteindre les objectifs fixés ou sécuriser l'activité. Compte tenu des interconnexions entre acteurs d'un même territoire, il est possible d'envisager un modèle d'Intelligence stratégique localisée qui serait applicable à tout type d'organisations (privées ou publiques, économiques ou non marchandes).

PATRICE SCHOCH

Projet Activ'Links
Institut de l'Ouest Droit et Europe
Chef d'escadron de gendarmerie (RC)

L'intelligence stratégique (IS) regroupe l'ensemble des pratiques managériales de gestion de l'information, de protection et d'influence, afin de permettre à tous les acteurs d'un territoire d'atteindre leurs objectifs. Compte tenu de leur nature et de leurs missions diversifiées, il est essentiel de considérer leurs interconnexions. La défaillance d'un acteur impacte nécessairement ceux qui lui sont limitrophes. Par exemple, si une entreprise dépose son bilan, il faut envisager son impact sur les autres entreprises, la population, les territoires, les services publics, les transports, etc. Si les différences entre certains acteurs (*publics/privés*) suscitent souvent des préjugés et des oppositions, force est de constater que les uns dépendent mutuellement des autres. Négliger les interconnexions entre les secteurs (*économiques, sociaux, politiques et publics*),

c'est à terme, prendre le risque de créer des dysfonctionnements futurs.

Quel que soit le secteur, chaque organisation évolue sur un territoire avec une multitude de réseaux d'acteurs. Il est essentiel d'être en capacité de sélectionner ceux qui sont pertinents dans un environnement afin d'établir une démarche planifiée d'actions. Parler uniquement de veille[1], c'est finalement faire peu de cas de l'origine même de l'information et du dédale que représentent les réseaux humains. Pour chaque organisation, territoire, mission et objectif, il existe un ou plusieurs réseaux de contacts pertinents. C'est ce que nous avons appelé *Relevant Network*[2] *ou Réseau pertinent d'influences*.

(1) Ensemble des pratiques de recherches, traitement et de gestion des données et des informations utiles à l'organisation.

(2) Relevant Network : Réseau Pertinent formalisant l'ensemble des contacts et liens utiles favorables à l'aboutissement des objectifs de l'organisation. La notion de pertinence souligne ici l'utilité d'entretenir certains liens. Le choix d'un terme anglais s'explique par la simplicité et la clarté du terme

La prise en compte de l'approche humaine par les réseaux identifiés

Depuis les années 1970, un certain nombre de chercheurs ont mis en exergue l'importance de l'être humain comme source d'information utile (*Cleland & King, 1975*). W.J. KEEGAN a démontré, en 1974, que 67% des informations avaient une origine humaine (Keegan, 1974). Bien que le développement de l'internet et des réseaux sociaux virtuels ait apporté une nouvelle donne dans la recherche d'information, il est apparu que le rôle des fonctions opérationnelles sur le terrain pouvait être décisif (*Carbonnel & Dorrance, 1973*).

La motivation des individus est la clé de voûte pour s'assurer d'un reporting régulier et fiable de l'information utile (*Thiétart & Vivas, 1981*). L'implication des fonctions opérationnelles et territoriales est une réponse à la détection de signaux faibles dans l'environnement d'une organisation. Ils constituent des informations infimes qui, mises bout à bout, permettent de détecter une menace ou une opportunité pour l'activité de l'organisation (*Le Bon, 2006*).

Il est nécessaire de préciser la portée de la notion d'influence. Le modèle de l'A.F.D.I.E. (*Association Française pour le Développement de l'Intelligence Economique*) définit l'influence comme le processus qui, à l'initiative d'un organisme, vise à modifier favorablement les interactions de celui-ci avec son environnement. Il est important de souligner que l'influence, et d'une manière générale la gestion des réseaux, peuvent prendre des formes très variées. L'action peut très bien viser l'influence sur le comportement d'un consommateur, sur ses concurrents, sur l'opinion publique, l'obtention d'un marché public, etc. L'influence peut également revêtir une forme plus solennelle comme l'influence politique, autrement

dit le lobbying. Il est essentiel de lier la gestion des réseaux publics et celle des réseaux privés, afin de bénéficier d'une stratégie et d'une vue d'ensemble.

L'approche innovante de la vision périphérique

La définition d'une stratégie concomitante des réseaux doit reposer nécessairement sur une approche permettant de définir la vulnérabilité et la vigilance d'une organisation. Cela permet de structurer, de manière pertinente, le *process* de veille et d'établir une stratégie de réseaux. Pour ce faire, il a été nécessaire d'y intégrer l'approche de Vision Périphérique développée par George S. Day et Paul J.H. Schoemaker (*Day & Schoemaker, 2006*).

Pour mettre en exergue leur théorie sur la *Vision Périphérique*, ces chercheurs ont réalisé un parallèle intéressant entre la vision d'une organisation et celle d'un œil humain. Contrairement à l'œil humain qui bénéficie d'un spectre périphérique très large, « l'œil » d'une organisation consacre majoritairement ses ressources organisationnelles à une vision focale, pouvant mettre à mal son avenir. Se concentrer uniquement sur son activité et son organisation créé une vulnérabilité liée au fait de ne pas détecter les signaux faibles venant d'un environnement plus éloigné : *la Périphérie*.

La Périphérie est définie comme « *partout où l'attention n'est pas* ». Elle n'est pas une région fixe et localisable dans l'environnement externe. Ces auteurs précisent que : « *la périphérie est toujours élusive. Chaque fois que vous tournez la tête pour la regarder, vous créez une nouvelle périphérie.* » *(Day & Schoemaker, 2006*). Quand vous changez votre modèle économique, social ou politique vers une nouvelle direction, vous créez de nouveaux angles morts dans d'autres directions.

L'estimation de la vulnérabilité et de la vigilance d'une organisation repose sur cinq éléments déterminants : la direction, la manière dont la stratégie est définie, le management de la connaissance, l'organisation et la culture. (*Day & Schoemaker, 2006*)

Ainsi, une organisation rigide et conformiste ne s'intéressant qu'à des données extérieures standards, se focalisant exclusivement sur ses performances et celles de ses concurrents, est présentée comme une organisation fragile. Cette vulnérabilité s'explique par une vision étriquée et rigide des informations venant de l'environnement. George S. Day et Paul J.H. Schoemaker recommandent donc de développer certaines qualités intrinsèques pour que l'organisation soit plus vigilante : *curiosité, flexibilité stratégique, collecte et partage des signaux faibles, ouverture sur le cœur et la périphérie de ses activités*.

Les auteurs Humbert et Nicolas Lesca, dans le cadre de leur recherche sur la détection des signaux faibles ont présenté, en 2009, quatre types d'obstacles à l'identification précoce de signaux faibles, liés aux organisations :

– la *force du court terme* reposant sur un mécanisme d'aveuglement fondé sur la rentabilité à court terme de chaque agent de l'organisation,

– la *force du quantitatif* fondée sur l'unique valorisation de données quantifiées et financières, au détriment des données humaines et qualitatives, uniques sources de signaux faibles,

– la *croyance qu'il suffit de poser une question pour obtenir la réponse* sans tenir compte de l'importance des retours d'expériences,

– l'*habitude d'avoir raison reposant sur un mécanisme psychologique de filtration des signaux faibles par les responsables*. A ce titre, les auteurs rappellent qu'observée de l'extérieur, *cette attitude est qualifiée de manque de vigilance, de myopie, voire d'attitude arrogante ou d'attitude de mépris. […] Ces signaux sont, par contre, parfaitement perçus par les responsables de proximité*.

Ce constat entre en résonance avec la notion de Cécité au changement qui se définit comme la défaillance d'observateurs à détecter des changements importants et soudains dans un dispositif visible. En favorisant une meilleure gestion des réseaux pertinents, ce Relevant Network permet d'accroître la possibilité de mieux connaître et évoluer dans son environnement.

Une intelligence stratégique localisée en faveur d'une prospective et d'une sécurité territoriale

Ainsi en formalisant une approche et des cartographies qui permettent d'identifier les acteurs clés et les informations utiles pour une organisation sur son territoire d'action, il est possible de formaliser une démarche concrète d'Intelligence Stratégique Localisée.

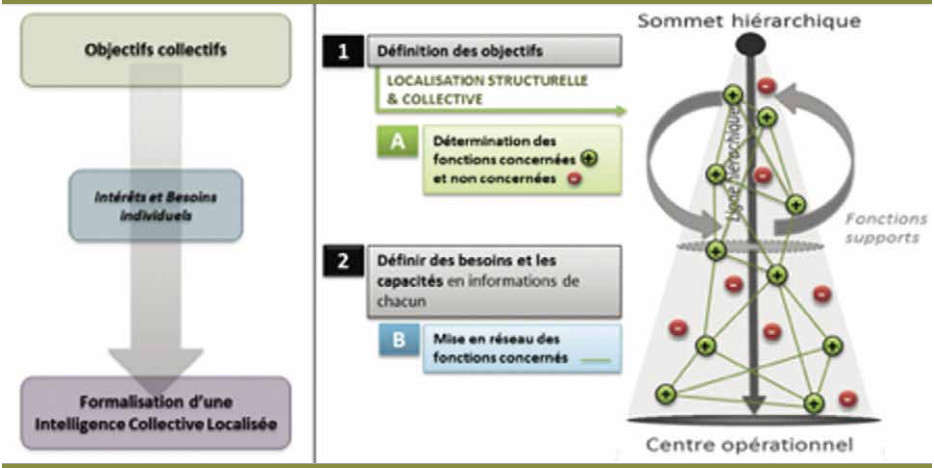
Nous définissons cette démarche créée comme :

– *l'utilisation et la localisation stratégique, opérationnelle et territoriale des pratiques informationnelles de veille, de protection et d'influence,*

– *par la mise en commun de ressources matérielles et humaines précises,*

– *en vue de capter et sélectionner les signaux faibles utiles,*

– *et d'agir de manière ciblée sur les réseaux publics et privés identifiés,*



Intelligence Stratégique Localisée – L'approche structurelle – Patrice Schoch – 2013.

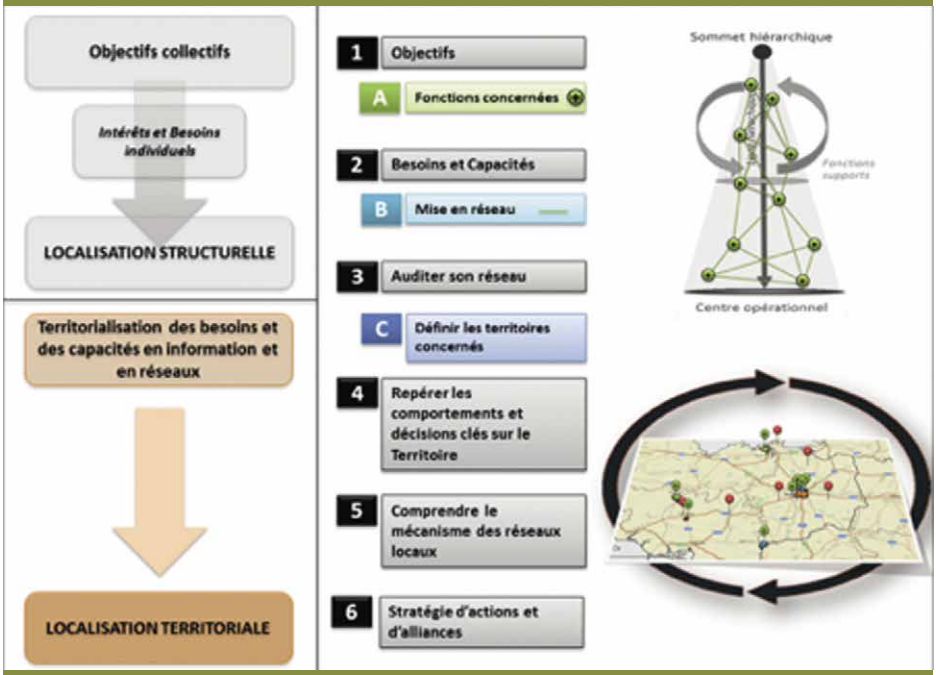
© Patrice Schoch

– *permettant l'atteinte des objectifs et la sécurisation de l'organisation, quelle que soit sa finalité intrinsèque.*

La gestion de la veille et des réseaux nécessite un investissement important, parfois très chronophage. Il convient de les structurer en localisant précisément les informations, les fonctions clés et les interlocuteurs extérieurs réellement utiles à l'atteinte des objectifs fixés. La démarche prend en compte les objectifs collectifs de l'organisation et détermine l'ensemble des fonctions concernées dans la structure.

Le recensement des besoins et des capacités de chacun au niveau informationnel permet, dans un second temps, de formaliser une *Intelligence Collective Localisée*, en mettant en réseaux les fonctions clés (figure 1).

La localisation stratégique repose sur la territorialisation précise des besoins et des capacités en information et en réseaux. L'étendue du territoire dépend, bien entendu, de l'ampleur des objectifs, du secteur d'activité et du degré de précisions que veut appliquer la direction de l'organisation.



Intelligence Stratégique Localisée - L'approche territoriale – Patrice Schoch – 2013.

© Patrice Schoch

Cette approche de gestion de l'information et des réseaux humains offre une opportunité réelle à toutes les organisations, privées comme publiques, marchandes ou non, de connaître et de comprendre les autres acteurs d'un même territoire. Cette compréhension permet d'optimiser leur approche managériale et ainsi de pouvoir entreprendre toutes les actions nécessaires à la bonne atteinte de leurs objectifs et à la sécurisation de leur activité.

L'intelligence stratégique localisée, tout comme le relevant network management, peut être intégrée dans une politique territoriale en intervenant sur plusieurs axes :

– Sensibilisation des acteurs territoriaux,

– Mise en place d'un dispositif d'accompagnement sur la détection des opportunités et des menaces territoriales,

– Intégration d'un cohérence territoriale des actions en facilitant les liens entre acteurs privés et acteurs publics.

Bibliographie

– Carbonnel, F., & Dorrance, R. Information sources for planning decisions. *California Management Review N°4*, P. XV., 1973

– CIADT. *Pour une nouvelle politique industrielle : la stratégie des pôles de compétitivité*, 2004.

– Cleland, D. ; King, W. *Competitive business intelligence systems. Business Horizons*, 1975

– D2IE, OEC, CCI France. *Le guide de l'intelligence économique* - Guide du routard. Paris : Hachette, 2012.

– Day, G. S. ; Schoemaker, P. J. *Peripheral vision : Detecting the Weak Signals That will Make ou break your Company. Harvard Business School Press*, 2006.

– Day, G.S. ; Schoemaker, P. Peripheral Vision : *What's that you see ? Associations Now*, (pp. 64 - 70), 2006.

– Diallo, A. *Méthodes techniques et outils. Documentaliste - Sciences de l'Information*, 2010/3 Vol.47, pp. 12-17, 2010.

– Ducrey, V. *Guide de l'influence*, Eyrolles, Paris, 2010.

– François, L. *Intelligence Territoriale, l'intelligence économique appliquée au territoire*. Paris : Lavoisier, 2008.

– Guillemot, D., & Jeannot, G. *Travail du Public, travail du Privé : similitudes et différences - Premiers apports de l'enquête « Changement organisationnel et informatisation »*. Revue française d'administration publique - n° 132, pp. 789-803, 2010.

– Harbulot, C. ; Springuel A. Stratégie, contrôle et influence, Centre d'Études et de Recherche en Gestion d'Aix-Marseille, septembre 2009.

– IAE-Orléans, & DIGIMIND. *Baromètre 2007 des pratiques de veille des grandes entreprises françaises - Étude de marché 2007*. Consulté le décembre 2010, 2010, sur wikiwix.com : http://wikiwix.com/cache/?url=http://digimind.fr/actu/publications/etudes-de-marche/341-barometre-2007-des-pratiques-de-veille-des-grandes-entreprises-francaises.htm&title=%5B1%5D

– Juillet, A., & Racouchot, B. *Les stratégies d'influence ou la liberté de l'esprit face à la pensée convenue*. R2IE 4, 89-102, 2012.

– Keegan, W. *Multinational scanning : a study of the information sources utilized by headquarters executives in multinational companies*. Administrative Science Quaterly, p. 19, 1974.

– Larivet, S. *L'intelligence économique : un concept managérial*. Market Management (Vol.6), pp. 22-35, 2006.

– Le Bon, J. *La force de vente et les activités d'intelligence économique*. Revue française de gestion- n° 163, pp. 15-30, 2006.

– Lesca, H., & Lesca, N. *Méthodes heuristiques d'entraînement à la détection des signaux faibles*. Revue internationale de Psychosociologie - n° 37 (Vol. XV), pp. 135-160, 2009.

– Marsan, C. ; Daverio, F. *Communication d'influence*, CFPJ, Paris, 2009.

– Martre, H. (1994). *Intelligence et Stratégie des entreprises - Œuvre collective du Commissariat du Plan*. Paris : La Documentation Française, 1994.

– MEDEF. *Réinventer la croissance-Agir ensemble pour une dynamique économique*, MEDEF, Paris, 2013.

– Ministère de l'économie et des finances – Service de coordination à l'Intelligence Economique – République Française. *scie*. Consulté le 02 05, 2015, sur economie.gouv.fr : http://www.economie.gouv.fr/scie

– Pautrat, R. *Prospective des dispositifs nationaux d'Intelligence économique* - De l'intelligence économique à l'Économie de la connaissance. Economica, 2003.

– Thiétart, R., & Vivas, R. *Strategic Intelligence Activity : The Management of the Sales Force as a source of Strategic Information*. Strategic Management Journal, Vol.2, pp. 15-25, 1981.

– Wilensky, H. *Organizational Intelligence : Knowledge and Policy in Government and Industry*. Basic Books, 1967.

L'AUTEUR

Patrice SCHOCH, chef d'escadron de la réserve citoyenne de la gendarmerie, docteur en Sciences de gestion, est consultant en intelligence stratégique et influence. Il est dirigeant d'Activ'Links et chercheur associé (Laboratoire IODE – UMR CNRS 6262 – Université de Rennes 1).

Patrice SCHOCH élabore des stratégies de réseaux et d'intelligence économique et stratégique pour aider les organisations (privées comme publiques) à développer leur activité en tenant compte des spécificités des territoires. Il développe avec ses partenaires, une technologie permettant d'optimiser la gestion des réseaux d'influences online et offline en tenant compte des objectifs opérationnels et territoriaux d'une organisation. Ce projet Activ'Links a été soutenu par la Technopole Rennes Atalante et l'incubateur Emergys.

Au titre de ses travaux de recherche appliquée dédiées à l'Intelligence Stratégique Localisée et in fine au Relevant Network Management, un projet de recherche est actuellement en cours autour du Darwinisme organisationnel et stratégique ou comment optimiser la vision stratégique d'une organisation privée comme publique face aux changements sociétaux.

DOSSIER

Un accompagnement face à la menace

Le cyberespace

ou un nouvelle représentation des équilibres géostratégiques et économiques

Par Stéphane Mortier

Tout le monde en parle, elle évoque quelque chose à chacun d'entre nous mais nous ne la maîtrisons pas… Elle nous emmène dans des mondes inconnus, mystérieux, impalpables mais nous y évoluons quotidiennement… Elle nous fait peur, suscite des craintes mais nous en avons besoin… La CYBER ! Nous y sommes : science-fiction et réalité ont fusionné. Notre environnement s'est adjoint une part de virtuel empreint d'infini et de bouleversements cognitifs. De nouveaux paradigmes guident la raison, redessinent le monde et repensent la guerre ! Bienvenue dans le cyberespace…

STÉPHANE MORTIER

Gendarme
Section sécurité économique et protection des entreprises
DGGN

Nous n'avons aucune prétention, en quelques lignes, de refonder la pensée humaine dans un nouveau monde qu'elle a elle-même créé. Nous avancerons simplement quelques pistes de réflexion sur le monde tel qu'il évolue, sur les réalités mouvantes d'aujourd'hui et sur la façon dont les entreprises doivent composer et évoluer avec ce monde nouveau.

Cyberespace ? Où sommes-nous ?

Le cyberespace n'est ni un espace géographique, ni un monde physique, ni un territoire au sens premier du terme. Il constitue un système complexe de représentations qui s'enchevêtrent, s'agrègent, s'opposent et contiennent un peu de notre monde, de nos réalités physiques.

Le terme « cyberespace » apparaît en 1984, dans le roman de science-fiction « Neuromancien », écrit par William Gibson : « Une hallucination consensuelle vécue quotidiennement en toute légalité par des dizaines de millions d'opérateurs, dans tous les pays, par des gosses auxquels

on enseigne les concepts des mathématiques... Une représentation graphique de données extraites des mémoires de tous les ordinateurs du système humain. Une complexité impensable. Des traits de lumières disposés dans le non-espace de l'esprit, des amas et des constellations de données. Comme les lumières de villes, dans le lointain... »

Cet ouvrage de science-fiction appartient au genre littéraire appelé « cyber-punk » dont Gibson est considéré comme le fondateur. Il décrit un monde violent, sombre, proche de l'apocalypse et où la technologie informatique et l'intelligence artificielle sont au cœur du fonctionnement de la société. En ce sens, ce genre littéraire est proche de la dystopie. Cette dernière recouvre une société imaginaire organisée de telle façon qu'elle empêche ses membres d'atteindre le bonheur. L'objectif des auteurs de ces courants littéraires est de mettre en garde le lecteur sur les possibles évolutions de notre monde réel. À titre d'exemple, d'autres romans tels que « Le meilleur des mondes » d'Aldous Huxley (thématique du clone) ou « 1984 » de George Orwell (thématique de la surveillance de la société et des individus – Big Brother) entrent dans cette catégorie et nous éclairent sur des pratiques qui hier relevaient de la science-fiction mais qui font désormais partie de notre quotidien ! Si le genre littéraire tient de la dystopie, pour d'autres, le cyberespace tient de l'utopie. En effet, un espace sans frontières, ni contrôle, ni contraintes pourrait être le « meilleur des monde » !

Au regard de cette vision idéalisée du cyberespace, la société de l'information est portée en véritable projet politique. Il faut rappeler qu'elle a vu sa consécration dans le même temps que les bouleversements géopolitiques engendrés par la fin de la Guerre froide. Ces deux événements créent le terreau sur lequel se développera le « cybermonde ». Notons que ces deux évènements sont également à l'origine du développement de l'intelligence économique en France et de sa consécration dans le Rapport Martre en 1994. Le projet des autoroutes de l'information (Global Information Infrastructure) porté par Al Gore aux États-Unis en 1993-1994 confirmera cette tendance. Ce dernier déclara d'ailleurs devant l'Union internationale des télécommunications en 1994 : « *La Global Information Infrastructure(GII) ne sera pas seulement une métaphore de la démocratie en fonctionnement ; elle encouragera dans la réalité le fonctionnement de la démocratie en rehaussant la participation des citoyens à la prise de décision. Elle favorisera la capacité des nations à coopérer entre elles. J'y vois un nouvel âge athénien de la démocratie forgée dans les forums que la GII créera.* »

Au fantasme de rapports sociaux harmonieux permis par l'Internet répond la crainte que la technologie ne dépasse l'humanité et conduise à l'avènement

d'un Big Brother ultime. Deux visions s'affrontent donc, l'une utopique, l'autre dystopique !

La représentation d'un cyberespace généré par les infrastructures de communication comme un espace de liberté, un facteur de progrès économiques et sociaux et un symbole même de la démocratie a été largement mobilisée dans le discours américain relatif à la gouvernance de l'Internet. Celle-ci est assurée par divers acteurs impliqués dans son fonctionnement, c'est là une avancée majeure : l'État et la société civile et par extension le monde économique gouvernent l'Internet.

Pourtant, deux visions de cette gouvernance de l'Internet s'opposent : celle d'un cyberespace libre (comme dans le discours aux États-Unis) et celle liée au contrôle de l'information dans le cyberespace (comme cela est pratiqué en Russie et en Chine entre autres). En effet, la représentation d'un cyberespace comme espace de liberté est un outil puissant de la stratégie américaine pour contrecarrer les velléités russes et chinoises de contrôle du réseau et surtout pour conserver leur position dominante dans la gouvernance de l'Internet[1]. Ces enjeux de puissance américaine se retrouvent dans tout le spectre de l'intelligence économique, l'extraterritorialité du droit des USA et un positionnement dans le cyberespace.

La tension entre ces deux visions pourrait dégénérer en un nouvel affrontement géopolitique si l'on laisse libre cours aux discours caricaturaux et si l'accent n'est pas mis sur des objectifs communs sur le fond : généralisation de l'accès, préservation de l'interopérabilité globale et équilibre entre accès à l'information (liberté d'accès et d'expression), protection de la vie privée (voir le récent Règlement Général sur la Protection des Données - RGPD) et exigences de sécurité (cybersécurité). Ces objectifs communs et leur réalisation sont une des conditions de survie de notre système et de nos économies.

La représentation libertaire et utopique consacre le cyberespace comme une entité virtuelle mais bien réelle... Pas de distance, pas de frontières, le cyberespace contribuerait à dissoudre « tout ce qui gêne (le territoire, les institutions, notamment l'État, et le corps physique) tout en restant un espace que se disputent les États… ». C'est dans ce contexte que doivent évoluer les entreprises et qu'elles doivent maîtriser pour

(1) De 1998 à 2016, l'Internet Corporation for Assigned Names and Numbres (ICANN), en charge de la gestion et de la normalisation de l'adressage sur internet, dépendait du Département du Commerce des États-Unis (National Telecommunications and Informations Administration). Depuis le 1er octobre 2016, une Assemblée générale composée de quatre collèges peut bloquer les décisions du Conseil d'administration :

Secteur privé : il réunit des acteurs comme les GAFA, de grandes entreprises et des PME ;
- La communauté technique ;
- Les gouvernements : composés de 160 membres avec une voix chacun ;
- La société civile : les associations de consommateurs, de défense des libertés.

maintenir ou accroître leur compétitivité. La maîtrise de ce monde mi-réel, mi-virtuel, totalement technique et informationnel est une condition de la survie des entreprises et de nos sociétés.

La « déclaration d'indépendance du cyberespace » rédigée par John Barlow[2], en 1996, est l'élément le plus fort de cette représentation. Elle est, à plus d'un titre, évocatrice. En effet, elle s'apparente clairement à une nouvelle idéologie fondée sur un espace virtuel, infini et impalpable et surtout, en opposition au monde physique partagé entre États-Nations qui ne sont ni les bienvenus ni capables de maîtriser le cyberespace :

(2) Poète et militant libertarien américain décédé en 2018, co-fondateur de l'Electronic Frontier Foundation (ONG dédiée à la défense de la liberté d'expression sur internet).

« *En Chine, en Allemagne, en France, à Singapour, en Italie et aux États-Unis, vous essayez de confiner le virus de la liberté en érigeant des postes de garde aux frontières du Cyberespace. Il se peut que ceux-ci contiennent la contagion quelque temps, mais ils ne fonctionneront pas dans un monde qui sera bientôt couvert de médias numériques* ».

En 1996 déjà, « l'infobésité » préfigurait les difficultés que rencontrerait le monde physique quant à sa capacité à gérer les quantités croissantes et exponentielles d'informations mises à disposition, tant par les acteurs institutionnels que par les acteurs économiques ; une nouvelle fois, le lien entre développement du cyberespace et de l'intelligence économique est clairement établi. Autre exemple de ce lien, la déclaration dispose que « *vos industries de plus en plus obsolètes se perpétueraient en proposant des lois, en Amérique et ailleurs, qui prétendent décider de la parole elle-même dans le monde entier* ». Ne faut-il pas, à nouveau, y voir un lien avec cet outil de guerre économique que représente l'extraterritorialité du droit américain et l'explosion des cas de harcèlement en contentieux dont sont victimes nos entreprises européennes ?

Ce rejet du monde physique, avec son organisation, son économie, sa société… impose des réflexions importantes sur ce que seront le monde de demain et sa gestion. De nouveaux paradigmes pointent à l'horizon. Comment les décideurs, les États, les entreprises s'y adapteront-ils ?

Quelle maîtrise de ce nouvel espace ?

Actuellement, les réponses sont diverses et systématiquement empreintes des pratiques propres au monde réel, physique. Face aux développements et à l'augmentation de la cybercriminalité et des menaces, les États cherchent à affirmer leurs frontières et leur souveraineté dans cet espace afin d'assurer leurs missions traditionnelles :

- la protection de leurs citoyens ;

- la sécurité de leur territoire ;

- la protection de leurs intérêts ;

- la protection de leur régime politique.

Le cyberespace représente donc pour les dirigeants des États un véritable défi car il remet en question l'exercice de leur pouvoir et de leur autorité. Or, le cyberespace est un territoire d'un autre genre qui ne peut être abordé selon une pensée traditionnelle. La maîtrise du cyberespace demande donc une façon de penser qui sorte des sentiers battus, une autre vision du monde et de son organisation, une véritable réflexion sur la notion de frontières (avec ses implications – sécuritaires, fiscales, de nationalité,…). C'est le mode de réflexion qui est à repenser pas le monde en tant que tel. Il est impossible d'aborder le cyberespace comme on aborde l'aménagement du territoire ou une politique publique de soutien au développement économique, faute de quoi il ne sera jamais maîtrisé.

La véritable question, problématique, est de savoir si cette prise de conscience et cette évolution du mode de pensée peuvent être concomitantes chez les représentants et les décideurs des États et chez les acteurs économiques. Effectivement, une entreprise qui assimilerait les nouveaux paradigmes induits par le cyberespace, sans frontières apparentes comme traditionnellement admises dans le monde physique, se heurterait violemment à la législation fiscale de son lieu d'établissement par exemple. La réflexion est donc à mener en commun : États et entreprises.

En France et dans le monde, cette démarche de réflexion approfondie sur une vision nouvelle de l'État, de son organisation, de son fonctionnement, de ses politiques publiques,. au regard des évolutions du monde et plus particulièrement de la prépondérance du cyberespace dans la vie quotidienne n'a pas ou peu vu le jour. Ne faut-il pas voir, au-delà de la société de l'information (infobésité, réseaux sociaux, fake news, attaques informationnelles, leaks, lanceurs d'alerte...) dans le volume des migrations dans le monde, dans les nouvelles formes de contestation, dans le recours de plus en plus systématique à l'optimisation fiscale, dans les nouvelles formes de prédations économiques, dans le rejet même parfois de la chose publique, autant de signaux faibles d'une volonté, probablement inconsciente, de mener cette réflexion de fond ?

AUTEUR

Stéphane Mortier, gendarme, affecté à la section sécurité économique et protection des entreprise de la DGGN. Diplômé en sciences politiques, en sociologie et en politique internationale de l'Université libre de Bruxelles, il est également diplômé de l'École de Guerre Économique et termine un doctorat en sciences de gestion à l'Université Paris 1 Panthéon-Sorbonne.

Il a publié : Au coeur de l'unité africaine, le droit OHADA – Harmonisation du droit des affaires et intelligence économique, Uppr, 2017.

La donnée valorisée
ou le trésor d'une entreprise

Par Denis Millard

Propos recueillis par le rédacteur en chef de la Revue : Monsieur Denis Millard nous fait part dans cette interview de son expérience d'une cyberattaque de son entreprise. Son contexte reflète l'état de l'art des petites et moyennes entreprises en la matière. C'est la raison pour laquelle nous avons voulu partager cette réflexion.

La revue : pourriez-vous situer le niveau d'expertise de votre entreprise et son métier.

Denis Millard : nous sommes un cabinet de géomètres-experts. Notre clientèle est diverse et peut se distinguer techniquement entre les particuliers, des professionnels de l'immobilier et les collectivités territoriales.

DENIS MILLARD

Directeur. Cabinet de Géomètre-Expert

L'essentiel des prestations servies aux particuliers concerne des bornages ou des divisions de propriété. Elles donnent lieu à la délivrance classique de devis avant acceptation et exécution de la prestation et de sa contrepartie numéraire. Notre fichier client ne contient que des informations techniques relatives à la prestation.

Les collectivités territoriales et les professionnels utilisent nos compétences pour des projets d'aménagements urbains, de création de lots à bâtir, de lotissements, ainsi que la mise en copropriété d'immeubles. Ces services sont régis par les classiques appels d'offres ou des commandes directes suivant l'ampleur et le coût des prestations. Ce fichier client contient donc les données des interlocuteurs des collectivités territoriales et des acteurs associés à ces tâches : syndic, promoteurs, maîtres d'ouvrage, etc.

La revue : quelles valeurs mobilières détenez-vous ?

Denis Millard : en fait, nous ne détenons pas de brevets comme une start-up ou un prestataire de services sur une surface concurrentielle intense et technologique mais nous usons

d'un savoir-faire spécifique. Nous utilisons un fichier client lié à des prestations qui n'ont pas de dimension particulière et qui suivent l'organisation classique de notre métier et des prescriptions de notre Ordre. Les données financières et comptables, les devis, les appels d'offre et marchés publics, le fichier client relèvent donc d'informations sensibles dans le sens où elles doivent être impérativement disponibles pour exercer notre métier.

Notre force réside essentiellement dans la qualité de la prestation et dans la réactivité quant aux attentes de nos clients. Nous n'avions donc pas conscience de détenir des informations qui auraient pu susciter un intérêt pour des prédateurs du cyberespace.

© Fotolia_70768033_© Creativa L

Les protocoles mis en œuvre par les hackers visent l'exploitation de vulnérabilités qui permettent l'exploitation des données valorisées d'une entreprise. Celle-ci n'a pas toujours conscience du fait de sa situation de cible potentielle.

La revue : comment s'est structurée votre entreprise sur le plan informatique et de gestion des données.

Denis Millard : notre démarche a été très classique. Initialement, chaque collaborateur avait une station de travail. Très rapidement, pour des questions de cohérence, de continuité dans les travaux et de partage d'informations, nous avons adopté une configuration en réseau.

Le choix a été délicat car les commerciaux en matière de réseaux sont nombreux, agressifs et tentent d'imposer des solutions pas toujours adaptées aux besoins d'une entreprise. De plus, les solutions proposées rendent l'entreprise captive d'une configuration et de ses maintenances souvent onéreuses.

Nous avons fait appel donc à un prestataire extérieur local connu sur la place et nous avons fait évoluer notre configuration au fur et à mesure de l'apparition de nouvelles fonctionnalités, méthodologies ou dispositions juridiques.

La revue : comment avez-vous anticipé le risque cyber ?

Denis Millard : initialement, notre réflexion nous a porté à adopter une protection classique par Firewall et antivirus. Il nous est ensuite apparu utile d'orienter nos données sur deux serveurs différents. Nos données sont sauvegardées simultanément sur un serveur local et sur le Cloud. Nous avons déterminé des rythmes de sauvegarde de données selon leur nature (quotidienne, hebdomadaire et mensuelle).

Nous avons divisé les accès aux données sous un double niveau : Une fonction de direction dévolue à mon adjoint et moi-même et un niveau de maîtrise dédié à mes autres collaborateurs.

Nous n'offrons pas d'accès client à nos bases de données. Les contacts clients sont réalisés essentiellement par messagerie, voie postale ou téléphonique. Nous n'avons donc pas eu à verrouiller notre base.

Nous n'avons pas intégré l'émergence des objets connectés et de configurations personnelles utilisées au domicile et au travail. Ces vecteurs portent des vulnérabilités mais sont incontournables pour faciliter le travail de mes collaborateurs. Nous n'avions pas non plus anticipé un usage personnel des configurations pour des séquences ludiques. Nous avons toutefois sensibilisé les collaborateurs de l'entreprise lors des réunions de travail à une hygiène de sécurité. Ces réunions nous permettent de distiller une information régulière sur la question du Phishing, de l'authentification des interlocuteurs et des escroqueries classiques liées à la gestion des mails.

La revue : êtes-vous informés des outils mis à disposition par l'ANSII, de plates-formes d'assistance à la cyber malveillance et sur les obligations liées au RGPD.
Denis Millard : notre information est parcellaire du fait de notre de travail qui mobilise l'essentiel de notre temps et de notre méconnaissance de canaux qui peuvent nous sensibiliser à ces vecteurs d'information.

Notre approche du RGPD a été faite essentiellement par les éditeurs de logiciels et des communications réalisées par l'Ordre des Géomètres-Experts. Nous avons bien compris le caractère essentiel de la protection des données personnelles.

La revue : quelles ont été les modalités de la cyberattaque que vous avez subie ?
Denis Millard : Selon notre prestataire de service, par l'intermédiaire d'un robot, les agresseurs ont testé avec succès les mots de passe de notre réseau.

Le lundi matin, lors de la mise en œuvre de nos outils informatiques, un message nous informait que les données de l'entreprise étaient cryptées et que leur récupération était sujette au paiement d'une somme sur un portefeuille Bitcoin.

Notre premier acte a été de débrancher toutes les stations et nous avons fait appel à un prestataire. Il est très vite apparu que le vendredi soir, un pirate a testé notre mot de passe qui était trop faible. Son dispositif logiciel a neutralisé notre antivirus, repéré nos données et les a cryptées.

Nous avons exclu de verser une rançon pour obtenir une restitution de nos données pour deux raisons : la première est liée au caractère opaque de l'auteur de l'attaque et à l'absence de garanties du rétablissement

de l'accès aux données sans compter une naturelle aversion pour une pratique de chantage. La seconde résulte du fait que nous avons décidé de restaurer les configurations puis les données de travail à partir de nos sauvegardes.

Ces opérations ont été réalisées avec succès et nous n'avons perdu qu'une journée de travail. Il nous a fallu en fait 48 heures pour redémarrer réellement les services de l'entreprise si on prend en compte les vérifications des données et leur croisement avec les opérations du vendredi précédent.

La revue : quelles conséquences a eu cette cyberattaque pour votre entreprise une fois passé le stade de la restauration.
Denis Millard : nous avons eu une attitude transparente quant à nos clients que nous avons contactés par mail pour leur faire connaître cette attaque. Nous avons joint les responsables des collectivités territoriales avec qui nous travaillons habituellement. Nous avons eu un contact avec le responsable de la sécurité informatique de la CCI. Nous avons maintenant une couverture assurantielle pour faire face à ce risque. Nous avons pu utiliser cette phase difficile pour délivrer une information plus précise en matière d'hygiène informatique à mes collaborateurs.

La revue : quel doit-être selon votre expérience le meilleur canal d'information afin que vous puissiez mieux cerner et anticiper un risque informatique sur la base de votre métier ?
Denis Millard : nous avons déjà eu une réunion organisée par la mairie de Chelles et avec un commissaire de police qui avait surtout trait à la sécurité des entreprises. Elle ne permettait d'aborder le risque cyber que parmi d'autres problématiques telles que la protection des biens : stocks, accès, surveillance, etc.

Il me semble que des thèmes aussi précis et spécialisés doivent être traités par métiers. C'est la raison pour laquelle je militerais pour une information délivrée par l'Ordre des Géomètres-Experts et la chambre des métiers. Cela nous permettrait également de mieux connaître les possibilités et informations offertes par l'ANSII ou des plateformes dédiées à l'information et à l'assistance aux victimes de cybermalveillances. En effet, tant que l'on n'est pas directement concerné par ce phénomène de cybermenaces, on discerne mal au sein d'entreprises de taille moyenne toute l'architecture juridique et technologique qui sous-tend ce phénomène nouveau et évolutif.

AUTEUR

Denis Millard est ingénieur diplômé de l'Ecole Supérieure des Géomètres Topographes (E.S.G.T.) et de l'I.A.E. de Paris.

Il est Géomètre Expert depuis 1997 et dirige le Cabinet MILLARD, S.A.R.L. de Géomètres Expert basé à CHELLES (Seine et Marne).

France Num :

La transformation numérique des TPE/PME en action. Être accompagné et protéger son entreprise pour développer son activité

Par Aurélie Gracia Victoria

France Num, nouvelle initiative nationale pour la transformation numérique des TPE/PME agit concrètement pour la sensibilisation des entreprises à la sécurité numérique via des recommandations, des mises en contact avec des accompagnants et des aides mobilisables.

(1) La transformation numérique des TPE/PME, Etude IFOP du 30 avril au 25 mai 2018 de nature ethnographique (menée dans 22 entreprises de 1 à 100 salariés en France) doublée d'une enquête quantitative du 13 juin au 14 juillet 2018, auprès de 700 entreprises

AURÉLIE GRACIA-VICTORIA

Cheffe du bureau des usages du numérique. Direction générale des Entreprises (DGE)

Selon l'étude IFOP : la transformation numérique des TPE/PME[1], l'attente majeure des employés en TPE/PME vis-à-vis du numérique - après les gains de temps dans leurs activités professionnelles - relève de la volonté de sécuriser leur entreprise. Par ailleurs, les employés déclarent ne pas savoir comment agir pour la sécurité informatique mais ils indiquent suivre scrupuleusement les orientations sur le sujet formulées par leur direction.

Comprendre, sensibiliser et accompagner : protéger son entreprise doit revenir un réflexe

Cette étude, qui a pour objectif de montrer où en sont les organisations dans l'appropriation du numérique et de dresser des pistes d'amélioration, relate un exemple particulièrement parlant : une PME, traitant des données confidentielles de par son activité, possède une poubelle où l'on met tous les documents confidentiels à jeter et qui est descendue tous les soirs dans le vide-ordures commun de l'immeuble…

À travers cet exemple parmi d'autres, on comprend bien que la sensibilisation, la formation et l'accompagnement humain

des TPE/PME aux enjeux des différents aspects de la sécurité numérique est essentielle non seulement pour la protection des données mais aussi pour l'intégrité de l'organisation interne de l'entreprise, les relations avec les clients, les partenaires, les fournisseurs et les administrations.

LES PME FRANÇAISES ET LA CYBERSÉCURITÉ : DES DIRIGEANTS CONSCIENTS DES RISQUES

En novembre 2018, une étude sur la cybersécurité des PME françaises réalisée par l'IFOP pour Kaspersky et Euler Hermes[2] menée auprès de dirigeants de ce type d'entreprises, met en avant que 21 % des PME interrogées ont subi une attaque informatique dans l'année écoulée. Pour 14 % d'entre elles, cette attaque a entraîné un coût supérieur à 50 000 euros. Les dirigeants ont bien conscience de ces risques. Cette même enquête révèle que 63 % des PME craignent de subir une attaque ayant pour conséquence la divulgation d'informations sensibles, 38 % un impact négatif sur leur image et réputation et 30 % une perte d'exploitation ou de chiffre d'affaires. Concrètement, les dirigeants des entreprises se méfient des emails frauduleux (52 %), du piratage des données (51 %), des malwares (41 %) ou encore des fraudes en ligne (24 %). Par ailleurs, 77 % des entreprises interrogées n'ont pas réalisé d'audit de sécurité en 2018.

(2) Les PME face aux enjeux de sécurité informatique, Etude IFOP du 5 au 9 novembre 2018 de nature quantitative auprès de 702 décideurs.

Aider les entreprises à passer au numérique en partant de leur besoin

Communiquer en ligne, augmenter sa clientèle en trouvant de nouveaux clients, vendre aussi sur Internet, améliorer la gestion avec ses clients grâce à un logiciel adapté, recruter et se former en ligne… Les raisons de passer au numérique sont nombreuses pour les 3,8 millions de TPE/PME en France.

France Num (https://www.francenum.gouv.fr), nouvelle initiative nationale pour la transformation numérique des TPE/PME, pilotée par la Direction générale des entreprises, a été lancée le 15 octobre 2018 par l'État et les Régions françaises. Elle vise à aider les TPE/PME à utiliser le numérique à partir de leur besoin, à leur fournir un accompagnement par des experts de proximité (appelés Activateurs). Le rôle de ces accompagnants est d'apporter des conseils et des solutions pour entamer ou accélérer la transformation numérique de l'entreprise ; tel est l'axe central du service offert par France Num.

Concrètement, toute entreprise, à partir de la page d'accueil du portail « francenum.gouv.fr », peut solliciter une recommandation parmi 10 grands thèmes de la transformation numérique (dont « Protéger mon entreprise ») en indiquant son secteur d'activité, la taille de son entreprise et une indication géographique (code postal ou commune).

© FranceNUM

L'entreprise se voit alors proposer une « recommandation conseil » courte avec la possibilité de contacter des Activateurs. Pour ce qui concerne le volet « Protection de l'entreprise », celui-ci a été rédigé avec l'appui de l'ANSSI (Agence nationale de la sécurité des systèmes d'information, partenaire de France Num).

Pour ce qui relève des aspects cybersécurité, France Num s'est associée

POUR UNE PME DE 10 À 49 SALARIÉS, LA RECOMMANDATION « PROTÉGER MON ENTREPRISE » FORMULÉE PAR L'ANSSI EN LIGNE SUR FRANCE NUM

« Afin d'assurer la continuité de votre activité et la protection de votre patrimoine et de votre image, vous êtes le premier acteur de votre sécurité numérique.

Adoptez ces bonnes pratiques simples au quotidien, et diffusez-les auprès de vos collaborateurs, pour se former et se protéger efficacement des risques majeurs : choisir avec soin vos mots de passe, mettre à jour régulièrement vos logiciels, connaître ses utilisateurs et ses prestataires, effectuer des sauvegardes régulières, sécuriser l'accès Wi-Fi de votre entreprise, être aussi prudent avec son smartphone ou sa tablette qu'avec son ordinateur, protéger ses données lors de ses déplacements, être prudent lors de l'utilisation de sa messagerie, télécharger ses programmes sur les sites officiels des éditeurs, être vigilant lors d'un paiement sur Internet, séparer les usages personnels des usages professionnels, prendre soin de ses informations personnelles, professionnelles et de son identité numérique.
La souscription à une cyber-assurance vous permettra par ailleurs de vous prémunir contre les conséquences financières d'une cyber-attaque ou fraude, et d'en minimiser l'impact sur le fonctionnement de votre entreprise. »

avec le GIP ACYMA (www.cybermalveillance.gouv.fr) pour une sensibilisation et un accompagnement par des experts qualifiés, inscrits comme activateurs sur la plate-forme. On compte aujourd'hui plus de 60 de ces conseillers prestataires qui sont capables de comprendre, d'anticiper et de faire face aux risques en matière de numérique.

En outre, afin d'aider les TPE/PME en matière de sécurité numérique, l'ANSSI a réuni sur la plate-forme des contenus de sensibilisation, recommandations et bonnes pratiques dont un kit de sécurité des données à caractère personnel, élaboré à l'occasion de l'entrée en vigueur du Règlement Général de la Protection des Données (RGPD).

Des financements mobilisables par les TPE/PME pour la cybersécurité

Pour financer un projet de transformation numérique en TPE/PME, France Num propose au sein de la rubrique « Financez un projet », un moteur de recherche spécialisé interfacé avec www.aides-entreprises.fr :

Plusieurs aides peuvent concerner un axe de sécurité numérique : en effet, la plupart des Régions ont mis en place des dispositifs d'aides sous la forme de subventions qui permettent de financer l'installation de logiciels (dont

la cybersécurité) et des prestations de conseil et d'accompagnement (incluant des prestations de mise à niveau de l'entreprise en matière de cybersécurité). Exemples : Chèque Transformation Numérique (Nouvelle Aquitaine), Pays de la Loire Investissement Numérique, Cap' Développement Centre-Val de Loire - Volet Commercial et Numérique, Pass Occitanie, Chèque Numérique (Bretagne), etc.

Outre les subventions régionales, les Prêts Croissance TPE proposés par les Régions et le réseau Bpifrance incluent le financement de dépenses immatérielles telles que la mise aux normes de sécurité de l'entreprise (y compris sur le volet cyber) : le Prêt Cap Croissance TPE Centre-Val de Loire, Prêt Croissance TPE Bretagne, Prêt Croissance TPE Ile-de-France, ou encore Prêt Croissance TPE Hauts-de-France.

Des contenus pratiques sur la sécurité numérique intégrés à France Num

Dans sa mission d'aide à l'accompagnement des entreprises de moins de 250 salariés, le portail France Num publie régulièrement des contenus utiles et pratiques, relatifs à la sécurité informatique, à destination des TPE/PME, artisans et commerçants. Il s'agit de MOOC, guides de bonnes pratiques et infographies pour passer à l'action, des mesures préventives… Ces ressources visent à être immédiatement exploitables par les dirigeants et collaborateurs de l'entreprise.

Sont aussi disponibles, des évènements (ateliers, conférences, salons professionnels) proposés par la communauté des Activateurs France Num.

France Num, une initiative multi-partenariale

Enfin, France Num a été conçue conjointement par les Régions de France et l'État, avec 30 partenaires, tous acteurs de l'écosystème de la transformation numérique des TPE/PME, avec la volonté que les activateurs sur un même territoire puissent échanger en ligne. C'est un programme agile et ouvert où la sécurité numérique compte au sein de préoccupations et d'actions prioritaires.

AUTEUR

Ingénieure des mines, Aurélie GRACIA VICTORIA débute sa carrière à l'Autorité de régulation des communications électroniques et des postes (ARCEP) où elle travaille sur les sujets des offres consommateurs, de la neutralité d'internet et des réseaux et du déploiement de la 4G. Elle est cheffe du bureau des usages du numérique de la Direction générale des Entreprises (DGE).

Elle y dirige notamment l'équipe qui pilote l'initiative France Num pour la transformation numérique des TPE/PME, en lien avec les Régions et les partenaires au contact des entreprises.

Cybermalveillance
et entreprises : 1er enseignements du dispositif d'assistance

Par Jérôme Notin

Lancé en octobre 2017, le dispositif national d'assistance aux victimes « Cybermalveillance.gouv.fr » était présenté dans l'édition n° 260 de décembre de la revue de la gendarmerie nationale de la même année. Un an plus tard, des premiers enseignements peuvent déjà être tirés sur les missions de ce dispositif et sa perception de la cybermenace, notamment pour ce qui concerne la sphère des petites et moyennes entreprises qui en sont fréquemment la cible.

JÉRÔME NOTIN

Directeur général du GIP ACYMA. Chef d'escadron de la réserve citoyenne cyberdéfense de la gendarmerie

Au fil du développement de son action, le dispositif « Cybermalveillance.gouv.fr » a pu confirmer, par son originalité et les services qu'il apporte, qu'il est de nature à pouvoir répondre à une réelle attente de ses publics. Près de 29 000 personnes sont venues rechercher de l'assistance sur la plateforme en 2018. Ce nombre de sollicitations, qui ne cesse d'augmenter, a été multiplié par quatre, passant de 500 par mois en janvier 2018 pour dépasser la barre des 4 000 en décembre. Leur analyse, les échanges que le dispositif peut avoir et les sondages auxquels il participe, lui permettent d'adapter son action aux attentes et aux réalités du terrain.

Un dispositif et un capteur original en partenariat public-privé

Aujourd'hui, le groupement d'intérêt public qui pilote Cybermalveillance.gouv.fr est fort de près d'une quarantaine de membres. Il rassemble des acteurs étatiques et de la société civile engagés dans la lutte contre la cybermalveillance. Outre leur soutien financier, ces membres renforcent et démultiplient les actions du dispositif.

Le dispositif dispense des conseils et une

orientation des victimes, principalement celles qui ne sont pas couvertes par d'autres dispositifs de l'État. La victime peut ainsi être guidée dans son diagnostic, ses démarches, voire être orientée selon son besoin et en fonction de la nature du problème qu'elle rencontre vers un des 1 500 prestataires de proximité qui sont référencés sur la plateforme.

Tant l'organisation retenue que les services apportés aux victimes, en complémentarité des autres dispositifs de l'État, font du dispositif « Cybermalveillance.gouv.fr » un modèle unique et original qui est regardé avec beaucoup d'intérêt par de nombreux autres pays.

L'originalité du dispositif réside également dans le fait qu'il intervient généralement en amont lorsque la victime rencontre un incident. Il est en cela un capteur, très intéressant pour les pouvoirs publics, d'une certaine réalité de la cybermalveillance pour des victimes qui n'envisagent pas en première intention de déposer plainte : soit parce qu'elles n'ont pas conscience que leur mésaventure pourrait faire l'objet de poursuites ; soit parce qu'elles pensent que les poursuites dans la sphère cyber ont peu de chance d'aboutir et que leur démarche ne serait qu'une perte de temps inutile ; soit parce qu'elles ont un peu honte de s'être fait gruger ou craignent pour leur image.

À ce stade, le dispositif intervient en incitant systématiquement la victime à déposer plainte chaque fois qu'une infraction pourrait être retenue mais aussi en l'aidant dans sa démarche par des conseils élaborés en collaboration étroite avec les services du ministère de l'Intérieur. Lorsque son cas est jugé adapté, la victime est également incitée à signaler les faits rencontrés sur les plateformes dédiées notamment celles du ministère de l'Intérieur, comme « Pharos », pour tout ce qui touche aux contenus illicites ou aux tentatives d'escroquerie, ou encore « Perceval » pour ce qui a trait aux fraudes sur les cartes bancaires.

Le dispositif intervient aussi en identifiant des phénomènes à partir d'événements qui, pris séparément, peuvent être considérés comme marginaux mais dont le rassemblement met en évidence des organisations ou des méthodes criminelles qui peuvent mériter une certaine attention. C'est ainsi que « Cybermalveillance.gouv.fr » a pu contribuer à l'identification du phénomène de masse cybercriminel de « l'arnaque au faux support technique » fin 2017, tant au travers des remontées des victimes, qui lui demandaient de l'assistance, que des rapports techniques d'intervention qui sont remontés par ses prestataires référencés. Dans la grande majorité des cas, si les victimes avaient bien eu l'impression à un moment ou un autre de s'être fait abuser, elles n'envisageaient généralement pas pour autant de dépo-

ser plainte malgré les incitations, pour les raisons évoquées précédemment.

L'identification de ce phénomène cybercriminel et les échanges opérationnels, qui ont pu être conduits avec les services des ministères de l'Intérieur et de la Justice, ont provoqué l'ouverture d'une enquête par la section de lutte contre la cybercriminalité du parquet de Paris en mars 2018. Confiées au centre de lutte contre les criminalités numériques (C3N) du pôle judiciaire de la gendarmerie nationale, les investigations ont conduit à la saisie de près de 2 millions d'euros début février 2019 et à la mise en examen de trois individus, travaillant en réseau, qui ont fait près de 8000 victimes.

Cette possibilité d'identification des menaces au plus près de leur apparition permet également au dispositif d'alerter les populations via son site Internet et/ou ses réseaux sociaux (Twitter, Facebook, LinkedIn). Grâce au relais et à l'appui de ses membres, plusieurs alertes émises par le dispositif ont été largement reprises par les médias, démultipliant ainsi les capacités d'atteindre le plus grand nombre de victimes potentielles.

Les TPE-PME : cibles de choix des cybercriminels

Même si elles ne sont pas exonérées de subir des cyberattaques très variées, les grandes entreprises ou les grandes administrations se sont souvent armées pour y faire face, tant en matière de compétences qu'en moyens de défense. Il n'en est malheureusement pas toujours de même pour les petites et moyennes entreprises ou les collectivités territoriales. Ces dernières représentent donc une cible de choix pour les cybercriminels qui cherchent évidemment toujours à maximiser leur profit avec un minimum d'effort. Les conséquences de ces attaques peuvent être dramatiques pour ces plus petites organisations qui y jouent parfois leur survie économique.

On peut aisément admettre que la priorité d'une entreprise réside dans la réalisation de son activité, dont les systèmes d'information ne sont généralement considérés que comme le simple support. La numérisation des activités en fait pourtant une composante particulièrement critique pour les entreprises. Sans leur système d'information, la plupart des organisations ne peuvent tout simplement plus fonctionner et donc voient leur activité s'arrêter.

Ces systèmes d'information sont souvent externalisés auprès de prestataires qui se livrent une concurrence féroce en tirant les prix vers le bas, ce qui est évidemment toujours un argument très scruté par leurs clients. Cette logique économique va souvent de pair avec un niveau des prestations qui peut s'avérer amoindri, notamment en ce qui concerne le domaine de la sécurité.

La sécurité informatique est un sujet assez complexe à appréhender et n'est donc pas toujours celui le plus regardé ou compris par les responsables des organisations.

Quand bien même ces organisations disposent de compétences internes qui chercheraient à convaincre les décideurs à améliorer le niveau de sécurité de leur entreprise, les arguments présentés sont souvent vus par les dirigeants comme des caprices technologiques ou des investissements supplémentaires non indispensables, car difficilement perceptibles ou compris en matière de retour sur investissement.

Enfin, pour la réalisation de leurs activités principales, les entreprises sont confrontées à une réalité opérationnelle où il faut aller vite. L'information doit être échangée et accessible en tout lieu et toutes circonstances et avec si possible le minimum de contraintes, de freins à leur productivité. La sécurité est souvent perçue comme une de ces contraintes jusqu'au jour où le drame arrive.

De leur côté, les cybercriminels ont bien conscience de cette réalité et des vulnérabilités induites pour ces entreprises qu'ils vont pouvoir exploiter afin d'en tirer profit. Le temps est révolu (ou presque) du stéréotype du « pirate » marginal qui s'attaquait seul, depuis sa chambre d'étudiant, à une multinationale. Les entreprises doivent aujourd'hui faire face à un écosystème cybercriminel qui se structure par expertises et domaines de compétences. Certains groupes criminels se sont spécialisés dans la réalisation d'outils d'attaques de haut niveau, d'autres dans la recherche de failles ou d'accès dans les systèmes, des « clients » les achètent pour les mettre en œuvre, d'autres enfin vont exploiter les résultats des attaques. Sur le fameux Darknet sur lequel ces cybercriminels évoluent, tout se vend et tout s'achète.

Au travers des échanges qu'il peut avoir avec les victimes ou ses prestataires référencés, le dispositif Cybermalveillance.gouv.fr constate que les attaques qui sont conduites par les groupes cybercriminels sont de plus en plus « professionnelles » et que les dommages qu'elles occasionnent sont de plus en plus conséquents pour les entreprises qui les subissent.

Parmi ces attaques, celles par rançongiciels (ransomware) sont une bonne illustration de l'évolution des techniques et des capacités cybercriminelles. Si initialement ces attaques étaient généralement déclenchées à partir de simples pièces jointes ou des liens malveillants contenus dans des messages d'hameçonnage (phishing), plus ou moins ciblés ou grossiers, aujourd'hui les entreprises qui sont victimes voient des modes opératoires radicalement différents les frapper.

Les cybercriminels cherchent aujourd'hui à pénétrer directement les entreprises par leurs accès extérieurs que ce soit par les voies du travail à distance ou de la télémaintenance. Ils y parviennent soit en exploitant une faille logicielle non corrigée, soit en arrivant à « casser » des mots de passe insuffisamment solides.

Une fois cette cartographie réalisée, les cybercriminels lancent la partie visible de leur attaque. Celle-ci se déroule généralement en dehors des heures ouvrées de l'entreprise qu'ils ont pu appréhender en l'observant. Ils commencent alors à chiffrer les données de l'entreprise en démarrant… par ses sauvegardes. Les cybercriminels ont bien compris que chaque entreprise a aujourd'hui peu ou prou des sauvegardes mais aussi que ces sauvegardes sont généralement, et par facilité, directement accessibles en ligne sur le réseau de l'entreprise, qui n'a d'ailleurs souvent aucune autre copie récente de ses données.

À l'ouverture des bureaux de l'entreprise, toutes ses données sont chiffrées, y compris ses sauvegardes, et un message de demande de rançon attend les décideurs. Cette rançon représente généralement une portion « acceptable » du chiffre d'affaires de l'entreprise au regard du préjudice qu'elle subit. De quelques centaines d'euros pour une TPE, à plusieurs milliers d'euros pour des collectivités, et jusqu'à des centaines de milliers d'euros pour des PME de taille plus conséquente. Cette variabilité des rançons demandées en fonction du chiffre d'affaires et des capacités de paiement de sa cible démontre bien que le cybercriminel qui commet l'attaque ne frappe pas au hasard, et qu'en amont et une fois dans la place il a cherché à estimer la somme qu'il pouvait demander à sa victime.

Les conséquences de ces attaques par rançongiciels ne se limitent pas à la perte financière de la seule rançon demandée que certaines victimes pourraient être enclines à payer. Il faut en effet toujours y ajouter le coût de la perte de production, parfois durant plusieurs jours, liée à l'indisponibilité du système d'information de la victime, ainsi que celui des travaux de remise en état.

On constate également que chez la plupart des victimes, la priorité va à la remise en service le plus rapidement possible de leur système d'information pour pouvoir reprendre au tôt leur activité. Il s'agit là d'une vision très court-termiste qui peut souvent avoir des conséquences désastreuses dans la durée. En effet, ne pas avoir clairement identifié par où et comment sont rentrés les criminels pour pouvoir y remédier, c'est prendre le risque conséquent de se voir confronté à une nouvelle attaque identique, soit par le même groupe criminel, soit par un autre groupe auquel la victime aura

été « vendue » par le primo attaquant. La vente aura d'ailleurs d'autant plus de valeur si elle mentionne que la victime paie les rançons qui lui sont demandées en partant du principe évident : « qui a payé, paiera ».

Un autre exemple, les « arnaques au Président » ont pu également frapper de grands groupes et touchent de plus en plus de PME. Ces attaques consistent à demander à un employé, souvent sous le sceau du secret, de faire un virement sur un compte off shore en se faisant passer pour un de ses dirigeants ou de ses mandataires. Les victimes sont généralement contactées par message électronique mais aussi parfois par téléphone. Les criminels se montrent toujours manifestement très bien renseignés sur les usages, l'organisation et les procédures de l'entreprise victime. Ils bénéficient là-aussi de la vulnérabilité induite par la facilité et la rapidité des échanges par messages électroniques ainsi que par l'anonymat que lié à la dématérialisation du fonctionnement des entreprises. Cette situation suppose qu'un employé peut travailler depuis des années, de manière électronique, avec des interlocuteurs qu'il n'a jamais vus et qu'il ne lui viendrait souvent même pas à l'esprit de demander la confirmation d'un ordre reçu par message ou par téléphone de ses dirigeants. C'est en jouant sur ces facteurs bien compris que les cybercriminels arrivent à commettre leurs escroqueries.

Ces exemples démontrent qu'une entreprise logiquement focalisée sur son cœur de métier et sa réactivité opérationnelle peut se retrouver insuffisamment préparée à subir de telles attaques. Elle peut alors se retrouver désemparée quand elle tombe sous le joug de cybercriminels qui sont pour leur part de plus en plus « professionnels » dans leurs actions.

La prévention : une arme défensive majeure

La prévention reste la meilleure arme des entreprises pour éviter les cyberattaques ou pour pouvoir y faire face lorsqu'elle se produisent.

Elle se limite souvent à la formation ou l'information des employés qui est certes un pan très important, mais ne saurait être le seul. L'outillage et l'anticipation des crises sont également des facteurs fondamentaux de la protection des entreprises.

La formation des employés aux cybermenaces et aux bonnes pratiques à adopter pour les éviter ou les détecter est primordiale. Cela reste souvent un exercice difficile, car les sujets de sécurité numérique sont généralement ressentis comme rébarbatifs, peu parlants et sources de contraintes pour les utilisateurs, quel que soit leur niveau dans l'entreprise : du dirigeant à l'employé, en passant par le cadre ou même «l'informaticien ». C'est d'autant plus

regrettable que beaucoup d'attaques pourraient être évitées si des mesures simples et pratiques de cybersécurité étaient appliquées, ce qui est malheureusement trop peu souvent le cas.

C'est à partir de ce constat issu des travaux conduits avec ses membres que le dispositif « Cybermalveillance.gouv.fr » a réalisé, en 2018, le premier volet de son kit de sensibilisation pour les collaborateurs. Ce kit peut être téléchargé gratuitement sur la plateforme du dispositif. Il comprend différents types de supports (courtes vidéos, infographies, fiches pratiques). Il interpelle le collaborateur dans ses usages personnels de manière pédagogique et illustrée, sur des sujets qui peuvent également intéresser l'entreprise dans ses usages professionnels. Par exemple, si un collaborateur sait détecter et réagir à un message d'hameçonnage (phishing) dans ses usages personnels, il saura également le faire dans ses usages professionnels. Dans le premier volet de ce kit, quatre thèmes sont abordés : l'hameçonnage qui est le principal vecteur d'attaque aujourd'hui ; la bonne gestion des mots de passe qui reste une des principales protections des systèmes ; la sécurité des appareils mobiles (smartphones, tablettes) qui présentent des vulnérabilités spécifiques importantes ; et la différenciation des usages professionnels et personnels. Ce premier volet du kit de sensibilisation des

© Acyma

La plate-forme permet d'obtenir des éléments de langage propres à la compréhension du phénomène criminel et à la construction de mesures de protection.

collaborateurs a connu un réel succès avec plus de 20 000 téléchargements en 6 mois. Il est utilisé et diffusé, y compris dans de très grandes entreprises. Un second volet de ce kit de sensibilisation des collaborateurs sera publié en 2019. Il abordera d'autres thématiques estimées essentielles au regard des premiers retours d'expérience.

Outre la formation de ses employés, d'autres mesures de prévention peuvent être mises en œuvre telles qu'un outillage adapté pour sécuriser ses systèmes d'information. Des systèmes de sauvegarde sécurisés et en partie hors ligne, voire délocalisés, permettront de pouvoir faire face à une attaque par rançongiciels comme décrite précédemment sans risquer de perdre toutes ses informations. Des dispositifs anti-virus permettront de filtrer tout ce qui peut être notoirement connu comme malveillant. Des systèmes de journalisation des accès et de détection d'intrusion pourront permettre de repérer une attaque en cours et la comprendre. Des pare-feux pourront protéger les entrées et sorties des systèmes d'information de l'entreprise et ne laisser passer que ce qui est dûment légitime. Des systèmes de déploiement centralisés de politique de sécurité ou des mises à jour permettront de standardiser son niveau de sécurité et de rapidement corriger une vulnérabilité sur l'ensemble de son parc informatique (sans oublier son parc d'appareils mobiles), etc.

Autrement dit, de nombreuses solutions techniques existent mais elles sont souvent encore insuffisamment mises en œuvre. Bien entendu, cet outillage a un coût, tant humain que financier mais ces solutions sont autant de ceintures de sécurité et d'airbags, dans lesquels il peut être important d'investir en prévention, pour éviter les accidents ou a minima pour pouvoir les affronter dans les meilleures conditions possibles.

Enfin, au titre de la prévention, on peut également citer la préparation à la gestion de la crise qu'engendre pour une entreprise toute attaque informatique majeure. Force est de constater que les entreprises, surtout les plus petites, sont généralement insuffisamment préparées pour affronter ces situations difficiles et pour elles exceptionnelles. De nombreux conseils en première intention sont disponibles sur la plateforme « Cybermalveillance.gouv.fr » sur les principaux types d'attaques. Par ailleurs, si l'entreprise dispose de compétences informatiques internes et/ou au travers de ses prestataires de support, ces compétences ne sont pas toujours adaptées pour affronter ces situations particulières. Il faut savoir le diagnostiquer et l'admettre afin de se faire aider par des prestataires spécialisés. Bien entendu, il reste évidemment préférable d'avoir contracté avec ces prestataires préalablement à l'incident pour s'assurer tant de leurs compétences que de leur

disponibilité le jour où leur intervention est nécessaire.

La question pour une entreprise n'est plus aujourd'hui de savoir si elle sera attaquée, mais quand ? Sera-t-elle suffisamment préparée pour l'empêcher ou y faire face ? Malheureusement, la cybermalveillance, ça n'arrive pas qu'aux autres…

AUTEUR

Impliqué dans la sécurité numérique depuis de nombreuses années, Jérôme Notin dispose d'expériences dans la création et la direction d'entreprises. Il a rejoint l'ANSSI en mai 2016 en qualité de préfigurateur du dispositif et a été nommé en mars 2017 directeur général du GIP ACYMA lors de sa création. Il est par ailleurs ancien gendarme auxiliaire (94/10 PSIG de Blois) et chef d'escadron de la réserve citoyenne cyberdéfense de la gendarmerie.

Cybermalveillance.gouv.fr est la plateforme nationale d'assistance aux victimes de cybermalveillance. Lancé au niveau national en octobre 2017, ce dispositif à une triple mission :
- la prévention par la diffusion d'alertes et de bonnes pratiques en cybersécurité ;
- l'assistance aux victimes en les aidant à diagnostiquer leur problème et en les conseillant et les orientant vers les services compétents, voire vers des prestataires spécialisés de proximité susceptibles de pouvoir les assister ;
- l'observation de la menace afin de détecter les phénomènes émergents pour pouvoir les anticiper et y répondre.

Ce dispositif s'adresse autant aux particuliers, qu'aux entreprises, aux collectivités, aux associations qui ne sont pas déjà couverts par d'autres dispositifs de l'État ou en les complétant.

Il est organisé sous la forme d'un groupement d'intérêt public, le GIP ACYMA. Ce partenariat public-privé rassemble les acteurs de l'État et de la société civiles engagés dans sa mission d'intérêt public de lutte contre la cybermalveillance parmi lesquels l'Agence nationale de la sécurité des systèmes d'information (ANSSI) qui relève des services du Premier ministre et le ministère de l'Intérieur qui en sont les fondateurs, ainsi que le ministère de la Justice, le ministère de l'Économie et des finances et le secrétariat d'État en charge du numérique, ainsi que de nombreux acteurs de la société civile comme des associations de consommateurs ou d'aides aux victimes, des représentations professionnelles, des assureurs, des opérateurs, des constructeurs, des éditeurs…

La gendarmerie
au cœur de la prévention des troubles à l'ordre économique

Par Jean-François Nativité

Présente sur environ 90 % du territoire métropolitain, la Gendarmerie nationale est un acteur séculaire majeur de la vie de la cité. Forte de ses missions régaliennes de sécurité publique, elle fait partie intégrante du dispositif public d'intelligence économique. Avec son maillage territorial et sa connaissance du tissu économique local, elle est un maillon essentiel dans la sensibilisation des entreprises, le recueil de leurs questions, inquiétudes et plaintes, mais aussi dans la détection de potentielles menaces. Elle contribue de ce fait à préserver les savoir-faire économiques et technologiques des entrepreneurs, et donc à pérenniser les emplois et l'équilibre économique des territoires.

JEAN-FRANÇOIS NATIVITÉ

Commandant de gendarmerie. Adjoint du délégué au patrimoine culturel de la gendarmerie

Un rôle prépondérant dans la sécurisation économique des territoires

En seulement un quart de siècle, la mondialisation et le déploiement rapide des technologies de l'information ont bouleversé le milieu économique. L'information est devenue une matière exploitable à des fins stratégiques, un enjeu de compétitivité. Les profondes mutations macroéconomiques, l'extrême volatilité de la finance mondiale et l'émergence de nouveaux pays concurrents ont conduit les acteurs économiques à se livrer une féroce bataille pour conquérir des parts de marché. C'est dans ce contexte d'insécurité économique que l'État a décidé, dès 2005, de mettre en place un dispositif d'intelligence économique (IE) territorial visant à soutenir les entreprises créatrices d'emplois et de richesses.

Fixée par la circulaire du Premier ministre du 15 septembre 2011, l'organisation actuelle du dispositif d'intelligence territoriale est placée sous l'égide du préfet de Région en

charge du pilotage et de l'animation de cette politique. Dans ce cadre, la Gendarmerie nationale s'intéresse exclusivement au volet défensif de l'intelligence économique nommé "sécurité économique". Cette approche s'inscrit dans son coeur de métier. Elle consiste à prévenir et à réprimer tout acte hostile visant à porter atteinte aux intérêts d'une entreprise implantée en zone de compétence de la Gendarmerie nationale[1].

(1) Ministère de la Défense, Ministère de l'Intérieur, de l'outre-mer et des collectivités territoriales, Sécurité économique territoriale. La région de gendarmerie de Rhône-Alpes « au service des entreprises », 2013, p. 3.

Grâce à son implantation territoriale historique, à ses compétences judiciaires et ses expertises en matière de sécurité, de cybercriminalité ou encore de délinquance financière, la Gendarmerie dispose d'une capacité importante de collecte d'informations utiles aux entreprises (menaces internes et externes). Il faut savoir que les atteintes économiques se concentrent à 75% vers des entreprises de moins de 500 salariés, implantées à 80% en zone de compétence gendarmerie[2]. Outre l'identification et l'accompagnement judiciaire (s'agissant des infractions économiques et financières constatées, vols, escroqueries, contrefaçons, etc.), l'un des principaux objectifs de la gendarmerie est de sensibiliser sur le terrain les chefs d'entreprises comme les salariés via notamment des conférences, tables rondes et autres participations à des réunions d'acteurs économiques, tout en effectuant en parallèle un travail de prévention (diagnostic de sûreté et/ou de sécurité économique, accompagné de recommandations pragmatiques et efficaces).

(2) Christophe ROHEL, « La gendarmerie au cœur de la politique publique d'intelligence économique », Intelligences économiques. Nouvelles pratiques & mentalités dans la recherche et la gestion de l'information, juin 2014, p. 1.

Il s'agit aussi pour elle d'identifier les entreprises représentant une sensibilité particulière (secteurs stratégiques, pôles de compétitivité) en collaboration avec les autres services de l'État et d'alerter au besoin les autorités et services compétents en cas de signaux faibles ou d'atteintes constatées, afin de protéger leur patrimoine matériel et immatériel[3]. En effet, depuis ces dernières années, les « cyber-vulnérabilités » sont en constante progression. Le monde s'est numérisé, les entreprises se sont connectées : site internet, réseaux sociaux, intranet, fichiers, cloud, etc. Autant de vecteurs aujourd'hui indispensables, contenant de l'information confidentielle, qui intéressent les cybercriminels. Selon le ministère de l'Intérieur, plus d'un tiers des entreprises françaises de moins de 250 salariés seraient victimes de ces « cyberattaques ». Celles-ci visent tout ce qui fait fonctionner l'entreprise ou détermine sa stratégie : fichiers clients, données personnelles, mais aussi la prise de

(3) Laura FORT, « Quand les gendarmes préviennent les troubles à l'ordre économique », La Tribune, 7 décembre 2012, pp. 2-3.

contrôle de systèmes opérationnels. D'après les derniers chiffres consolidés, le risque cyber concerne environ 50 % des attaques subies par les entreprises. Le reste intéresse les atteintes aux savoir-faire (contrefaçon), les intrusions consenties (clients, stagiaires, prestataires…), les atteintes à la réputation (informations malveillantes), les atteintes physiques (intrusions, vols…) sur site et les risques financiers.

La sécurité économique, une affaire de spécialistes organisés en réseaux

A compter de 2002 et de la loi d'orientation et de programmation pour la sécurité intérieure (LOPSI 1), la gendarmerie a été impliquée dans le paysage de la prévention situationnelle à destination des opérateurs économiques. Peu après la nomination d'Alain Juillet au poste de haut responsable chargé de l'intelligence économique en janvier 2004, la Direction générale de la Gendarmerie nationale (DGGN) a désigné un officier afin d'élaborer les premiers éléments de doctrine « intelligence économique » de la gendarmerie.

Au sein de la sphère publique, conformément à la circulaire du 1er juin 2010, la Gendarmerie nationale agit en complémentarité des actions entreprises par la Direction générale de la sécurité Intérieure (DGSI) et du Service central de renseignement territorial (SCRT), au sein du ministère de l'Intérieur, et par la Direction de la protection et de la sécurité de la défense (DPSD) au sein du ministère de la Défense. Elle a mis en place un dispositif à la fois vertical et transverse, adapté la formation de ses personnels dès 2005 (première session de formation de référents « intelligence économique ») et 2007 (première session de formation des « référents sûreté » en commun avec la Police nationale). La gendarmerie dispose en effet de spécialistes au niveau de chaque strate administrative. Tout d'abord au sein de la DGGN, une section sécurité économique et protection des entreprises (SECOPE) de la sous-direction de l'anticipation opérationnelle (SDAO) a été créée en novembre 2013. Cette dernière a notamment dans ses attributions le traitement de la sécurité économique en métropole et en outre-mer (art. 5 de l'arrêté du 6 décembre 2013)[4].

(4) Catherine de La ROBERTIE, Norbert LEBRUMENT, Stéphane MORTIER, « La mission intelligence économique de la gendarmerie nationale au prisme des entreprises », Cahiers de la sécurité et de la justice, n° 34, 2016, pp. 87-88.

Au sein de chaque région de gendarmerie se trouve ensuite un officier de gendarmerie référent « intelligence économique » formé au cours d'un cycle spécialisé à l'Institut National des Hautes Études de la Sécurité et de la Justice (INHESJ).

Des sous-officiers « référents intelligence économique », répartis sur tout le territoire métropolitain et outre-mer ainsi que dans les formations spécialisées de la gendarmerie, sont formés en interne via une structure de formation spécifique : le

Centre National de Formation au Renseignement Opérationnel (CNFRO). Ils sont généralement placés au sein de cellules renseignement de chaque département (CORG) et agissent en complémentarité des 260 gendarmes « enquêteurs technologies numériques » (N'TECH) du réseau territorial CYBERGEND piloté par le centre de lutte contre les criminalités numériques (C3N).

Technicien CyberGend C3N, lutte contre la cybercriminalité et lutte anti terroriste (2017).

Des outils d'analyse et une fonction de conseil

Pour les référents « intelligence économique », l'activité au quotidien consiste essentiellement en un travail d'identification des acteurs, de sensibilisation et de renseignement. Ils disposent d'outils de diagnostic mis à leur disposition par le Service interministériel de l'Information Stratégique et de la Sécurité Économique (SISSE) créé en 2016, au nombre desquels le logiciel DIESE (Diagnostic d'Intelligence Économique et de Sécurité des Entreprises) qui évalue les vulnérabilités de l'entreprise et son niveau de protection.

Les référents sensibilisent également les entreprises aux risques « cyber » (risques économiques ou financiers, risque de

réputation, *etc.*), notamment par la diffusion des documents de l'Agence Nationale pour la Sécurité des Systèmes d'Information (ANSSI)[5]. Afin d'améliorer les résultats de leurs missions, ils partagent de manière transverse les cas concrets, informations utiles et axes d'actions à travers *ResoGend* un site de partage et de discussion en ligne dédié à la communauté de l'IE créé en 2015[6].

(5) Stéphane MORTIER, « Action territoriale de la gendarmerie : entre intelligence économique et sûreté », dans Olivier COUSSI (dir.) et Patricia AUROY (dir.), Intelligence économique des territoires. Théories et pratiques, Paris, Éditions du CNER & Caisse des Dépôts, 2018, pp. 90-92.

(6) Christophe CLARINARD (Lieutenant-colonel), « La gendarmerie nationale au coeur de la politique publique d'intelligence économique », SECEM Mag, n° 7, janvier/mars 2016, p. 33.

Un partenariat actif

L'efficacité du dispositif repose également sur les liens de partenariats tissés avec les acteurs du monde de l'entreprise. Depuis 2012, en région Champagne-Ardenne, l'Union des maisons de Champagne, le Syndicat général des vignerons et la Gendarmerie nationale sont par exemple à l'initiative d'un plan de la lutte contre la contrefaçon ayant contribué à la réduction significative de ce type d'atteintes.

Au niveau national, une convention de partenariat en matière de sécurité économique a été signée en 2016 entre le ministère de l'Intérieur et la CCI-France afin de renforcer les échanges d'informations et de bonnes pratiques. De même, les échanges réguliers avec les fédérations professionnelles permettent d'associer les acteurs publics et privés dans les démarches d'intelligence économique et de renforcer la lutte contre les malveillances. Depuis 2005, ce sont plusieurs dizaines de milliers d'entreprises qui ont ainsi pu être sensibilisées aux risques et vulnérabilités qui les menacent.

Décloisonner et renforcer les partenariats pour approfondir une action attendue des acteurs économiques.

(7) Stéphane MORTIER, Ibid., p. 94.

(5) MPTAM : Loi du 27 janvier 2014 de modernisation de l'action publique territoriale et d'affirmation des métropoles. https://www.vie-publique.fr/actualite/panorama/texte-discussion/projet-loi-modernisation-action-publique-territoriale-affirmation-metropoles.html

NOTRe : Loi N° 2015-991 du 7 août 2015 portant sur la nouvelle organisation territoriale de la République. https://www.vie-publique.fr/actualite/dossier/elections-regionales-2015/competences-regions-apercu-apres-loi-notre.html

Si l'on en croit les retours des référents territoriaux, ces actions particulières de la Gendarmerie nationale correspondent bien aux besoins et attentes des PME-PMI[7]. Pour autant le chantier reste immense. De nombreuses atteintes au tissu économique local ne sont pas connues des services de l'État faute de remontées directes des chefs d'entreprises ou de partages suffisants d'informations entre les différentes strates d'intervention : État vs collectivités, public vs privé. Compte tenu des nouvelles législations

territoriales (MPTAM, NOTRe[8]) en vigueur, les territoires doivent davantage être parties prenantes dans la coordination et la mutualisation des services de l'État (gendarmerie, police douanes, DGSI, ANSSI…) et des acteurs économiques privés de la sécurité économique et numérique, dans le but de les rendre plus efficients et de renforcer leurs capacités opérationnelles.

AUTEUR

Docteur en Histoire militaire et études de Défense (2010), le commandant Jean-François Nativité est également diplômé de l'Ecole d'Administration (Mastère spécialisé en gestion des risques sur les territoires - Promotion Théodore Monod 2007). Spécialisé dans les questions d'intelligence économique territoriale et de sécurité économique, il a occupé de 2007 à 2015 les fonctions de directeur du développement territorial au sein de l'ADIT (Agence pour la Diffusion de l'information technologique).

TPE-PME :
un enjeu de cybersécurité ?

Par Roland Majorel

Les très petites entreprises (moins de 10 salariés et chiffre d'affaire inférieur à 2 M€) et les petites et moyennes entre prises (moins de 250 salariés et moins de 50 M€) représentent l'immense majorité des 3,5 millions d'entreprises en France réparties sur l'ensemble des territoires[1]. Aussi, forts du poids du nombre, ces acteurs économiques sont les moteurs essentiels de la performance et de la vitalité de l'économie française ainsi que de la vie des populations locales[2]. La transformation numérique en cours qui se traduit par l'interconnexion des technologies et des entreprises, la numérisation ou le fait que les systèmes d'information dépendent d'un très petit nombre d'acteurs américains ou chinois (les GAFAM ou les BATXH), s'accompagne pour les entreprises d'un fort besoin en sécurité. Les TPE/ PME sont bien sûr concernées au premier chef, d'autant que leur mode de croissance et d'évolution est bien souvent éloigné de la notion de security by design[3]. Or, et c'est un constat, il n'y a pas de sécurité économique sans cybersécurité[4] ….

(1) Selon le géographe Claude Raffestin, le territoire est « un espace transformé par le travail humain ».

(2) TPE/PME et ETI représentent en 2015, 73 % des emplois français et 19 millions d'emplois.

(3) L'intégration de la sécurité dès la phase de conception.

(4) Ensemble des lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies qui peuvent être utilisés pour protéger les personnes et les actifs informatiques.

ROLAND MAJOREL

Lieutenant-colonel de gendarmerie. Chargé de mission. MINEFI

L'argent étant le nerf de la guerre et la notion de souveraineté de l'État passant par la nécessité d'avoir une économie saine et résiliente, l'Etat-stratège, à travers une politique publique d'intelligence économique (PPIE) mobilisant l'ensemble des acteurs

de sécurité économique publics et privés, s'attache à procurer aux entreprises un environnement numérique sécurisé tout en promouvant une culture de la sécurité, économique, dans laquelle la cybersécurité prend une place importante. La gendarmerie nationale, présente et compétente sur 95 % du territoire national, participe pleinement à la mise en œuvre de la cybersécurité des entreprises notamment grâce à l'action de son réseau de référents « intelligence économique territoriale ».

Les grandes lignes de la PPIE en matière de cybersécurité

En 2015, seules 12,5 % des entreprises du CAC 40 annonçaient avoir lancé un programme de cybersécurité … et 79 % des microprocesseurs étaient des Intel[5]. Dès lors, on ne peut qu'imaginer avec crainte les scénarii à « l'estonienne » [6] dans lesquels notre économie et nos administrations seraient attaquées et durablement paralysées en raison de leur manque de préparation ou d'une faible résilience. Sans même aller jusqu'à l'implication d'un Etat (préalable à un conflit classique ou une mesure de rétorsion), les différentes vagues d'attaques de types WCry, WannaCry, WanaCrypt0r, WannaCrypt, Wana Decrypt0r, NotPetya[7] et Mirail qui touchait les objets connectés, sont autant de menaces qui appellent une prise de conscience des acteurs économiques et notamment des entreprises.

Pour mémoire, ces différentes attaques ont infecté jusqu'à 75 millions d'ordinateurs dans le monde entier dont ceux de grandes entreprises françaises, des administrations et services publics mais aussi d'un grand nombre de TPE/PME (en 2018, 40 % des TPE/PME françaises ont subi une ou des attaques informatiques et seules 38 % ont nommé un référent en charge de la sécurité informatique[8]). En 2018, le secteur français le plus touché par les cyberattaques a été celui des entreprises (37 % si on s'en tient au secteur hors bancaire 56 % si on l'inclut) et cela aurait coûté à l'économie française 15 milliards d'euros (projection potentielle de 30 milliards en 2019).

Face à un risque systémique, c'est-à-dire pouvant remettre en question la survie même du secteur financier et donc de l'économie du pays, l'État garant de la sécurité de la Nation doit à travers une politique publique trouver les ressources nécessaires pour protéger nos intérêts.

La politique publique de sécurité économique, qui est l'un des pilier de la PPIE

(5) Source Cybermenace, avis de tempête de l'institut Montaigne.

(6) Le 27 avril 2007, une attaque informatique massive débutait contre l'Estonie, organisée depuis la Russie voisine et décidée, selon un faisceau d'indices concordants, par l'Etat russe lui-même.

(7) Qui touche toutes les versions non mises à jour de Microsoft Windows, de Windows XP à Windows 10 et utilise, pour se propager, la faille de sécurité volée à la NSA par un groupe de pirates informatiques.

(8) Enquête sur la cybersécurité des entreprises TPE/PME de janvier 2019 par CPME.

(9) En toute sécurité, Patrick Haas.

s'appuie bien sûr en matière de cybersécurité sur un volet défensif porté par l'ANSSI[10] (qui peut intervenir au profit d'entreprises attaquées, affaire TV5 Monde en 2015 et agir en prévention grâce à son réseau de délégués régionaux) et promu par la plateforme publique cybermalveillance.gouv.fr (ACYMA, action contre la cybermalveillance) qui s'adresse aux particuliers et aux entreprises victimes d'attaque informatique. Mais ce pan défensif s'accompagne aussi d'un volet plus large s'appuyant sur la promotion, la formation et l'accompagnement des entreprises, notamment des plus petites.

(10) Agence nationale de la sécurité des systèmes d'information.

La PPIE s'inscrit dans la dynamique de la République numérique en acte (2015) et vise à instaurer un cadre économique de confiance en mettant notamment en avant la liberté d'innover pour libérer le potentiel numérique. L'État a dans cette optique créé les outils d'accompagnement pour les entreprises, avec la mise en place de France Num, portail de la transformation numérique pour aider les TPE et PME, la création de la French Tech[11] à destination des startups (fond BpiFrance[12] de 200 m d'euros) et la création d'une filière des industries de sécurité, …

(11) La « French Tech » c'est le nom de l'écosystème des startups françaises qui désigne tous ceux qui travaillent dans ou pour les start-up françaises en France ou à l'étranger : les entrepreneurs en premier lieu, mais aussi les investisseurs, ingénieurs, designers, développeurs, grands groupes, associations, medias, opérateurs publics, instituts de recherche.

(12) Bpifrance gère des fonds d'investissements qui investissent en fonds propres ou quasi-fonds propres dans des start-up, des PME et des ETI françaises.

Les plus gros acteurs économiques, tels les opérateurs d'importance vitale (OIV) ou les secteurs d'activités d'importance vitale (SAIV) font l'objet d'une attention particulière de l'administration, en même temps que de contraintes spéciales, mais les TPE/PME ne sont pas oubliées et font aussi l'objet de mesures de protection, notamment celles qui sont considérées comme stratégiques. Dans cette catégorie figurent les TPE/PME détentrices de savoir-faire irremplaçables ou de technologies d'avenir. Tout l'enjeu de la politique de sécurité économique, dans laquelle le Service de l'information stratégique et de la sécurité économiques (SISSE)[13] et son réseau territorial des délégués à l'information stratégique et à la sécurité économiques (DISSE) jouent un rôle prépondérant, est d'identifier et de défendre ces actifs stratégiques que l'on peut considérer au niveau de l'État comme des « bijoux de famille ».

(13) Service à compétence nationale au sein de la Direction générale des entreprises du ministère de l'économie et des finances en charge de la sécurité économique et du pilotage en lien avec les autres ministères de la protection du potentiel scientifique et technique de la Nation.

Animée et portée par de nombreux acteurs étatiques ou privés, la PPIE est tournée vers l'ensemble des acteurs économiques du pays et notamment les TPE et PME. L'extrême dispersion de

© MINEFI

L'implantation décentralisée des spécialistes de la Gendarmerie nationale est en adéquation avec la dispersion géographique des TPE / PME sur le territoire national.

ces entreprises couplée à une culture de la sécurité économique moins développée, notamment dans le domaine cyber, rend parfois la portée du message moins audible. La Gendarmerie nationale, qui participe pleinement à la PPIE, possède tous les atouts pour jouer un rôle de premier plan dans le volet cybersécurité.

Le rôle de la gendarmerie dans la PPIE et notamment dans le volet cybersécurité

Avec son maillage territorial composé de 3 600 brigades et son modèle d'organisation pyramidale, la gendarmerie est certainement la dernière administration présente dans tous les territoires métropolitains et ultramarins. Force de police de pleine compétence (sécurité publique générale mais aussi service enquêteur chevronné avec le C3N[14] et les 2 000 enquêteurs spécialisés du réseau décentralisé « cybergend »), la gendarmerie possède son propre canal d'échange et de remontée d'informations, ce qui lui permet d'alerter rapidement les autorités et administrations partenaires et d'apporter des réponses directement aux entreprises.

(14) Centre de lutte contre les criminalités numériques de la Gendarmerie.

© Gendarmerie nationale

Présente à tous les stades du cycle de la PPIE (de la définition des objectifs au niveau des ministères, à la veille au niveau des régions et des départements, jusqu'à l'application des solutions arrêtées), la gendarmerie est bien souvent le premier ou dernier interlocuteur régalien des TPE/PME, notamment en matière de criminalité liée au cyber.

Grâce aux index statistiques de la criminalité, nous connaissons bien la forte implication de la gendarmerie dans la lutte judiciaire contre la cybercriminalité mais il est plus difficile de rendre compte de son implication dans le domaine de la prévention, notamment en faveur des nouveaux territoires numériques[15]. Afin de prévenir la criminalité cyber, la gendarmerie s'est engagée très fortement dans la diffusion d'une culture de la sécurité afin de développer, notamment chez les dirigeants de TPE et PME, un maximum d'actes réflexes minimaux. Cet effort en faveur de la prévention et de la coproduction de sécurité se traduit par le développement des différents réseaux de référents de la gendarmerie. Ainsi, dans le domaine de la sécurité économique, la gendarmerie consacre chaque année un réel effort de formation en faveur de ses 200 officiers et sous-officiers référents « sécurité économique protection des entreprises » (SECOPE) grâce aux formations de haut niveau dispensées à l'INHESJ[16], au CNFRO[17] et à l'Ecole européenne d'intelligence économique (EEIE). Les référents SECOPE, qui sont de véritables guichets uniques de la gendarmerie pour les TPE/PME, viennent enrichir l'offre de protection générée par les NTECH et les référents « sûreté » afin d'offrir une réponse de sécurité économique globale et intégrée. Dans ce dispositif déjà étoffé, il convient de souligner le rôle essentiel joué par des milliers de réservistes opérationnels ou citoyens qui sont non seulement des facilitateurs, découvreurs, apporteurs d'affaires mais aussi des capteurs inestimables et dévoués, constituant une formidable richesse de profils et d'expertises mobilisable au service de la Gendarmerie et des entreprises.

(15) Le territoire numérique est la transposition d'un espace géographique dans un espace numérique. Cette notion est née à la fin des années 1990, de la rencontre des territoires avec les technologies de l'information et de la communication, et avec la volonté de limiter la fracture numérique.

(16) Institut national des hautes études de la sécurité et de la justice.

(17) Centre national de formation au renseignement opérationnel.

La présence de la Gendarmerie sur l'ensemble de l'arc de crise (de la prévention cyber à la résolution judiciaire d'un acte cybercriminel) lui permet d'être un acteur important de la transformation numérique des entreprises notamment des TPE/PME. Aussi, en matière de lutte contre la cybercriminalité, la Gendarmerie s'inscrit-elle une fois de plus dans le classique « protéger, alerter et le cas échéant secourir » et exerce ses missions aux côtés des autres services spécialisés (dont le réseau des DISSE) tout en conservant et en utilisant les atouts conférés par son modèle d'organisation unique et sa longue tradition d'excellence.

AUTEUR

Le Lieutenant-colonel Roland Majorel, outre une Maîtrise de droit privé est titulaire d'un Master 2 (M2) intelligence économique (EEIE - Ecole Européenne d'Intelligence Economique). Il est auditeur à l'INHESJ. Après un parcours de commandement territorial (Compagnie et EDSR), il sert au sein de la direction générale de la gendarmerie nationale comme chargé de projet et en tant que chef de section. Il est depuis 2 ans mis à la disposition du MINEFI.

La chaîne de valeur
des PME/PMI, cible des atteintes à la sécurité économique

Par Jean-François Auzet et Stéphane Mortier

Dans ses relations avec le monde de l'entreprise, l'activité de la gendarmerie nationale porte essentiellement sur la prévention (la surveillance générale, les relations avec les décideurs économiques, les conférences de sensibilisation, les visites en entreprise). Pleinement inscrite dans cette politique publique, mise en place en 2004, la gendarmerie nationale a su tirer profit de son maillage territorial pour mettre en place un dispositif de sensibilisation du tissu économique à l'intelligence économique sur l'ensemble du territoire. Cette tâche, singulière pour l'institution, s'est totalement imbriquée dans ses missions régaliennes.

JEAN-FRANÇOIS AUZET

Lieutenant-colonel de gendarmerie. Chef de la section sécurité économique et protection des entreprises. DGGN

STÉPHANE MORTIER

Gendarme. Section sécurité économique et protection des entreprises. DGGN

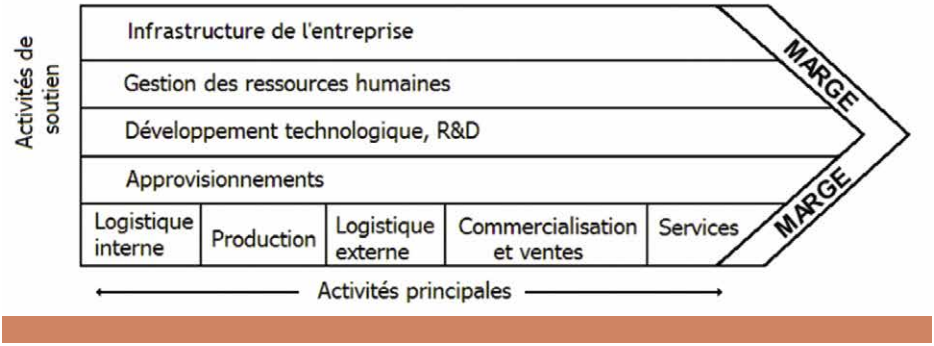
Plusieurs dizaines de milliers d'entreprises sont sensibilisées aux risques et vulnérabilités qui les menacent. L'intelligence économique, et plus particulièrement son volet sécurité économique, est une démarche que la gendarmerie offre aux entreprises afin qu'elles se préservent de toute forme de prédation. Cette mission est dévolue à la section sécurité économique et protection des entreprises (SECOPE) de la sous-direction de l'anticipation opérationnelle (SDAO) de la direction générale de la gendarmerie nationale (DGGN) qui s'appuie sur environ deux cents référents, formés, présents partout sur le territoire national, outre-mer et gendarmeries spé-

cialisées (transports aérien, maritime, air, armement) compris.

Toute entreprise poursuit plusieurs objectifs : économiques, sociétaux et réputationnels. La création de valeur impliquant la compétitivité de l'entreprise répond aux objectifs économiques ; la contribution à la vie de la société (emploi, fiscalité, responsabilité sociale de l'entreprise) aux objectifs sociétaux ; la recherche de notoriété, la conformité, le développement et l'accroissement de la taille de l'entreprise aux objectifs réputationnels. Les PME/PMI, à l'instar de tout acteur économique, évoluent alors dans un écosystème, dans un environnement (concurrentiel, normatif, technologique, social, sécuritaire, politique, informationnel,...) qui leur est propre et qu'elles doivent maîtriser pour réaliser leurs objectifs. Au sein de cet environnement global se situe la chaîne de valeur. Cette dernière contient les différentes activités de l'entreprise utiles à la création de valeurs. Il convient d'ajouter à ces activités la logistique entrante et la logistique sortante, c'est-à-dire toutes les étapes reliant les fournisseurs de biens ou services à l'entreprise ainsi que toutes les étapes reliant l'entreprise aux clients, sans omettre les prestataires, y compris les banques, assurances et même les pouvoirs publics.

La chaîne de valeur ainsi entendue constitue une cartographie utile à toutes les parties prenantes de la création de valeur, mais aussi à tout acteur malveillant qui souhaiterait nuire à une PME/PMI. En effet, que ce soit au niveau de la logistique entrante, des activités internes ou de soutien, de la logistique sortante, une multitude d'atteintes est possible.

Dans le cadre de sa mission de sécurité économique, la gendarmerie nationale distingue plusieurs catégories d'atteintes



© MINEFI

pouvant être menées, n'importe où, sur la chaîne de valeur d'une entreprise en vue de la déstabiliser, de l'affaiblir ou de la spolier. Les référents « sécurité économique et protection des entreprises » de la gendarmerie nationale ont pour mission de sensibiliser les PME/PMI aux risques liés à ces atteintes. Dans un contexte de guerre économique, aucune entreprise n'est à l'abri d'une prédation ou d'une déstabilisation. Acteurs économiques, société civile, puissances étrangères, cybercriminels sont autant d'acteurs potentiellement hostiles, quelles que soient leurs motivations. Les conséquences des atteintes à la sécurité économique sont systématiquement un affaiblissement de l'entreprise et donc une exposition plus grande à la prédation. Elles emportent souvent des conséquences sur la trésorerie des entreprises, point névralgique de leur stabilité et de leur capacité de résilience.

Ces atteintes sont donc catégorisées en huit familles dont voici les principales caractéristiques :

– Les **atteintes physiques** qui vont essentiellement concerner les intrusions, destructions, vols de matériels et de matériaux. La difficulté réside dans la détection des raisons de l'atteinte : simple vol crapuleux avec effraction ou vol ciblé visant un affaiblissement ou une appropriation de données, de savoirs,… stratégiques de l'entreprise victime ? Régulièrement et depuis plusieurs années, des entreprises sont victimes de vols de cuivre. Il peut s'agir soit d'un vol crapuleux en vue de revendre un matériau dont le cours est élevé au moment du méfait (vol de bobines de fils, de lingots,…) soit d'un vol ciblé visant à nuire de façon plus diffuse à l'entreprise victime (privation de matière première, mise hors d'utilisation du système électrique,…). Prenons l'exemple d'une intrusion dans une entreprise pour y voler de l'outillage se trouvant être remisé dans un local abritant un prototype non encore présenté publiquement. S'agit-il d'un simple vol d'outillage ou de la dissimulation de prises de vue du dit prototype ? En matière économique, la criminalité sait être particulièrement astucieuse. C'est la raison pour laquelle le recueil, l'analyse et le recoupement des faits peuvent donner le véritable sens d'un délit.

– Les **désorganisations et fragilisations** sont des actions venant de l'extérieur. On retrouve dans cette catégorie la raréfaction des approvisionnements, les nouvelles concurrences étrangères ou encore le harcèlement en contentieux. La raréfaction des approvisionnements peut revêtir différents aspects. La fibre de carbone est essentiellement fabriquée par deux acteurs dans le monde : l'un est américain, l'autre japonais. Le secteur de l'aéronautique est un

grand consommateur de cette matière. Les avionneurs européens sont donc dépendants de producteurs étrangers même si ces derniers peuvent produire en Europe. Une rupture d'approvisionnements est une menace réelle qu'il convient, aux sous-traitants et donc aux PME/PMI du secteur aéronautique, d'anticiper. Quant au harcèlement en contentieux, il concerne des procédures contentieuses devant des juridictions nationales ou étrangères (parfois également des arbitrages), généralement sur des motifs fallacieux, afin de faire perdre du temps, de l'énergie et des liquidités à l'entreprise visée.

– Les **risques cyber** sont aujourd'hui un véritable fléau dans les entreprises. Faut-il rappeler les ransomwares *WannaCry* et *NotPeytia* qui, en mai et juin 2017, ont touché plusieurs centaines de milliers d'entreprises dans plus de cent-cinquante pays à travers le monde ! Il en va de même des escroqueries au faux président ou au faux virement international (FOVI) dont des centaines d'entreprises ont été victimes sur le territoire national ces dernières années. Par ailleurs, les entreprises détiennent aujourd'hui un patrimoine dématérialisé de plus en plus conséquent qu'il s'agit de protéger. Les données personnelles font partie de ce patrimoine et le RGPD illustre à quel point la question est prise en considération. Se prémunir de la cyber-malveillance implique certes le recours à des solutions de cybersécurité mais force est de constater que les comportements humains dans la majeure partie des cas, constituent la faille la plus importante des systèmes de protection… Sensibiliser le personnel de l'entreprise permet une limitation du risque et réalise un premier pas dans la cybersécurité. Aujourd'hui, si l'on peut constater que toutes les grandes entreprises ont pris conscience de ce risque et ont déployé des moyens pour s'en protéger, y compris sur le plan assurantiel, le chemin est encore long pour les PME/TPE dont les dirigeants manquent de temps et de ressources à consacrer à ce sujet… tant qu'ils n'en sont pas victimes.

– Les **risques financiers** ne constituent généralement pas d'infraction au sens du droit pénal mais sont des outils de prédation par excellence. L'injection de capitaux, étrangers notamment, dans une entreprise peut déboucher, à terme sur une délocalisation, un changement dans la gouvernance de l'entreprise, voire une cessation d'activité. De plus, certains investissements peuvent sembler stratégiques pour les uns, anecdotiques pour les autres. Le phénomène d'achat de terres agricoles ou de domaines viticoles par des investisseurs étrangers a fait couler beaucoup d'encre ces dernières années. Y-a-t-il, derrière ce phénomène,

des stratégies d'appropriation, de réorientation du marché ? Racheter ou injecter des capitaux dans une PME/PMI française peut cacher une tentative de prédation sur un client de cette entreprise. D'où la nécessité pour les entreprises de maîtriser au mieux leur environnement global et leur chaîne de valeurs. L'investissement étranger est toutefois contrôlé en France pour certains secteurs d'activité considérés comme stratégiques.

– Les **atteintes aux savoir-faire** sont relatives, essentiellement, aux questions de propriété intellectuelle et par conséquent à la contrefaçon. On y retrouve également les problématiques liées aux transferts de technologies. En matière de contrefaçon, le premier devoir d'une PME/PMI est d'être en mesure de détecter si ses produits sont contrefaits. Cela passe par l'organisation d'une veille régulière sur son marché et dans son environnement. Breveter ne suffit pas à se protéger, encore faut-il détecter et identifier le contrefacteur puis intenter une action en contrefaçon.

– Les **atteintes à la réputation** ont pris une dimension considérable avec le développement des moyens de communication au premier titre desquels les réseaux sociaux. Il n'est pas rare de voir la société civile (ONG, associations, collectifs,…) militer contre une entreprise ou un secteur d'activité. Ce type d'action peut mettre en difficulté toute une filière économique voire conduire à la disparition de petites entreprises.

Quant à l'identité numérique de l'entreprise et son positionnement sur les réseaux, elle peut être rapidement mise à mal si une surveillance permanente n'est pas opérée et si des réponses adaptées ne sont immédiatement diffusées en cas d'attaque informationnelle. Huile de palme, glyphosate, diesel, alimentation animale, bien-être animal, contrats dans des pays en conflits sont autant d'arguments utilisés pour nuire, à tort ou à raison, à une entreprise.

– Les **fragilités humaines** ne sont bien évidement pas à écarter du spectre des atteintes à la sécurité économique. Pour qu'il y ait corruption, il faut un individu qui se laisse corrompre… Les salariés indélicats, qui nuisent à l'ambiance de travail ou à la productivité pour des raisons qui presque systématiquement ne sont pas connues, engendrent des préjudices graves aux entreprises et plus encore aux petites entreprises. Le débauchage de personnel est également une menace pour les entreprises qui ont concentré le ou les savoir-faire entre les mains d'un seul employé. Quid s'il part à la concurrence ? Les clauses de non-concurrence dans le contrat de

travail peuvent limiter le risque mais ne sont pas une solution miracle. La gestion des ressources humaines est particulièrement impliquée dans ces problématiques.

– Les **intrusions consenties** enfin sont des facteurs de risques très importants. Permettre à des personnes de rentrer dans l'entreprise, qu'elles soient stagiaires, clients, fournisseurs, prestataires, délégations officielles, délégations étrangères...implique des mesures de sécurité spécifiques (parcours de notoriété, limitation des accès – physiques et informatiques – clauses de confidentialité, tenue d'un registre visiteurs,…). Les étudiants stagiaires ayant copié et diffusé des données sensibles, les prestataires ayant subtilisé un document ou réalisé une prise de vue, un visiteur récoltant discrètement un échantillon d'un produit quelconque ou tout simplement avoir laissé à la vue d'une personne étrangère à l'entreprise une technique de fabrication sont autant d'exemples de risques liés aux intrusions consenties.

Au travers de ce bref panorama des atteintes à la sécurité économique, on constate que la chaîne de valeur peut être attaquée partout, en tout temps. Une culture de la sécurité économique, sans tomber dans une paranoïa démesurée, s'impose aux PME/PMI afin de limiter les risques. C'est dans cette optique et dans le cadre de la politique publique d'intelligence économique que les « référents sécurité économique et protection des entreprises » de la gendarmerie nationale sensibilisent les entreprises. Aucune solution clé en main n'existe mais permettre la prise de conscience des risques inhérents à l'environnement et à la chaîne de valeur des entreprises constitue l'un des fondements de la sécurité économique.

Dans un contexte ultra concurrentiel et de guerre économique sans retenue, la sécurité économique doit être perçue aujourd'hui par les dirigeants comme une autre condition de réussite de leur développement. Bien que la compétition économique ait toujours existé, la numérisation de l'économie lui donne aujourd'hui une nouvelle dimension en augmentant de manière exponentielle les conséquences dommageables. Des solutions de protection existent. Leur appropriation par les dirigeants devient un enjeu immédiat. L'un des moyens simples et opérationnels de cette appropriation pourrait résider dans l'implication du réseau des experts-comptables. En effet, ces derniers sont aussi en contact permanent avec les entreprises et leurs apportent nombre de conseils en matière de gestion des risques. Pourquoi ne pas imaginer dès lors qu'ils apportent également un conseil en matière de

(1) Diagnostic d'intelligence économique et de sécurité des entreprises.

cyber-sécurité, à travers par exemple un outils de diagnostic du type DIESE[1], à l'élaboration duquel l'Ordre des experts-comptables avait notamment contribué.

AUTEUR

Jean-François AUZET, lieutenant-colonel de gendarmerie, est diplômé de l'ESM Saint-Cyr ainsi que de l'executive MBA de l'EMLyon et du master 2 d'intelligence économique de l'école européenne d'intelligence économique de Versailles. Après une période de disponibilité pendant laquelle il a occupé des fonctions de direction en entreprises privées, il est aujourd'hui chef de la section sécurité économique et protection des entreprises à la Direction générale de la gendarmerie.

AUTEUR

Stéphane MORTIER, gendarme, œuvre à la section « sécurité économique et protection des entreprise » de la DGGN. Diplômé en sciences politiques, en sociologie et en politique internationale de l'Université libre de Bruxelles, il est également diplômé de l'École de Guerre Économique et termine un doctorat en sciences de gestion à l'Université Paris 1 Panthéon-Sorbonne.

Il a publié Au coeur de l'unité africaine, le droit OHADA – Harmonisation du droit des affaires et intelligence économique, Uppr, 2017

UNE NOUVELLE ÉCOSPHERE CRIMINELLE QUI SUSCITE UNE ADAPTATION DES DISPOSITIONS LÉGISLATIVES

Les technologies de l'Internet suscitent des paradoxes. L'utilisateur expose sa vie privée sur les réseaux tout en demandant une protection quant à des pratiques commerciales relatives à ses données personnelles.

Les capacités données par la structure de la toile et l'architecture logicielle qui y est déployée sont le substrat d'une nouvelle écosphère criminelle. Son caractère diffus, opaque, multimodal et son évolutivité mettent en échec des législations strictement nationales.

Faces à ces nouvelles menaces, l'état de droit s'est adapté par l'évolution de son arsenal juridique, notamment celui qui réprime les atteintes aux traitements automatisés des données, et en prenant des mesures assurant la coordination de services d'investigations spécialisés, tant au niveau national qu'international, et en créant au sein du ministère de la justice des instances dédiées à cette nouvelle criminalité.

Cybersécurité :
les nouveaux défis du monde économique

Par Xavier Leonetti

Internet fait désormais partie de nos vies. Tous les jours, à chaque instant, nous sollicitons cet assistant multifonctions dans la plupart des tâches de notre vie quotidienne (rendez-vous, démarches administratives, réservations de sorties, …). La vie sans le numérique ne nous paraît plus possible. Mais à quels risques ? La vague du progrès numérique semble parfois nous submerger, entraînant notre abandon à ce nouveau maître du quotidien.

XAVIER LEONETTI

Magistrat
Juridiction inter-régionale spécialisée de Marseille

Le recours massif aux nouvelles technologies va souvent de pair avec une autre forme d'abandon liée à une vigilance moindre sur les réseaux sociaux comme si le filtre des écrans nous protégeait de toutes menaces. Ainsi, dans ce monde virtuel, chacun adopte des comportements qu'il n'aurait pas dans la vie réelle. Par exemple, s'imagine-t-on distribuer sur la voie publique des prospectus décrivant notre vie intime, nos dates de départ ou de vacances ou le dernier plat que l'on vient de manger ?

Évidemment non, pourtant qui pourrait affirmer ne l'avoir jamais fait. En cela, nous sommes pour la plupart les victimes d'un « privacy paradoxe » qui nous conduit d'un côté à exposer notre vie privée aux yeux de tous, tout en réclamant de l'autre toujours plus de protection et de respect de notre intimité.

Mais un tel comportement n'est pas sans conséquences. En effet, la confiance trop grande des internautes est souvent à l'origine d'escroqueries, de fraudes ou de rançonnage.

Ainsi, plus de 90 % des cyberinfractions recensées chaque année par l'Observatoire national de la délinquance et des réponses pénales (ONDRP) sont des escroqueries et des attaques financières. C'est dire qu'à l'image de l'économie réelle qui repose sur la confiance, l'économie souterraine dolosive qui prospère sur internet se nourrit d'un manque de vigilance et de nos failles de sécurité personnelles.

Cybercriminalité : les nouveaux chemins du crime

Le monde criminel s'est très tôt saisi des opportunités numériques. Jamais, sans doute, le prédateur n'a été aussi près de sa victime puisqu'au moyen des smartphones et des objets connectés il est partout et constamment avec elle. Mais, jamais aussi le délinquant n'a été aussi loin de son juge, ne serait-ce qu'en raison des frontières juridiques et de la lenteur de la coopération judiciaire comparée à la vitesse des transactions sur la Toile.

Ainsi, depuis dix ans la délinquance traditionnelle vit au rythme des innovations commerciales et économiques. Dans un premier temps, les banques se sont ouvertes à leurs clients sur le credo « *j'aime ma banque* », supprimant de ce fait les portiques de sécurité et logiquement l'argent détenu aux guichets. Les auteurs de vols à main armée ont naturellement reporté leur attention sur les liquidités détenues par les commerces de proximité (tabac, presse,...).

Aujourd'hui, une seconde évolution est en cours sous l'effet de l'introduction dans nos smartphones et nos cartes bleues de puces de paiement sans contact. Les paiements virtuels se généralisent, les caisses des commerces se vident progressivement et l'extorsion directe de liquidités devient une infraction en voie de diminution.

Dans le même temps, la « révolution numérique » offre une extraordinaire opportunité pour la criminalité et la délinquance. La cible principale devient alors la donnée (la « data ») détenue par une personne ou une entreprise. Désormais, afin d'obtenir des données bancaires, des virements de fonds ou de valeurs financières, on menace, rançonne et escroque. Internet ne permet pas simplement un transfert de délinquance entre les mondes réel et virtuel. Il s'agit également d'une révolution industrielle de « l'écosystème criminel » qui développe désormais des outils de délinquance de masse, permettant en un clic d'infecter ou d'escroquer des milliers de victimes.

Ainsi, la matière cybercriminelle est aujourd'hui définie au travers de trois grandes catégories :

– La première est relative aux infractions liées aux systèmes d'information et de

traitement automatisé des données (STAD). Il s'agit, par exemple, d'intrusions sur un serveur informatique ou de piratage de données. Ce type d'infraction concerne tout particulièrement les grands groupes ou les TPE/PME développant des solutions technologiques particulièrement innovantes. À cet égard, Internet et les réseaux sociaux facilitent les « vols » de données

© Cyber security concept By tippapatt File #: 162645021

L'apparition d'une cyberdélinquance de masse oblige les entreprises à promouvoir une hygiène reposant sur la mise place d'outils de protection et la formation des personnels à des actes de prévention simples mais efficaces notamment quant à la gestion des mails, mots de passe et des objets connectés personnels (clés USB, notebook, smartphones).

lesquels concourent souvent à des formes d'espionnage économique.

– La seconde catégorie regroupe les infractions liées aux formes « traditionnelles » de criminalité qui utilisent internet et les nouvelles technologies de l'information et de la communication (NTIC) comme étant de nouveaux modes opératoires. Rappelons que les entreprises représentent 77,4 % des victimes d'escroqueries. Par exemple, les entreprises ont longtemps été victimes de la fraude dite « au Président ». Celle-ci consiste à user de fausses demandes de paiement en usurpant l'identité d'un dirigeant de l'entreprise. Par son intensité, ce pillage organisé met en danger la survie financière des entreprises victimes. Dès 2016, les actions de prévention mises en œuvre par les services de police et de gendarmerie ont permis d'infléchir la courbe de ces infractions. Néanmoins, les escrocs renouvellent sans cesse leurs techniques et pratiquent aujourd'hui de nouvelles formes d'atteintes (par exemple le « rançonnage par déni de service » consistant à bloquer les outils informatiques d'une entreprise avant de lui réclamer une rançon).

– La troisième catégorie présente les infractions commises par internet relatives à la dignité ou à la personnalité et les atteintes sexuelles commises par ce même biais. Dans ce cas, les entreprises doivent principalement veiller au respect de la protection des données, de l'image et de la vie privée de leurs salariés. En la matière, les atteintes à la réputation entre dirigeants et employés ont tendance à se multiplier sur les réseaux sociaux.

Cybersécurité : la mobilisation des services de l'État

En écho à ces nouvelles menaces, le droit s'est adapté tandis que les services de sécurité et de Justice ont progressivement fait évoluer leurs modes d'organisation et d'investigation. Ainsi, l'arsenal pénal permettant de réprimer les comportements cyberdélinquants s'est particulièrement étoffé, notamment depuis l'adoption de la LOPPSI2 du 14 mars 2011. Par exemple, l'accès ou le maintien frauduleux dans un système de traitement automatisé de données (C. pén., art. 323-1, al. 1er) permet de réprimer le phishing qui consiste à soutirer des informations personnelles à des internautes en leur envoyant un courriel usurpant l'identité d'une banque ou d'un site marchand (TGI Paris, 2 sept. 2004). De même, une personne peut être poursuivie pour sa participation à un groupement de pirates (art. 323-4 du Code pénal), en l'espèce lorsqu'il est établi que les participants n'ignoraient pas que les informations échangées avaient pour finalité de commettre des atteintes au système informatique d'accès à *Canal*

plus (T. corr. Carpentras, 25 juin 2004).

Du point de vue de l'adaptation des structures de l'État aux nouveaux modes d'actions criminels, dès 2013, des travaux ont été engagés par le ministère de l'Intérieur afin de renforcer et de mieux coordonner les moyens d'actions en matière de prévention et de lutte contre la cybercriminalité. Ainsi, de manière non-exhaustive, il convient de souligner que la police et la gendarmerie nationales disposent de cyberenquêteurs dont la spécialité croît selon le niveau d'infraction.

Par exemple, la police nationale s'est dotée d'une sous-direction de lutte contre la cybercriminalité. De même, au sein du Pôle judiciaire de la gendarmerie nationale (PJGN) la division de lutte contre la cybercriminalité (DLCC) devenue le Centre de lutte contre les criminalités numériques (C3N) dispose de compétences uniques en matière de cybercrime destinées à appuyer les unités locales.

Par ailleurs, l'action de la gendarmerie se trouve renforcée par l'apport du réseau de la « réserve citoyenne cyberdéfense » placée sous l'autorité du ministère de la Défense.

La direction générale de la sécurité intérieure (DGSI) dispose de compétences spécifiques notamment s'agissant de cyberradicalisation ou de lutte contre le cyberespionnage.

Rappelons d'ailleurs que les articles 706-102-1 à 706-102-6 du Code de procédure pénale créent une nouvelle catégorie de technique d'enquête, relative aux captations des données informatiques. Il s'agit d'un dispositif ayant pour objet, sans le consentement des intéressés, d'accéder en tous lieux à des données informatiques, de les enregistrer, les conserver et les transmettre.

Au sein du ministère de la Justice, depuis septembre 2014, des services spécialisés ont compétence pour connaître de ces infractions. Ainsi, les services du parquet de Paris ont été réorganisés afin d'être plus efficaces dans le traitement des dossiers financiers, de cybercriminalité. Désormais, le parquet financier de Paris comporte un pôle cybercriminalité, « section F1 », au sein de la division économique, financière et commerciale. Elle traite plus particulièrement des dossiers d'atteintes aux systèmes de traitement automatisé de données commises à l'encontre des services de l'État et des entreprises situés à Paris.

Au plus près des territoires, les juridictions interrégionales spécialisées (JIRS) ont également à connaître de nombreux cas de cybercriminalité. Aussi, plusieurs d'entre elles se sont dotées de magistrats

référents en matière de cybercriminalité.

Cyber « bonsens » : des gestes simples pour une protection maximale

À l'image des précautions en matière d'hygiène et de sécurité, il convient d'adopter des réflexes de «cyber-bon sens», que ce soit dans la vie professionnelle ou privée.

1. « *Fermer sa porte* » : Il convient de bien choisir son pare-feu et son anti-virus. À l'image du monde réel, l'utilisation d'une porte blindée réduit les risques de cambriolage.

2. « *Ne pas laisser traîner ses clefs* » : Selon l'étude Privacy Index 2016, 62 % des internautes ne modifient pas régulièrement leur mot de passe (71 % en France).

3. « *Ne pas laisser entrer un inconnu* » : Il convient de ne pas télécharger un logiciel inconnu et de ne pas ouvrir de pièces jointes provenant d'une personne inconnue.

4. « *L'habit ne fait pas le moine*: Il s'agit là de ne pas répondre aux appels/courriels imitant ceux d'un organisme officiel qui demandent, par exemple, de transmettre des coordonnées bancaires.

5. « *Ne pas croire tout ce que l'on dit* » : Vérifier le texte d'une information afin de détecter les fausses nouvelles et les rumeurs.

6. « *Ne pas se précipiter* » : Très souvent la cyberattaque joue sur le fait que les internautes consultent rapidement leurs courriels et cliquent trop vite sur un lien, lequel renvoie vers un faux site web.

7. « *Payer en toute sécurité* » : Utiliser une solution technique de paiement en ligne, de type e-carte bleue ou paiement par solution « 3DSecure ».

8. « *Pour vivre heureux, vivons cachés* » : Sans devenir un inconditionnel du secret, une certaine discrétion est recommandée sur les réseaux sociaux.

9. « *Rester vigilants* » : Pour cela, il convient de se sensibiliser aux cybermenaces et de signaler les comportements suspects et les contenus illicites sur la toile.

10. « *En cas de problème appeler à l'aide*: Trop souvent les victimes d'attaques n'osent pas se signaler ou déposer plainte soit parce qu'elles ont honte de leur crédulité, soit parce qu'elles pensent que cela ne servira à rien.

AUTEUR

Xavier Leonetti intègre l'école des officiers de la gendarmerie nationale en 2002. Après un commandement opérationnel à la compagnie de gendarmerie départementale de Castellane, il revient à l'école des officiers de la gendarmerie nationale comme officier professeur en 2008. Il rejoint en 2010 la direction générale en tant que responsable du service national « sécurité et intelligence économiques ». Il intègre les rangs de la magistrature en 2016 en tant que substitut du procureur au parquet général d'Aix-en-Provence puis rejoint en 2017 la Juridiction inter-régionale spécialisée de Marseille, Criminalité organisée.

Docteur en droit, il enseigne au sein du Master 2 « Management de l'information » auprès de l'Université Paul-Cézanne – Aix-Marseille III. Il a publié des ouvrages : « Guide de cybersécurité », Paris, l'Harmattan, octobre 2015. – « La France est-elle armée pour la guerre économique ? », Paris, Armand Colin, avril 2011. – « Les outils de l'intelligence économique », Presses de Science-Po Aix, novembre 2000.

© Antivirus and firewall concept By alphaspirit. File #: 40120476

UN NOUVEAU RÉGIME DE PROTECTION JURIDIQUE DE L'INNOVATION

Le législateur a sanctuarisé les actifs informationnels d'une entreprise. Le droit a consacré une norme unifiée qui permet de situer le niveau de confidentialité de « savoir-faire » ou d'informations commerciales spécifiques. Elle est assortie de conditions précises mais préserve des exceptions liées à l'ordre public et au droit d'informer.

Ces savoirs sont de tous ordres : algorithmes, plan business, fichiers clients, pour peu qu'ils participent à la valorisation d'actifs informationnels et technologiques propres à l'entreprise. Il faut toutefois, pour s'en prévaloir devant une juridiction, établir que les mesures propres à assoir cette confidentialité ont bien été prises et que le caractère particulier des données ou des pratiques a bien été distingué et valorisé.

Le secret des affaires : un nouvel outil de protection numérique

Par Olivier de Maison Rouge

La loi n° 2018-670 du 30 juillet 2018, relative à la protection du secret des affaires, a contribué à donner corps à un nouveau régime de protection juridique de l'innovation, notamment à destination des ETI, PME-PMI et TPE, en complément des règles relatives à la sécurité des systèmes d'information contenues sous les articles 323-1 et suivants du Code de commerce.

En effet, au-delà de la répression pénale des délits d'intrusion et de piratage informatique des systèmes d'information, le législateur a voulu sanctuariser commercialement les créations et « inventions » numériques qui ne pouvaient recevoir de protection par la propriété intellectuelle.

OLIVIER DE MAISON ROUGE

Avocat
Docteur en droit.
École des relations internationales (ILERI)

Avec cette approche, le secret des affaires se veut donc un outil supplémentaire permettant de renforcer la compétitivité et l'innovation de l'entreprise, quelle que soit sa taille, ainsi que la préservation robuste de ses actifs informationnels[1]. Plus largement, il s'agit d'assurer l'avantage technologique de son titulaire dans une économie de la data exposée aux prédateurs économiques.

(1) Directive, préambule 1) et suivants.

Une définition couvrant les actifs immatériels

Toute publicité des délibérations, en matière de stratégie ou de tactique, renseigne adversaires et rivaux. La transparence nuit à l'action, que le secret, lui, favorise.
Roger-Pol DROIT

Éléments immatériels du secret protégé :
Cela pouvait être une gageure de définir, de la manière la plus large possible, ce qui par principe n'est connu que d'un petit nombre

d'initiés. Pourtant, relevant ce défi, le droit a consacré une norme juridique unifiée afin « d'étalonner » cette notion confidentielle constituée de R & D, « de savoir-faire et d'informations commerciales non divulguées » pour reprendre le titre de la directive européenne que la loi a transposée.

Les secrets d'affaires sont ainsi identifiés sous trois conditions cumulatives :

1) non connus du grand public et/ou du secteur professionnel concerné ;

2) ayant une valeur commerciale, réelle ou potentielle, parce que secrets ;

3) et faisant l'objet de mesures spécifiques destinées à les garder confidentiels.

Cela peut être un algorithme, une méthode de calcul ou d'analyse, un plan de développement, une base de prospects, un fichier clients, une liste de fournisseurs, une stratégie commerciale comme le lancement d'un nouveau produit, un business plan, des accords commerciaux, un schéma organisationnel, la composition d'une recette, d'un parfum, …

Sous cette définition commune et extensive, le secret des affaires est un support juridique alternatif permettant de consolider la sécurité des actifs informationnels et technologiques de l'entreprise.

Exceptions au secret :

Par dérogation, le secret des affaires n'est toutefois pas protégé lorsque :

– le droit en impose la communication, notamment en cas de contrôle ou d'enquête des autorités judiciaires ou administratives ;

– le secret est divulgué par des journalistes dans le cadre de la liberté d'expression et du droit d'informer ;

– un lanceur d'alerte révèle de bonne foi, de manière désintéressée et dans le but de protéger l'intérêt général, une activité illégale, une fraude ou un comportement répréhensible ;

– il s'agit d'empêcher ou de faire cesser toute atteinte à l'ordre public, à la sécurité, à la santé publique et à l'environnement ;

– il a été obtenu dans le cadre de l'exercice du droit à l'information des salariés ou de leurs représentants.

La protection de la technologie par le secret des affaires

Le vrai secret est une connaissance que son détenteur rend délibérément inaccessible. (…)

Le secret, suivant le cas, interdit de connaître, de prouver, de diffuser ou de reproduire l'information qu'il protège voire de la modifier, comme lorsqu'un mot de passe empêche le sabotage de données informatiques.
François-Bernard HUYGHE

La protection de l'algorithme par le secret des affaires :
Moteur de l'économie immatérielle, l'algorithme participe de manière fondamentale au cycle du « raffinage » des données brutes dont il se nourrit pour parvenir à un résultat pertinent. Cela se traduit par le *data mining* et le *big data*, d'une part, et le *machine learning*, d'autre part. Ce n'est toutefois qu'une formule mathématique, grille d'analyse vertueuse telle un athanor, qui toutefois n'est pas éligible au rang des droits de propriété intellectuelle en tant que tel, sauf à s'intégrer dans un logiciel (type *Saas* par exemple).

S'il emprunte des caractères au droit d'auteur ou au droit des logiciels, selon son niveau d'intégration, il n'est pas protégeable séparément.

Aussi, en application de la directive sur le secret des affaires qui renforce la préservation des actifs immatériels de « l'économie de la connaissance », s'il répond aux conditions essentielles et cumulatives, l'algorithme peut et doit être préservé par la confidentialité relevant du secret des affaires[2].

(2) Voir aussi « La valorisation des données numériques par la protection juridique des algorithmes » par Maryline BOIZARD, in Dalloz IP/IT, février 2018, pp. 99-103.

Cela vaut plus largement pour toute « création » numérique.

Secret des affaires et données personnelles :
D'une certaine manière, l'approche relative à la protection des données confidentielles relevant du secret des affaires n'est pas une démarche éloignée de celle instituée par le RGPD applicable depuis le 26 mai 2018.

Elle diffère néanmoins par ce besoin d'identification préalable des secrets de l'entreprise qu'il lui appartient de désigner au vu de la définition ci-dessus, tandis que le RGPD protège les données des tiers, strictement désignées par la loi.
En réalité, le RGPD, c'est la protection des données des tiers ; le secret des affaires, c'est la protection des données de l'entreprise.

En outre, le mode de protection des données personnelles est beaucoup plus contraint selon des obligations règlementaires (registre, data protection officier (DPO), analyse d'impact, consentement, *privacy by design* …), quand le choix des moyens de protection raisonnable est à la discrétion de l'entreprise ; mais par souci d'efficacité opérationnelle, la politique de protection des données personnelles peut inspirer celle organisant la sécurité des secrets d'affaires de l'entreprise, ne serait-ce qu'en désignant un seul et même DPO.

En outre, comme dans un fichier clients (B to C), par exemple, le secret des affaires et la protection des données personnelles peuvent se chevaucher. Un secret d'affaires peut donc être constitué de données personnelles.

La notion de secret de l'entreprise suppose l'identification technique et juridique de biens immatériels valorisés et la définition d'une architecture de la préservation de leur accès par les seules personnes habilitées à en connaître.

La protection du secret des affaires par la technologie

Si vous voulez que l'on garde votre secret, le plus sûr moyen est de le garder vous-même. SENEQUE

Des « mesures de protection raisonnable »

Seule une entreprise ayant mis en place en amont des « protections raisonnables » (article L ; 151-1 du Code de commerce) pour garder leurs informations confidentielles pourra faire valoir leurs droits devant les tribunaux et revendiquer la protection légale du secret des affaires.

Si elle ne le fait pas, elle risque de ne pas pouvoir invoquer la protection des secrets d'affaires devant le juge qui écartera la qualification de secret des affaires et la protection juridique qui va de pair. Autrement dit, le texte suppose que les entreprises prennent en charge leur protection en amont, selon une politique de sécurité (notamment PSSI, mais aussi juridique) qu'il leur appartient de définir en fonction de la nature des informations qu'elle entend protéger.

Par conséquent, une protection efficace du secret des affaires suppose la mise en œuvre d'un processus composé de trois étapes-clés :

1) l'identification des informations confidentielles (sachant que l'économie supposant la souplesse et la fluidité, toutes les informations n'ont pas vocation à être protégées) ;

2) leur classification selon leur niveau de sensibilité ;

3) l'organisation de leur protection par des moyens adaptés et la gestion des droits d'accès et de disponibilité.

Protections innovantes

Une fois ce travail accompli, il faut également délimiter le périmètre des personnes ayant accès à ces informations et juger de leur « besoin d'en connaître ». La direction devra allouer à chacune des personnes autorisées des identifiants et des codes d'accès spécifiques, non sans avoir préalablement cloisonné les informations classifiées sur le

réseau informatique.

En complément, afin de créer une traçabilité des accès, il peut être imaginé de nombreux ressorts empruntés aux technologies innovantes telles que :

– l*a blockchain*, privée en l'occurrence, pour assurer une date certaine et un schéma organisationnel décentralisé de classification des informations sensibles ;

– des services d'identité numérique et d'authentification forte, tels que définis par la règlementation européenne, destinés à régir strictement les droits d'accès électroniques ;

– le recours au coffre-fort numérique pour conserver les données confidentielles ;

– l'utilisation du chiffrement des données.

Au-delà de la simple attraction des nouvelles technologies qui offrent quelques garanties certaines, il s'agit également, le cas échéant, de rendre passible du Code pénal (art 323-1 et s) les atteintes susceptibles d'être portées aux données sensibles : intrusion, extraction, reproduction, … En effet, la loi du 30 juillet 2018 n'a pas intégré de nouvelle sanction pénale relative à la violation du secret des affaires. Dès lors, il s'agit de créer un espace de confinement numérique dont la transgression, indépendamment de la qualification des données, constitue un délit répréhensible.

AUTEUR

Olivier de MAISON ROUGE est avocat spécialisé dans les domaines du numérique, de la protection des données, du secret des affaires, de l'intelligence stratégique et sécurité économique.

Docteur en droit. Diplômé de Sciences politiques, il est professeur associé à l'Ecole des relations internationales (ILERI) et à l'Ecole de Guerre Economique (EGE). Il intervient régulièrement à l'IHEDN et à l'Ecole Nationale de la Magistrature (ENM). Il est membre de la commission permanente « secrets d'affaires » de l'AIPPI, du comité d'éthique du syndicat français de l'intelligence économique (SYNFIE) et vice-Président de la Fédération Européenne des Experts en Cybersécurité (EFCSE). Enfin, il est rapporteur du Groupe de travail (Ministère de l'Economie et des Finances / SISSE) sur la transposition de la directive n°2016/943 du 8 juin 2016 sur le secret des affaires.

Ayant été amené au cours de sa carrière à défendre des entreprises confrontées aux tentatives d'espionnage économique et ingérences économiques (notamment pillage technologique), il a développé une véritable doctrine en matière de contre-mesures juridiques et de protection du patrimoine informationnel. Il est ainsi un des spécialistes de la sécurité des actifs incorporels et de leur valorisation. Il contribue ainsi à l'élaboration de références et standards en matière de sécurité économique et de souveraineté en matière d'informations sensibles.

Il est l'auteur d'ouvrages :
Cyberisques. La gestion juridique des risques numériques, LexisNexis, 2018
Penser la guerre économique. Bréviaire stratégique. VA Editions, 2018
Le droit du renseignement - renseignement d'Etat, renseignement économique, LexisNexis, coll. Actualité, 2016
Le Droit de l'intelligence économique. Patrimoine informationnel et secrets d'affaires, Lamy, coll. Axe Droit, 2012.

LA RÉACTION A UNE CYBERATTAQUE COMPORTE UNE DIMENSION JURIDIQUE

Les cyberattaques combinent des processus automatisés d'exploitation de failles logicielles ou de faiblesses dans l'organisation des réseaux d'une entreprise. Une intelligence de ce phénomène requiert la mise en place de mesures techniques de sécurisation des systèmes informatiques et de coordination des acteurs susceptibles de contrer ces pratiques invasives. Il faut également prendre en compte la question du recueil des éléments probatoires établissant formellement l'attaque. Outre une classique sensibilisation des personnels, il faut penser l'environnement juridique des pratiques de l'entreprises, de ses relations avec ses partenaires ou prestataires et les inscrire dans un régime contractuel.

Il importe également de connaître les formalités impératives liées à la notification à la CNIL des incidents, notamment liés à une atteinte aux données personnelles.

Cybersécurité :
quelle réaction juridique face à une attaque ?

Par Georgie Courtois

Plus une semaine ne passe sans qu'une nouvelle cyberattaque de grande ampleur ne soit révélée et défraye la chronique. Ces cyberattaques ont tendance à viser des cibles mal préparées, comme certaines ETI, PME et TPE. Georgie Courtois nous explique comment les entreprises doivent anticiper et réagir en cas de cyber attaque.

À quels types de menaces sont confrontées les entreprises ?

Les menaces cybers ont pour particularité d'être protéiformes. Leur point commun est évidemment l'utilisation de moyens informatiques par les attaquants. Toutefois, les techniques utilisées sont très différentes en fonction de l'objectif des attaquants.

GEORGIE COURTOIS

Avocat
De Gaulle Fleurance & Associés

Les cyber-attaques les plus répandues sont les suivantes :

– *Attaque par déni de service (Denial of Service, DDoS)* : action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu. La cible est un serveur et l'objectif est de le submerger de requêtes afin de rendre son accès impossible. Cette attaque est souvent coordonnée par des serveurs, eux-mêmes contaminés, qui envoient des requêtes sans que leur propriétaire en ait conscience. Cette attaque peut avoir pour conséquences une perte de capacité de communication et de chiffre d'affaire pour la société visée ;

– *Défiguration (defacement)* : attaque visant à modifier l'apparence ou le contenu d'un serveur Internet. L'objectif est souvent pour l'attaquant de faire part de revendications ;

– *Ransomwares :* programmes informatiques malveillants, téléchargés à l'insu de la victime, dont l'objectif est de rendre inaccessibles des données en les chiffrant et de demander une rançon en échange de la clé de déchiffrement. WannaCry et Petya ont immobilisé de nombreuses entreprises en 2017.

– *Hameçonnage (Phishing)*: utilisation d'un e-mail d'apparence légitime (faux mails d'opérateur téléphonique, de banque…) aux yeux de la victime afin d'obtenir des informations personnelles, notamment leurs mots de passe.

– *Spoofing*: méthode d'usurpation d'identité électronique visant à se faire passer pour une autre personne (changement d'apparence du suffixe d'un e-mail ou d'un nom de domaine) afin d'obtenir des informations personnelles, d'ordonner des virements bancaires (arnaque au Président) ou encore d'envoyer des virus (type Ransomware) pour prendre le contrôle du système informatique de la victime.

– *Exploitation d'une faille de sécurité*: l'objectif de l'attaquant est de s'introduire dans un système informatique mal sécurisé afin d'obtenir et exploiter les données présentes sur le système.

Ces typologies de cyber-attaques les plus répandues peuvent être combinées afin de parvenir au résultat escompté. La majorité d'entre elles exploite souvent des interactions sociales avec des salariés des entreprises mal préparés ou crédules. Cela caractérise le fait que l'humain est au cœur du processus des cyber-attaques et constitue le maillon faible de la sécurité des systèmes informatiques.

Comment anticiper un risque de cyber-attaque ?

L'anticipation du risque cyber passe par trois types de mesures :

– *Les mesures techniques*: socle indispensable à la sécurité des systèmes d'information, les entreprises doivent veiller à avoir un système informatique le plus sécurisé possible (Firewall, Antivirus, chiffrement des données, gestion des accès…). Cela passe par la structuration même du système, avec la coordination des informaticiens ou des prestataires externes. Ces mesures techniques permettent également de détecter plus rapidement qu'une attaque est en cours. À défaut, les attaquants peuvent rester plusieurs mois de manière dormante dans les systèmes d'information avant de mettre en œuvre leur attaque ;

– *Les mesures juridiques*: ces mesures consistent à mettre en place un environnement juridique contraignant pour encadrer les comportements au sein d'un système d'information. Cela passe notamment par la mise en place d'une charte informatique, par des obligations

dans le cadre des contrats de travail, par la gestion des questions de responsabilité avec les prestataires informatiques et les sous-traitants de données personnelles ou encore par la sécurisation du dispositif en souscrivant une assurance cyber risque ;

– *La sensibilisation* : encore une fois, les employés d'une entreprise doivent être sensibilisés afin d'éviter d'être à l'origine d'une attaque cyber en raison de leur manque de compréhension des mécanismes utilisés par les attaquants.

Au-delà de ces prérequis, il est recommandé de mettre en place au sein de son organisation une « cellule de crise Cyber » afin que chacun des intervenants, en partant de la direction jusqu'aux responsables du système informatique et aux opérationnels dont les données sont concernées, puisse réagir très rapidement. Plus l'attaque dure longtemps, plus il est difficile de revenir rapidement à la normale et de reprendre son activité. Cette cellule de crise doit également faire intervenir des juristes ou des avocats afin qu'ils puissent mettre en œuvre rapidement les obligations légales auxquelles sont soumises les entreprises victimes.

© Man with futuristic digital tablet on a project par Kir Smyslov

Une expertise menant à la construction d'un système sécurisé, un environnement juridique des pratiques et des responsabilités des acteurs constituent un socle de mesures propres à assurer la protection des valeurs de l'entreprise.

3) Comment réagir lorsque l'on a fait l'objet d'une cyber-attaque ?

Lorsqu'une entreprise a fait l'objet d'une attaque, il est nécessaire de pouvoir gérer plusieurs actions très rapidement :

– ***Si des données personnelles sont concernées***[1] : aux termes de l'article 33 du RGPD[2], si des données personnelles ont fait l'objet d'une violation (perte de disponibilité, d'intégrité ou de confidentialité, de manière accidentelle ou illicite), il est nécessaire de **notifier cette violation à la CNIL dans un délai de 72 heures** à la suite de la constatation de la violation. À défaut, il faudra expliquer lors de la notification les motifs du retard ;

– ***Si l'entreprise est un opérateur de service essentiel*** : la loi[3] et le décret[4] publiés en 2018, issus de la transposition de la Directive Network Information Security, mettent à la charge de certaines entreprises des obligations de sécurité et de notifications[5]. Elles doivent **notifier à l'ANSSI, sans délai après en avoir pris connaissance**, les incidents affectant les réseaux et systèmes d'information nécessaires à la fourniture de services essentiels susceptibles d'avoir, compte tenu notamment du nombre d'utilisateurs et de la zone géographique touchés ainsi que de la durée de l'incident, un impact significatif sur la continuité de ces services ;

– ***Recherche et aménagement de la preuve*** : dès que l'attaque a été détectée, il convient de sécuriser au maximum la preuve informatique qui est un élément essentiel afin de comprendre la raison de l'attaque, éviter qu'une telle attaque ne se reproduise et surtout permettre d'agir contre les auteurs de l'attaque. Il convient de faire appel à des experts informatiques habitués à gérer ces crises et à recueillir la preuve sans la dénaturer ;

– ***Action judiciaire*** : en parallèle des interventions de recueil de preuve et de remédiation, il convient de porter plainte auprès des services de polices et de gendarmerie spécialisés dans la fraude aux technologies. Ces services disposent de moyens d'analyse très performants et sont susceptibles de remonter aux auteurs des infractions, malgré le fait que de nombreuses attaques proviennent de l'étranger.

(1) https://www.cnil.fr/fr/

(2) https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article33

(3) LOI n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité.

(4) Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.

(5) Energie, Transport, Banques, Infrastructures de marchés financiers, Santé, Fourniture et distribution d'eau potable, Infrastructures numériques, les moteurs de recherche en ligne, les places de marché en ligne (« marketplace »), les services de Cloud computing

AUTEUR

Georgie Courtois intervient en conseil et en contentieux en droit des nouvelles technologies (informatique, internet, cryptologie, données personnelles…) et en droit de la propriété intellectuelle (droit d'auteur, droits voisins, marques, dessins et modèles, brevets).

Il enseigne la pratique des procédures judiciaires et du contentieux liés à la Propriété Intellectuelle dans le Master 2 PIDN (Propriété Intellectuelle Droit du Numérique) à la Faculté Jean Monnet, Université de Paris Saclay et intervient en droit des technologies innovantes dans le Mastère Spécialisé DAIM (Droit des Affaires Internationales et Management) de l'ESSEC Business School.

Il est membre fondateur du #HubFranceIA, association française sur l'intelligence artificielle, dont il pilote le groupe sur l'accompagnement juridique et il est membre du groupe « Technologie » de l'International Bar Association (IBA).

NOTES

DIRECTEUR DE LA PUBLICATION

Général de brigade **Laurent BITOUZET**

RÉDACTION

Directeur de la rédaction :
Général d'armée (2S) **Marc WATIN-AUGOUARD,**
directeur du centre de recherche de l'EOGN

RÉDACTEUR EN CHEF

Colonel (ER) **Philippe DURAND**

MAQUETTISTE PAO

Maréchal des logis-chef **Anne PELLETIER**
SDG

IMAGES

Stéphane MICHAUX
DICOM/Phototèque

COMITÉ DE RÉDACTION

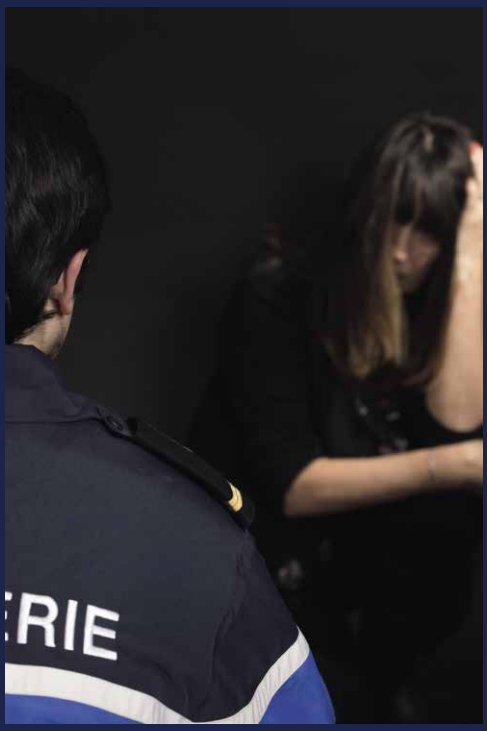
• Général de corps d'armée **Christian RODRIGUEZ,**
major général de la Gendarmerie nationale
• Général de corps d'armée **Thibault MORTEROL,**
Commandant des écoles de la Gendarmerie nationale
• Général de brigade **Laurent BITOUZET,**
Conseiller communication du directeur général
de la Gendarmerie nationale - chef du Sirpa-gendarmerie
• Lieutenant-colonel **Jean-Marc JAFFRÉ,**
Directeur-adjoint au centre de recherche de l'EOGN

COMITÉ DE LECTURE

• Général d'armée **Jean-Marc LOUBÈS,**
Inspecteur général des armées – gendarmerie
• Général de corps d'armée **Christian RODRIGUEZ**
Major général de la Gendarmerie nationale
• Général de corps d'armée **Thibault MORTEROL,**
Commandant des écoles de la Gendarmerie nationale
• Général de corps d'armée **François GIERÉ,**
Directeur des opérations et de l'emploi
• Général de brigade **Laurent BITOUZET,**
Conseiller communication du directeur général
de la Gendarmerie nationale - chef du Sirpa-gendarmerie
• Colonel **Laurent VIDAL,**
délégué au patrimoine – DGGN
• Lieutenant-colonel **Édouard EBEL,**
département gendarmerie au sein
du service historique de la Défense

DÉPOT LÉGAL

Raison sociale de l'éditeur :
CREOGN, avenue du 13e Dragons,
77010 Melun cedex
Général (2S) Watin-Augouard
Imprimerie : SDG - 11 rue Paul Claudel
87000 Limoges
Mars 2019
ISSN 1243-5619



© LPC/SIRPA

Violences familiales, entre volonté et réalités

Les pouvoirs publics et les milieux associatifs ont rendu visible le mal social que sont les violences familiales. La lutte contre celles-ci fait l'objet de différents plans d'action et de partenariats. La lutte contre les violences infra-familiales (VIF) est entrée dans le champ d'action des policiers par la mise en place de différents dispositifs, des campagnes de sensibilisation et une évolution des modes opératoires des primo-intervenants et enquêteurs. La revue N° 265 donnera un éclairage actualisé et prospectif sur ce phénomène social effarant par ses conséquences humaines et sociétales.