SECEM

MAGAZINE

Le magazine sur la Sécurité Economique et la Compétitivité des Entreprises en Méditerranée

N°8 ■ Avril | Juin 2016

ISSN 2429-5167

DOSSIER SPÉCIAL

CYBERSECURITÉ

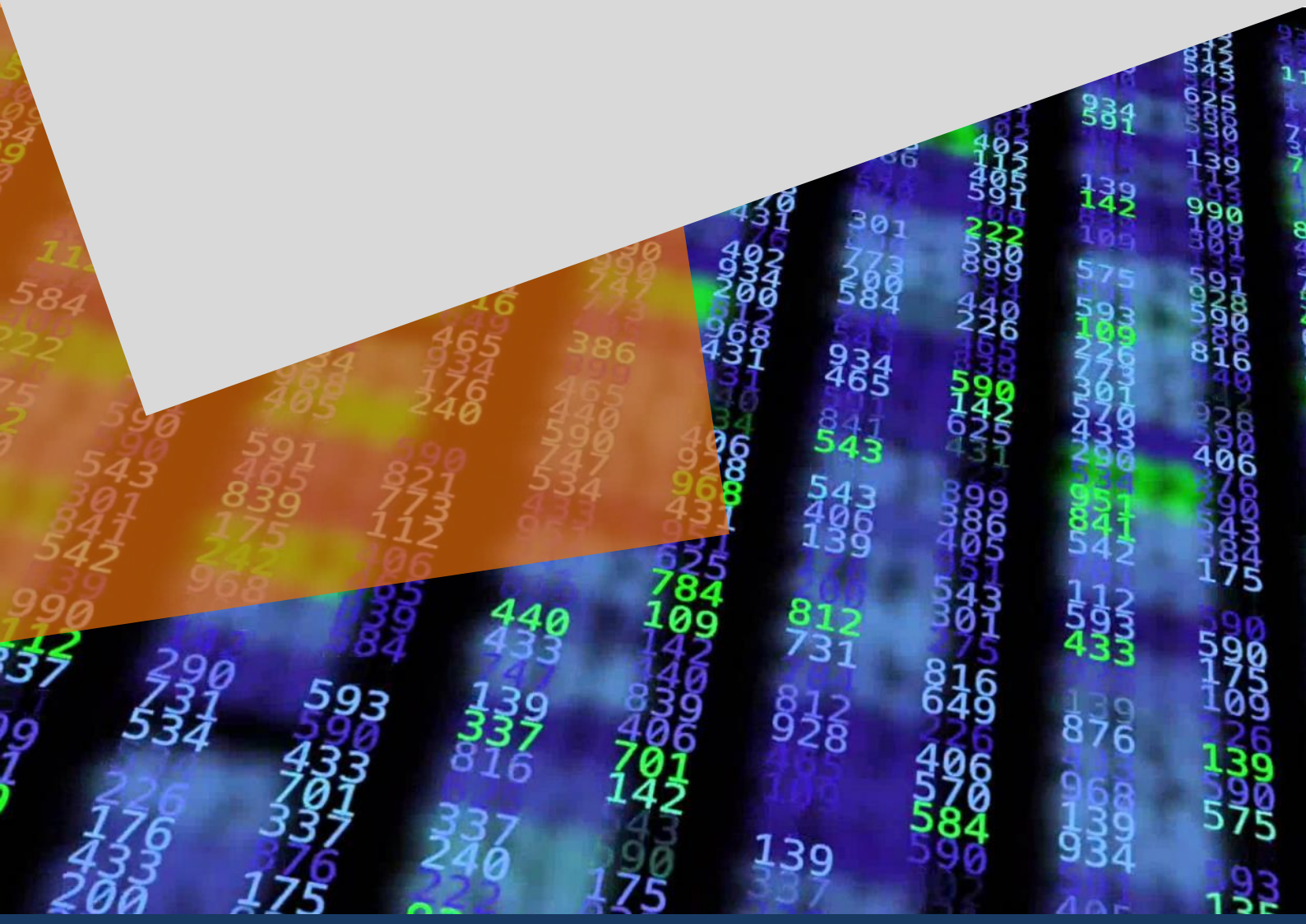
La cybercriminalité en entreprise

Sommaire

SECEM Magazine
N°8 ■ Avril | Juin 2016

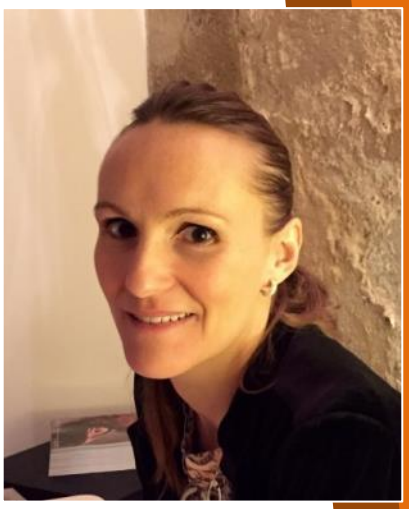
DOSSIER SPECIAL

CYBERSECURITÉ
La cybercriminalité en entreprise



Edito

Cybersécurité, un impératif de sécurisation partagé au sein de l'entreprise.



Bernadette LEROY

Présidente de l'ACBM
Présidente d'AESATIS

L'avènement d'Internet dans l'entreprise a révolutionné nos modes de communication et a bouleversé notre manière d'entretenir nos relations. Aujourd'hui, nos échanges professionnels dans le cyberespace ne se résument plus à de simples courriels ou échanges d'images statiques. Un individu contemporain désire désormais exposer au grand jour ses aptitudes, ses réussites, ses prestations, ses talents, ses prouesses. Il en va de même pour une entreprise à l'heure actuelle qui s'expose plus que jamais dans le cybermonde.

Selon le Cabinet PwC, 42,8 millions d'incidents cybercriminels ont été enregistrés dans le Monde en 2015 soit une hausse de 48% et un équivalent de 120 000 attaques par jour. Longtemps, les entreprises françaises ont pensé que la menace venait d'ailleurs et ne touchait que les sociétés étrangères. Or, selon un récent chiffre, près de 9 cyberattaques sur 10 subies par des entreprises françaises seraient réalisées par des pirates « locaux » agissant depuis la France. Désormais, en plus d'être le 3ème pays au rang des états les plus ciblés par ces attaques cybercriminelles, 87% de celles-ci seraient endogènes.

Vol externe d'informations, fuite de données, intégration d'un virus par une clé USB infectée, espionnage industriel, rançonnage, sabotage… Toutes ces attaques ont pour corollaire de viser les données de l'entreprise. Ce sont de véritables objets de convoitise provoquant une augmentation perpétuelle des cybers atteintes. En cela, la cybercriminalité apparaît aujourd'hui comme l'une des préoccupations majeures de toute entreprise. De plus, si l'inquiétude des acteurs de l'entreprise grandit, c'est que la cybercriminalité n'est pas toujours identifiable. En effet, les cybercriminels peuvent introduire des virus dormants sur n'importe quelle poste dans l'entreprise et les déclencher à tout moment.

Tout récemment, MySpace, Swift, VTech sont des exemples parmi tant d'autres de cyberattaques. Inéluctablement, la médiatisation accrue de celles-ci alerte l'opinion publique et la conscience de tout chef d'entreprise ou cadre dirigeant. Pourtant, selon l'étude du Cabinet EY France, 65% déclarent ne pas avoir les moyens suffisants pour protéger leurs données correctement et 31% n'ont même aucune politique de sécurité contre les menaces provenant du cybermonde. TPE, PME et grand groupes doivent donc impérativement mettre en sûreté leurs systèmes d'Information numériques pour faire face à des criminels toujours plus performants. Cette sécurisation passe par la mise en place d'une Politique de management de la Sécurité des Systèmes d'Information numériques. Dans toute organisation, le risque zéro n'existe pas. De fait, prendre la mesure du niveau de sa vulnérabilité est un point essentiel afin de prévenir plutôt que guérir. Une telle politique de sécurisation du système d'Information numérique se veut être aussi un engagement collectif avec une adhésion forte de la Direction. Elle est l'affaire de chacun et ce tous les jours en adoptant au quotidien des bonnes pratiques souvent simples et relevant du bon sens.

Faire un dossier sur la thématique de la cybercriminalité en entreprise, c'est vouloir informer, sensibiliser et alerter nos lecteurs sur les problématiques de l'ouverture à Internet et de la transformation digitale de l'entreprise ainsi que sur les nouvelles menaces que cela amène. Au travers des interviews et des articles qui ponctueront ce dossier, nous avons pour souhait de vous donner les moyens de comprendre l'impératif de la mise en place d'un système de management de la sécurité de l'information et de poser les bases nécessaires à la construction de cette politique de sécurisation au sein de toute entreprise. ■

CJCS

club des jeunes cadres en sûreté

Association créée en 2012, le Club des Jeunes Cadres en Sûreté (CJCS) réunit déjà plus de 55 membres d'horizons différents proposant aux jeunes cadres, jeunes diplômés et étudiants de tous les domaines de la sûreté et de la sécurité une structure conviviale et efficace d'échanges et de partages.

Jérôme LAURENT

Président du Club des Jeunes Cadres en Sûreté

Jonathan SCHIFANO et Paul MARREC

Membres du Conseil d'Administration du CJCS

■ **Pouvez-vous nous présenter l'intérêt d'un tel Club des Jeunes Cadres en sûreté à la fois du point de vue du Président en lui-même puis du point de vue de l'un de ses membres du conseil d'administration ?**

Jérôme LAURENT : La création de l'association par mon prédécesseur, Jérémy MARTI, répondait à l'absence de *jeunes* dans les organisations professionnelles existantes, organisations plus axées sur des profils confirmés. L'association rassemble donc des jeunes diplômés et professionnels de la sûreté et de la sécurité de tous les secteurs d'activité, qu'ils soient prestataires, prescripteurs ou utilisateurs issus du secteur privé ou public. L'objectif premier du CJCS est de pouvoir échanger et partager nos expériences et nos pratiques et également participer aux grands débats qui animent actuellement notre profession.

Jonathan SCHIFANO : L'intérêt du CJCS, c'est justement de ne pas se limiter à un intérêt. Bien au contraire, notre volonté est de dégager de la valeur, d'aller chercher des nouveaux talents, d'être bienveillants et d'accompagner les métiers de la sécurité dans leur globalité par une conduite du changement. Le CJCS est également un lieu d'échange, de débat libre et de partage entre ses membres. Jérémy MARTI, Président d'Honneur a commencé cette conduite au changement dès la création de l'association. Cette aventure lancée, par un conseil d'anciens perdure et grandit, quatre ans après et ce, avec toujours la même vision. Ce métier a besoin d'un nouvel élan, de nouvelles idées et de transversalité. Voici un simple constat général : « *La sécurité n'est pas un domaine que l'on choisit mais, une voie qui nous choisit* ». Et si la sécurité devenait une filière-métier où l'on aborde tous les aspects d'une entreprise que l'on soit de jeunes diplômés et professionnels de la sûreté et de la sécurité de tous les secteurs d'activité, qu'ils soient prestataires, prescripteurs ou donneurs d'ordre issus du secteur privé ou public ? Le CJCS prend à cœur d'œuvrer au travers de ce qui existe dans notre métier pour le faire connaître, pour le rendre plus attractif et dynamique en intégrant des nouveaux systèmes de communication et de partage des informations de tout horizon.

Paul MARREC : En tant que Membre du bureau, depuis maintenant près d'un an, j'ai pu constater que le CJCS me permettait d'aller au-delà de ma profession initiale. J'ai ainsi eu l'occasion d'échanger avec des personnes aux profils et aux parcours variés, enrichissant toujours ma culture de sûreté.

■ **Vous représentez aujourd'hui la relève des cadres en sûreté. Comment voyez-vous cette nouvelle génération dont vous faites partis ?**

Jérôme LAURENT : La nouvelle génération de cadres œuvrant dans le secteur est une génération ayant suivi un cursus d'études en lien direct avec la sécurité et qui a choisi ce secteur d'activité. Cela s'explique par le nombre de formations qui se sont développées. Ce qui n'est pas forcément le cas de la génération précédente pour qui le fait de travailler dans la sécurité était davantage une reconversion qu'une volonté initiale de travailler dans ce secteur.

Jonathan SCHIFANO : Nous sommes des jeunes cadres dans le domaine de la sûreté. Et parce que nous sommes acteurs au quotidien dans les missions qui nous sont attribuées, nous affirmons que le CJCS permet aujourd'hui pour un

les donneurs d'ordre d'établir un vrai dialogue. En ce sens, j'ai en face de moi des personnes qui sont formées aux métiers de la sécurité et qui m'apportent un véritable enrichissement de par leur chemin de vie. Ils englobent à la fois des questions de sécurité, couplées ou non, aux moyens innovants actuels mais aussi la notion de qualité de service et de suivi par la mise en place de Key Performance Indicator (KPI). Le dialogue s'établit alors sur la performance du service. Dès lors, cette génération accompagnée par ses pairs œuvre chaque jour et innove car, l'innovation, la remise en question, la réactivité font parties intégrantes des qualités des jeunes cadres de demain.

Ce que je souhaite retrouver à l'avenir dans ce métier est d'être challengé sur la performance et qu'en face, j'ai la même chose. Tout cela facilite le dialogue et la transparence et de ce fait, la confiance. Etre accompagnés par nos pairs, pour nous les jeunes cadres, c'est bénéficier de leur expérience terrain et de mener leur combat au changement de la vision sécurité avec notre nouvelle dynamique et nos formations tout en prenant en compte l'évolution des technologies et des organisations. On ne déconstruit pas le passé. On le modifie pour que l'ensemble des services d'une entreprise acquièrent une vision de la sécurité au sens large.

Paul MARREC : Selon moi, la jeune génération de cadres en sûreté du secteur privé ne se prédestinait pas toujours à travailler dans ce milieu professionnel singulier qu'est celui de la sûreté. C'est au travers de rencontres, de parcours universitaires et d'expériences professionnelles que chacun a pu pénétrer au sein de cette profession particulière.

■ Trouvez-vous qu'il y ait une évolution visible du métier et du profil des cadres en sûreté aujourd'hui ?

Jérôme LAURENT : Oui, il y a une évolution dans les profils des professionnels, notamment par l'offre de diplômes toujours plus large : DU, licence, master, MBA… Cependant, cette évolution n'est pas forcément visible chez nos interlocuteurs. Cela peut parfois porter à confusion et ainsi créer un décalage de compréhension.

Jonathan SCHIFANO : Comme nous l'avons dit, aujourd'hui et encore plus par les évènements que nous subissons, la sécurité se professionnalise et se démocratise au sein de notre société. Dès le plus jeune âge, des cours de secourisme sont dispensés dans les écoles et des simulations de confinement sont réalisées. Nous mesurons les incidents et nous travaillons avec tous les acteurs sur des scénarios à risques. La sécurité ne se limite pas à mettre des agents dans un poste de sécurité. La sécurité, c'est l'affaire de tous. Malheureusement, c'est lors d'évènements douloureux que nous nous rappelons à quel point nous sommes acteurs. Les jeunes adolescents qui cherchent leur voie aujourd'hui s'orientent vers des métiers de la sécurité publique, souvent par patriotisme ce qui n'était plus au goût du jour il y a encore quelques années. D'autres secteurs transverses comme les acheteurs et les services des ressources humaines par exemple s'intéressent désormais de connaître, évaluer et mesurer leur niveau et leurs moyens de sécurisation des personnes et des publics. Enfin, la sécurité, c'est aussi la sécurité de l'informatique qui est aussi un des segments essentiels de cette filière. Donc, il y a bien eu une évolution grâce à la création de diplômes, de formations, de nouveaux métiers tels que le « risk management ». Dès lors, ces nouvelles générations montantes seront à même de dessiner les métiers de demain.

Paul MARREC : On constate la montée en puissance de jeunes cadres issus des nouvelles filières universitaires dédiées à la sûreté, dont je fais partie. Le profil-type du senior issu des services de l'Etat tend à ne plus être la norme absolue sans pour autant se marginaliser. Le label "ancien policier" ou "ancien militaire" reste un gage rassurant pour les employeurs qui pour certains maîtrisent encore mal les enjeux de cette profession. Je pense que d'ici quelques années la proportion des responsables sûreté n'étant pas passés par l'armée ou les forces de l'ordre continuera de croître.

■ Quels sont tous deux les sujets d'actualité qui vous tiennent à cœur d'aborder et de travailler au sein du programme du CJCS et pourquoi ?

Jérôme LAURENT : De par mes fonctions professionnelles, ingénieur commercial, je dirais que c'est la place de la sécurité humaine au sein de son association dans la sécurité électronique. En effet, cette dernière permet de nouvelles possibilités. Néanmoins, rien ne remplace l'humain dans la prise de décision. Il faut donc trouver le juste équilibre.

Jonathan SCHIFANO : De par mes fonctions professionnelles exercées, Responsable National Sécurité au sein d'un groupe international dans l'ameublement, je dirais que c'est l'alliance de la sécurité humaine associée à des solutions technologiques. Le premier sujet est de trouver le juste équilibre et d'en mesurer la performance. Enfin, le second sujet touche les bonnes pratiques d'achats sécurité. Dans mon activité de tous les jours, je m'efforce de travailler en étroite collaboration avec mes acheteurs afin de garantir des prestations de service de qualité.

Paul MARREC : J'ai évidemment plaisir à traiter des sujets ayant un rapport direct avec ma profession. J'ai ainsi eu la chance de pouvoir suivre les travaux de nos membres qui ont travaillé sur les questions liées au projet d'encadrement par la loi du secteur du conseil en sûreté (travail qui a débouché sur la diffusion d'un communiqué). Cette question très complexe a trouvé au sein du CJCS un espace de débat libre et sans entrave, davantage je pense, que dans d'autres structures de réflexion.

■ Comment voyez l'avenir pour le CJCS ?

Jérôme LAURENT : Le CJCS fête cette année ses 4 ans d'existence dans un secteur, qui depuis quelques mois, est sous les feux des projecteurs de par l'actualité en perpétuelle évolution et de par les avancées technologiques. Il faut donc que nous soyons capables de suivre cette évolution en nous développant de façon maîtrisée.

Jonathan SCHIFANO : Comme le souligne très justement Jérôme LAURENT, nous nous développons de façon maîtrisée. Le CJCS est une marque de fabrique de jeunes cadres et de fait des cadres qui doivent faire leur preuve et leur place dans la société. Donc, pour cela, nous nous devons de maîtriser notre développement, nos sujets et nos orientations. Nous ne voulons pas subir l'activité de l'association. Nous voulons la faire grandir et perdurer. Cette année, nous fêtons donc nos 4 ans. Nous rentrons petit à petit dans la cour des grands avec beaucoup de sérénité et pleins de projets en particulier, celui de faire fédérer des jeunes cadres issus d'horizons transverses.

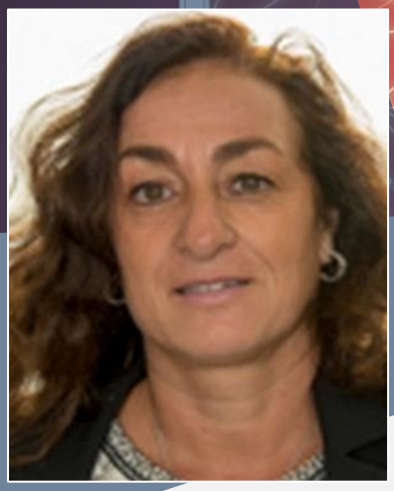
Paul MARREC : Selon moi, l'enjeu pour le CJCS à moyen terme est de continuer à croître tout en diversifiant le profil des membres. Au-delà des catégories actuelles d'organisations dont proviennent les adhérents, j'estime que nous devons nous ouvrir davantage aux jeunes donneurs d'ordres.
Cela devra se faire sans pour autant perdre l'aspect "jeune" du club. Je pense principalement aux étudiants provenant des nouvelles filières de la sécurité pour lesquelles, le CJCS devra rester dynamique s'il espère rester attractif. ■

Club des Jeunes Cadres en Sûreté (CJCS)

Chez L-Conseils - 1 rue Patry - 92220 Bagneux

www.cjcs.fr

« La sécurité n'est pas un domaine que l'on choisit mais, une voie qui nous choisit »



Christine ALEJANDRO

Conseillère Mobilité Carrière au sein du Ministère de l'Intérieur

Mission Reconversion et Reclassement Professionnel (M2RP)

■ Pouvez-vous me parler de ce nouveau dispositif dont, vous faites partie, mis en place au sein de la Police Nationale ? Dans quel contexte a-t-il vu le jour ?

Mise en place en septembre 2011 au sein de la sous-direction de l'action sociale et de l'accompagnement du personnel (SDASAP) de la Direction des Ressources et des Compétences de la Police Nationale (DRCPN), la Mission Reconversion et Reclassement Professionnel (M2RP) propose une prestation de conseil aux agents de la Police Nationale qui souhaitent se lancer dans une transition professionnelle hors Police Nationale. Cette prestation n'existait pas jusqu'à présent. Cette création participe à la valorisation qualitative de la politique RH de la Police Nationale. Ainsi, un Commissaire divisionnaire, chef de la M2RP, dirige un réseau national de 29 Conseillers Mobilité Carrière (CMC) composé de corps actifs de la Police Nationale (officiers, gradés et gardiens) et de corps administratifs (attachés d'administration de l'État). Nous sommes répartis à raison de 4 à 5 CMC dans chacune des 7 zones de défense et de sécurité de la métropole.

Nous suivons un cursus de formation initiale et continue qui a pour but de nous professionnaliser afin que nous puissions répondre avec compétence aux nombreuses et diverses sollicitations des agents de la Police Nationale et à celles des employeurs des secteurs publics et privés intéressés par les profils et les compétences des policiers. Dans chaque zone :

- 2 CMC exercent le métier de conseil aux agents de la Police Nationale. Ainsi, ils accompagnent ceux qui, à travers une démarche volontaire et confidentielle, souhaitent mettre en œuvre un projet professionnel (conseil, définition, orientation) de mobilité ou de reconversion temporaire ou définitive (hors champ Police Nationale) dans les trois fonctions publiques d'État, territoriale, hospitalière ou dans le secteur privé).
- 2 CMC exercent le métier de conseil aux employeurs. Pour la zone sud, avec mon homologue Romain SAUTEREAU, nous sommes en charge du développement des partenariats. Notre rôle est de promouvoir auprès des employeurs publics et privés les compétences et les profils des agents de la Police Nationale en développant un réseau de partenariats locaux de proximité et favorisant ainsi la mobilité hors Police Nationale.

■ Vous êtes issue d'un parcours riche d'expérience dans les ressources humaines. Aujourd'hui, en tant que conseillère mobilité carrière, en quoi consiste votre rôle et vos missions auprès des fonctionnaires que vous accompagnez dans cette phase de transition professionnelle ?

Notre rôle est de mettre en adéquation localement les besoins des employeurs des secteurs du privé et du public ainsi que les compétences des agents de la Police Nationale. Notre expérience permet d'apporter des informations concrètes aux fonctionnaires qui souhaitent faire une transition professionnelle hors de la Police Nationale et de les préparer à cette fin. Ils seront mieux informés et donc mieux armés.

■ Vous êtes en charge du portefeuille entreprises pour la région PACA. Quelle relation de confiance et quels liens de coordination se créent-t-ils entre la Police Nationale et les entreprises de la région ?

Tout d'abord une connaissance réciproque, c'est un enjeu de notoriété, nous sommes désormais identifiés. Confiance, disponibilité et réactivité nous caractérisent. Les entreprises, au-delà de la sécurité privée, recherchent un intermédiaire capable de répondre avec pertinence à leurs besoins. Nous connaissons les profils et les compétences policières qui sont variés et nous faisons l'interface. Cela nous permet de nous positionner comme l'un des acteurs régionaux dans le domaine du recrutement. Nous sommes maintenant bien intégrés dans le paysage RH de la région.

■ Le passage du secteur public au privé est toujours délicat. Trouvez-vous que la reconversion des fonctionnaires de police vers l'entreprise est plus difficile aujourd'hui ?

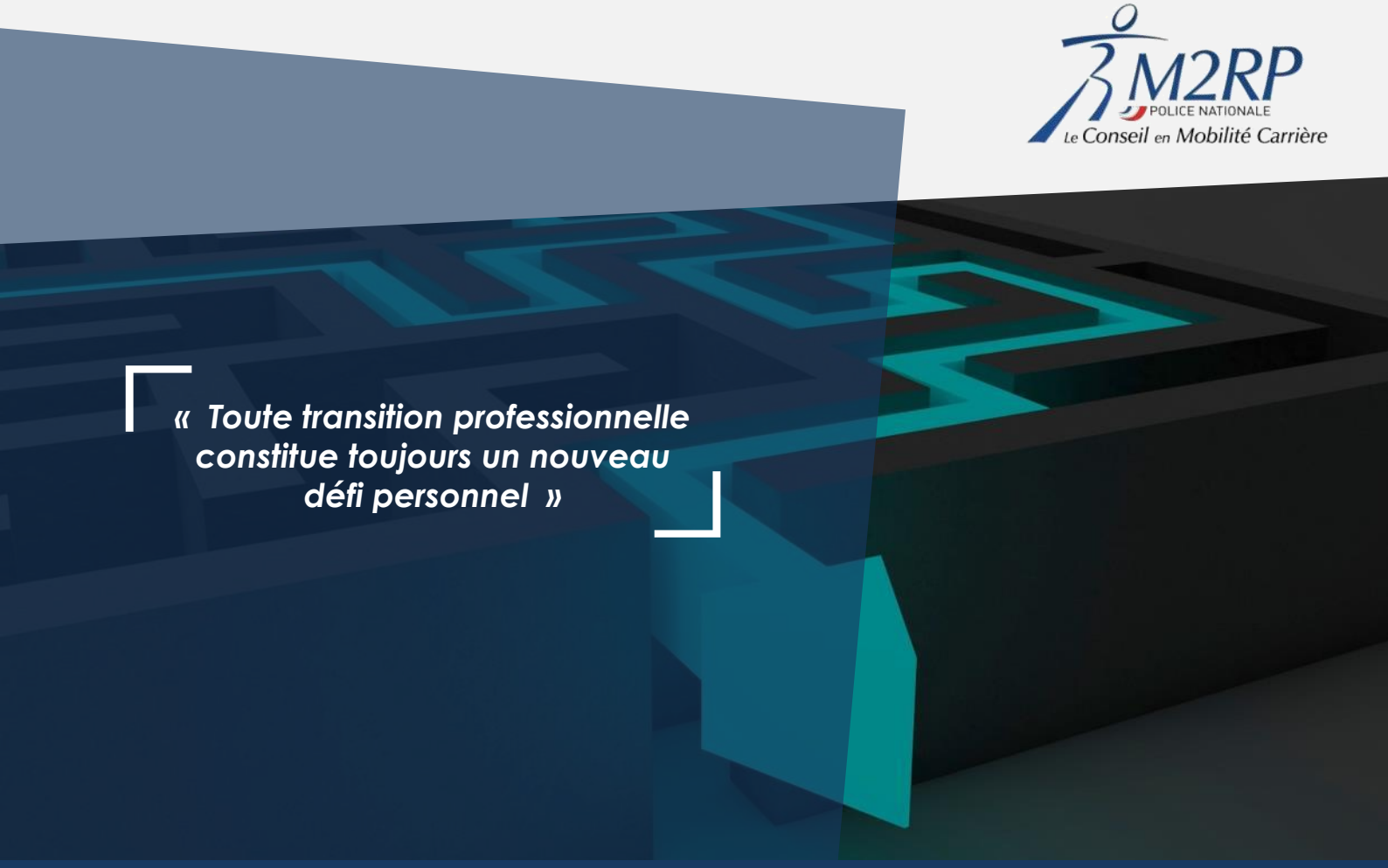
Toute transition professionnelle constitue toujours un nouveau défi personnel surtout lorsqu'il s'agit de passer du secteur public au secteur privé. En fonction de la situation économique et des dispositifs réglementaires, cette transition sera facilitée ou non. Tout dépend aussi de la maturation du projet du fonctionnaire et de nombreux facteurs personnels qui vont le pousser à aller jusqu'au bout ou non de sa démarche pour quitter temporairement ou définitivement la « Maison police ». Pour notre part, nous aidons l'agent à identifier le fonctionnement de l'entreprise et nous nous formons nous-mêmes à cette fin. Cela nous permet d'être plus compétents, efficaces et plus efficients pour le conseiller. Je tiens à préciser que l'une des qualités premières du policier est sa capacité d'adaptation, véritable atout de savoir-être et de savoir-faire apprécié par les entreprises.

■ La Police Nationale attire également beaucoup les jeunes. Elle compte plus de 11 000 Adjoints de sécurité (ADS). Certains souhaitent rester dans la Police Nationale, d'autres pas. Comment accompagnez-vous ces derniers ?

Les ADS de la Police Nationale (des contractuels de droit public pouvant effectuer au maximum six ans) sont informés du dispositif de reconversion lors de la formation initiale et nous les informons également durant la dernière année de contrat. Tous effectivement ne souhaitent pas, à l'issue de leur contrat, poursuivre une carrière dans la police. Lors de cette dernière année de contrat, nous leur présentons le plan de reconversion professionnelle mis en place par la direction des ressources et des compétences de la Police Nationale au profit des adjoints de sécurité : financement de formations qualifiantes (SSIAP 1), convention de stage en entreprise, etc. Cette présentation se déroule sur une journée, le matin une information collective et l'après-midi un entretien individuel avec un CMC. Ce dernier va accompagner l'ADS pour l'aider à élaborer ou à finaliser son projet professionnel.

Nous sommes des conseillers techniques dotés d'une solide expérience professionnelle, apportant une vision réaliste à ces jeunes. Nous les aidons à rechercher des débouchés professionnelles où les compétences acquises et le savoir-être trouveront à s'exprimer dans divers secteurs professionnels, même si les métiers de la sécurité restent, pour eux, une débouché naturelle. ■

M2RP POLICE NATIONALE
Le Conseil en Mobilité Carrière



« Toute transition professionnelle constitue toujours un nouveau défi personnel »

FORMATION ■ DÉTECTION DU MENSONGE ET GESTION DES PERSONNALITÉS DIFFICILES

A travers une initiation au décodage du langage non-verbal cette formation vous apportera des clefs pour :

DETECTER LE MENSONGE

Comprendre les intentions

Décoder le mensonge en situation complexe

Déceler les émotions cachées

GERER LES PERSONNALITES DIFFICILES

Identifier les types de personnalités

Adapter sa communication à son interlocuteur

Manager des personnes difficiles

Jeudi 13 octobre 2016
New Hôtel of Marseille
9h00 à 18h00

Animé par
Bernadette LEROY
Criminologue

250 € HT par personne
(soit 300 € TTC
déjeuner inclu)

INFORMATIONS ET INSCRIPTION

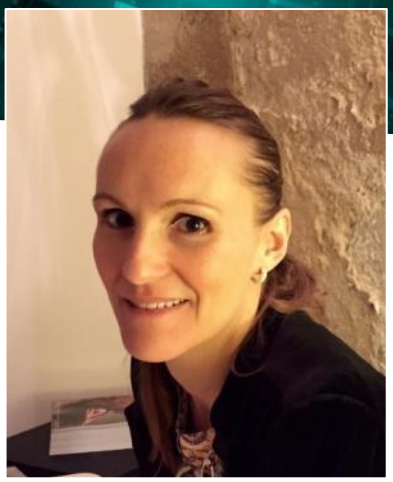
AESATIS ■ 79 bis, boulevard de l'Europe, 13127 VITROLLES
Numéro d'organisme formateur : 93131587713 ■ ☽ - 04 42 46 20 88 ■ ✉ - aesatis@aesatis.com ■ - www.aesatis.com

DOSSIER SPECIAL

CYBERSECURITÉ

La cybercriminalité en entreprise

DOSSIER SPECIAL



L'ADDICTION INTERNET, UNE NOUVELLE MALADIE DE LA SOCIÉTÉ MODERNE

Bernadette LEROY | Criminologue et experte en Intelligence Economique et Protection des entreprises. Présidente de la société AESATIS et de l'Association de Criminologie du Bassin Méditerranéen.

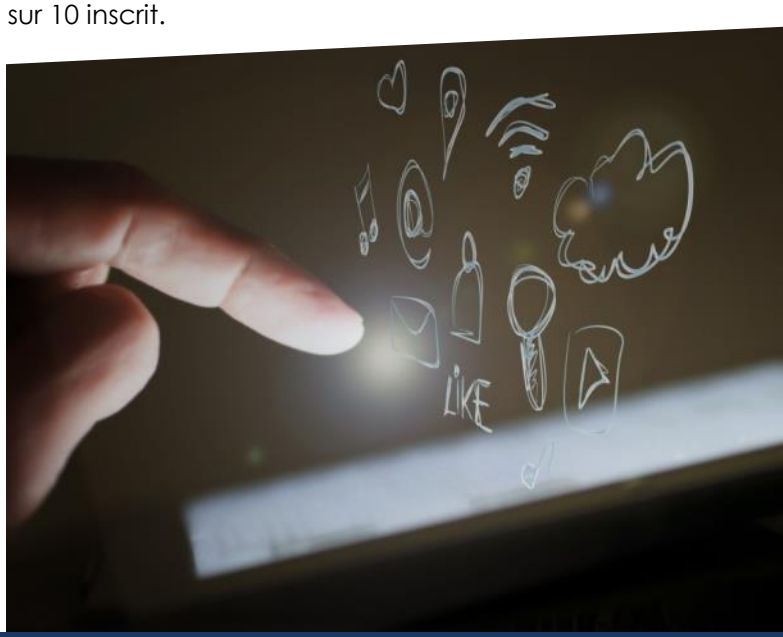
Selon l'étymologie latine, addiction vient du terme « addictus » qui signifie « s'adonner à ». Aujourd'hui, dans notre société de communication et du numérique, on ne cesse de s'adonner à de nombreuses activités sur Internet. Ces pratiques, toujours plus nombreuses et toujours plus diversifiées, évoluant à une vitesse folle, font naître de nouvelles pathologies et de nouvelles addictions.

Dès 1996, Dan VELEA et Michel HAUTEFEILLE, deux psychiatres et addictologues furent les premiers à signaler le risque addictif d'Internet dans le cadre d'utilisation accrue autant chez les adolescents que chez les adultes. Selon leurs propos, « *L'addiction est vue comme lien avec un objet ou une substance qui dépasse l'intention et qui déforme son utilisation* ». Dans le cadre de leurs travaux de recherche sur le sujet, tous deux distinguent très vite deux types d'addiction. D'un côté, la cyberdépendance générée directement par l'outil Internet via les jeux vidéo, les réseaux sociaux, les chats en ligne, l'obsession des mails… De l'autre, la dépendance assistée qui renvoie à une addiction préexistante que le web va démultiplier comme par exemple le voyeurisme ou les achats compulsifs.

Cet ouvrage, datant de la fin des années 90 ne fait que confirmer l'influence et le poids d'Internet dans les années 2000. En effet, cette technologie a totalement bouleversé notre rapport au temps et à l'espace. Aujourd'hui, il est difficile de vivre sans être connecté. Cela n'est presque plus envisageable dans le cadre de notre vie professionnelle ou personnelle.

L'année 2015 est présentée comme « l'Année Internet » avec plus de 44,8 millions d'internautes français dits « hyper connectés ». En effet, Médiamétrie a publié le 25 février dernier le bilan Internet 2015. Une année sous le double signe de la croissance des usages et de la très forte montée en puissance des écrans mobiles. Selon cette étude, plus de 8 internautes sur 10 sont hyper connectés, c'est-à-dire qu'ils accèdent à plusieurs écrans. Ils sont donc 17,3 millions à utiliser 3 écrans en novembre 2015. C'est un chiffre en hausse de 36% par rapport à janvier 2015, soit 4,6 millions d'internautes supplémentaires. Néanmoins, ce sont ceux qui utilisent deux écrans simultanément qui sont les plus nombreux : 20,3 millions. La question est donc la suivante : Que consultent les internautes sur ces petits écrans mobiles ?

Ce même bilan nous indique qu'en 2015, 35 millions de français âgés de 15 ans et plus, soit plus de 3 internautes sur 4 (77%) sont inscrits sur au moins un réseau social. Deux réseaux centrés sur la photo se distinguent, Instagram et Snapchat, avec pour chacun 1 internaute sur 10 inscrit.



L'attrait pour ces réseaux est favorisé par leur caractère « mobile native » combiné à la montée en puissance des écrans mobiles et à la jeunesse de leurs utilisateurs (37% des 15-24 ans sont inscrits sur Snapchat).

Réactualisation des informations sur Internet, volonté d'accéder à l'information à tout instant, voyeurisme permanent via les réseaux sociaux, sentiment d'être aimé et d'exister auprès des internautes, faire des rencontres, échapper à la réalité sont autant de raisons qui, entrepris de manière excessive, mènent à l'addiction. Pour le magazine Psychologies, Margaux RAMBERT recueille des propos poignants d'un « webaddict ». Victime d'un burn-out numérique et d'une overdose numérique, celui-ci déclare *« Le phénomène pervers, c'eux que pour exister en ligne, il faut y être tout le temps. Tous les outils comme Facebook ou Twitter nous y poussent d'ailleurs. C'est cette dictature du temps réel qui est dangereuse. A force d'y passer trop de temps, le net m'avait consumé. J'étais intoxiqué »*. Face à de tels témoignages, un parmi tant d'autres, nous pouvons presque aisément parler de « cyber-addiction » aujourd'hui. Néanmoins, ce propos est à nuancer. Toutes les personnes ayant une utilisation accrue d'Internet ne sont pas addicts. L'addiction est là lorsque le comportement sur Internet devient envahissant au point de prendre le pas sur toute autre activité, empêcher de travailler, dormir, se nourrir. Ce phénomène est encore peu reconnu comme une addiction à part entière. Le terme « addiction » est utilisé à tout va, décrédibilisant l'importance de ce mal des temps modernes. De plus, à la différence des drogues dures, il est évident que les conséquences générales seront moins dramatiques que des addictions à l'alcool ou à la drogue, même si elle peut avoir de graves conséquences. Isolement, repli sur soi, agressivité, perturbations neurologiques, décalages des rythmes biologiques… Ce sont autant de séquelles remarquées chez les personnes souffrant de cette addiction au web.

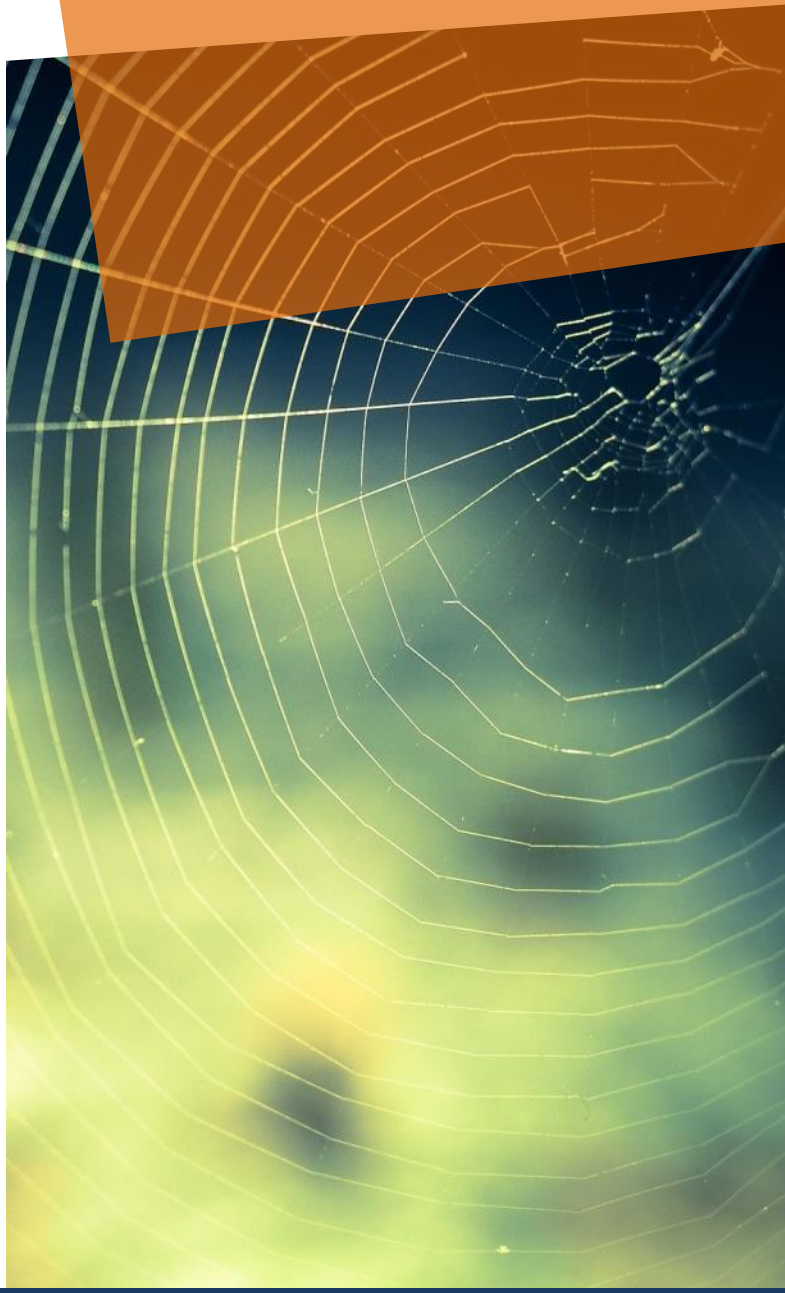
Ce type d'addiction peut également engendrer des pertes de contrôle. Celles-ci peuvent être de tout ordre et plus ou moins dramatique pour son auteur. Dans ce cas-là, la personne n'est plus maître de son comportement et n'a plus conscience des conséquences de ses actes. C'est par exemple, la personne qui se connecte sur son compte Facebook personnel via son poste de travail. Or, au lieu d'y passer cinq minutes comme une personne normale qui a conscience que ce n'est pas un endroit propice pour le faire, ne va pas pouvoir s'empêcher d'y passer des heures, celles-ci étant perdues pour l'employeur.

Il est donc notoire que pour qu'il y ait une addiction, il faut qu'il y ait une impossibilité de résister à une pulsion. La pulsion, dans le cadre d'Internet, se matérialise par le fait d'avoir besoin en permanence d'un accès à Internet, à son téléphone, à sa tablette, à son ordinateur ou de manière plus générale à tout objet connecté de près ou de loin à Internet.

Dans un second temps, l'addiction va prendre la forme d'une sensation de tension croissante qui est l'étape préliminaire au début du comportement addictif. Celle-ci aura pour corollaire la dotation à porter de main de son smartphone ou son ordinateur par exemple. La période de latence d'allumage ou de connexion de celui-ci va plonger le sujet dans une sorte de comportement d'impatience et d'énervement. Vient ensuite le moment de plaisir où, le sujet peut enfin jouir de sa connexion.

A noter qu'addiction et toxicomanie ne sont pas les deux termes d'un même maux. Il est important de ne pas les confondre et de ne pas les associer à tort. La toxicomanie est une addiction sévère, qui s'aggrave avec le temps, et dont les symptômes et leurs conséquences comme la dépression, la phobie sociale, l'automutilation sont beaucoup plus graves. Historiquement, le terme de toxicomanie est apparu pour qualifier essentiellement le comportement des héroïnomanes.

> ***« L'addiction est là lorsque le comportement sur Internet devient envahissant au point de prendre le pas sur toute autre activité, empêcher de travailler, dormir, se nourrir »***



A tort, nous assistons donc à une dérive sémantique. Selon l'Organisation Mondiale de la Santé (OMS), la définition stricte de la toxicomanie correspond à quatre éléments suivants : envie irrépressible de consommer le produit, tendance à augmenter les doses, dépendance psychologique parfois physique et conséquences néfastes sur la vie quotidienne.

Il est vrai que l'addiction d'Internet peut être vue comme une « toxicomanie sans drogue ». Addiction, toxicomanie ou simple pulsion, les frontières deviennent poreuses entre ces termes. Il convient donc toujours de bien analyser et nuancer les types de comportements avant de se prononcer dans le cadre d'un diagnostic. Mais si l'addiction est révélée, peu importe le nom que l'on veut bien lui donner, des moyens sont là pour l'éviter et des solutions existent pour soigner les personnes atteintes de ces troubles. Il est clair que la prévention et la sensibilisation ont un rôle majeur à jouer. Il est nécessaire de rappeler sans cesse que l'utilisation de cet outil doit être maitrisée, limitée et segmentée. Internet est un outil au service de l'Homme et non l'inverse. Il y a là un gros travail psychologique à instaurer pour replacer à son juste titre le produit addictif. C'est un travail à entreprendre pour les parents dès l'enfance. Le rôle du cadre parental et de l'éducation est grand dans cet enjeu d'équilibre des activités. Limiter l'accès aux écrans dès le plus jeune âge est un bon moyen d'éviter toute dérive lors de la construction identitaire de l'adolescent par exemple. Or, les parents de la Génération X/Y sont souvent dépassés par cette technologie en perpétuelle évolution. Il convient donc de les sensibiliser et de les accompagner également dans la mise en place de cadre d'utilisation et de limites pour leurs enfants en matière de technologie numérique. C'est d'autant plus important que c'est l'enfance qui conditionne notre futur en tant qu'Homme.

A l'âge adulte, des propositions de traitement par des thérapies cognitives comportementales sont à termes efficaces pour réduire à néant ce penchant. En parallèle, dans le cadre professionnel pour freiner les dérives, des actions de sensibilisation sont mises en place et se multiplient. Elles mettent en garde contre les effets dramatiques et les dommages collatéraux d'une utilisation abusive d'Internet à titre personnel dans le monde du travail donnant lieu à des avertissements voire des licenciements.

Aujourd'hui, des tests en ligne permettent même d'identifier et de définir votre dépendance à Internet. Ces plateformes en ligne, totalement gratuites à titre informatif, peuvent être de bonnes sirènes d'alarme pour prévenir ce type d'addiction, véritable question de société à part entière. ■

Bernadette LEROY

ACBM
ASSOCIATION DE CRIMINOLOGIE DU BASSIN MEDITERRANEEN

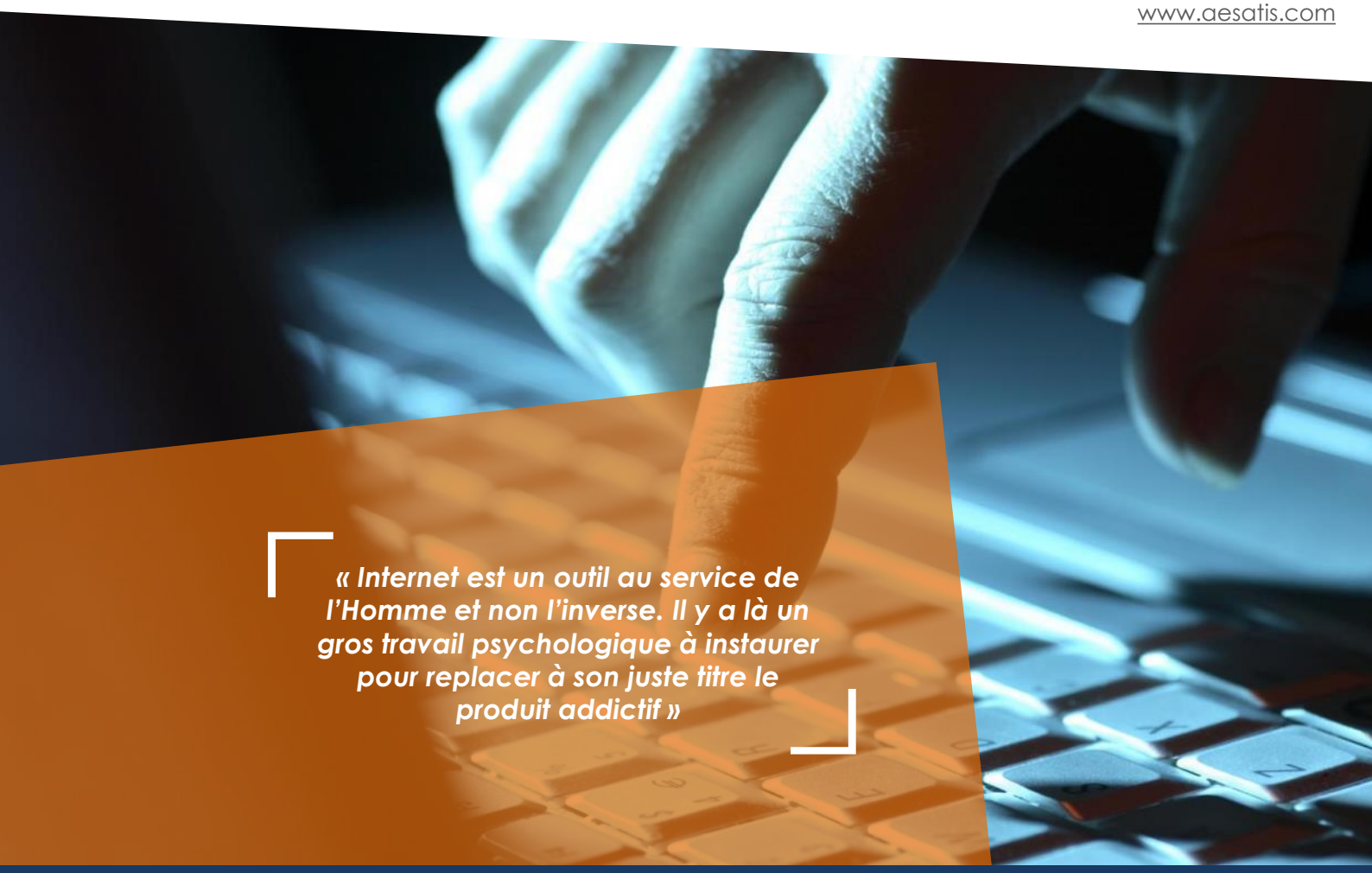
Association de Criminologie du Bassin Méditerranéen

www.acbm-paca.com

AESATIS

AESATIS – Conseil en sécurité et sûreté des entreprises

04 42 46 20 88
www.aesatis.com



« Internet est un outil au service de l'Homme et non l'inverse. Il y a là un gros travail psychologique à instaurer pour replacer à son juste titre le produit addictif »

LA CULTURE DU RISQUE NUMÉRIQUE S'IMPOSERA AUX MANAGERS

Nicolas ARPAGIAN | Directeur scientifique du cycle « Sécurité Numérique » à l'Institut National des Hautes Etudes de la Sécurité et de la Justice (INHESJ).

La numérisation des processus de production et de commercialisation sont déjà une réalité du quotidien pour nombre de secteurs d'activités. Qui misent sur les technologies de l'information pour accroître leur compétitivité, élargir leurs zones de chalandise et monter en puissance dans la chaîne de création de valeur. C'est la face éclairée de l'économie numérique. Les dirigeants qui se contenteraient de celle-ci hypothèquent l'avenir de leur organisation. Car aujourd'hui quelques minutes de navigation sur Internet permettent d'accéder à des offres de piratage de comptes de messagerie ou à des tutoriels très pédagogiques pour bloquer temporairement l'accès à un site Internet. Ces arsenaux numériques de proximité popularisent l'usage de ces modes d'agression sur la Toile. Les entreprises et leurs dirigeants constituent des gibiers privilégiés : l'ère de la communication les incite à ouvrir leurs agendas, les portes de leur société et une partie de leur vie professionnelle pour les rendre accessibles presque en direct aux internautes. C'est un matériau de premier choix pour conduire des opérations d'ingénierie sociale visant à réaliser de lucratives campagnes de pénétration de leurs systèmes d'Information.

S'ils persistent à voir dans la thématique du numérique un simple appareillage technique sans en comprendre les enjeux stratégiques et les menaces qui y sont liées, les dirigeants d'entreprise exposent leur patrimoine informationnel et leurs finances à toutes les convoitises. Il ne s'agit pas d'en faire des experts de la cybermenace mais bien de leur faire prendre conscience des dégâts pouvant être causés à partir d'une simple connexion à Internet. Cela fait partie intégrante de l'indispensable culture numérique de l' « Honnête Femme/Homme » du XXIème siècle.

Une étude publiée par le Nasdaq en avril 2016 et réalisée aux Etats-Unis, au Japon, en Grande-Bretagne, Allemagne et dans les pays nordiques révèle que 91% des dirigeants reconnaissent ne pas être en mesure d'analyser les rapports sur l'état de la cybersécurité de leur entité qui leurs sont transmis. A quoi bon être informé si les messages fournis restent illisibles et dénués d'intérêt stratégique ? Ne limitons pas la connaissance des opportunités liées au déploiement du numérique aux seuls périmètres des métiers. Il convient d'y ajouter une information régulière et facilement compréhensible sur les questions de sécurisation des actifs numériques. Au risque de voir s'évaporer les éléments différenciateurs qui fondent l'existence d'une entreprise et lui assurent un avenir économique. Cette perspective relève pleinement des attributs d'un dirigeant. Charge à lui/elle de trouver les moyens de bénéficier de cet éclairage et de l'intégrer avec profit dans les avantages concurrentiels qui participeront à son succès. ■

Dernier ouvrage paru :

« La Cybersécurité », Collection Que Sais-je ? Presses Universitaires de France.

Pour le contacter :

Twitter : @cyberguerre

www.arpagian.eu

CYBERCRIME : QUAND LA NÉCESSITÉ D'UNE COOPÉRATION INTERSERVICES ET INTERNATIONALE S'IMPOSE

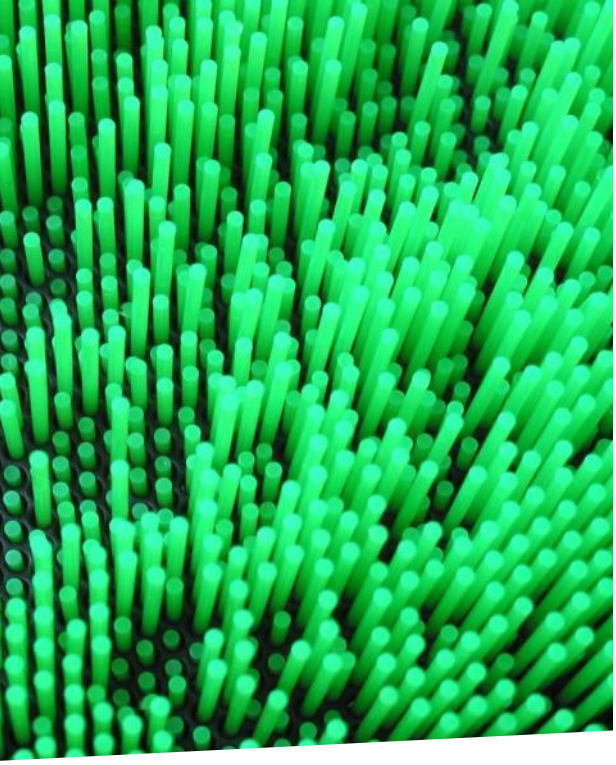
Général d'armée (2S) Marc WATIN-AUGOUARD | Directeur du Centre de recherche de l'École des officiers de la Gendarmerie Nationale.

■ Mon Général, vous vous êtes beaucoup investi dans la découverte du cyberespace et dans la lutte contre toute forme de cybercrime. On vous qualifie souvent de « cybergendarme dans l'âme ». Cette appellation vous fait-elle sourire ?

C'est très sympathique ! « Cybergendarme », je le suis peut-être, espérant que tous ceux qui œuvrent sur le terrain m'acceptent dans leur communauté « Cybergend », malgré mes faibles connaissances techniques. « Dans l'âme », c'est mon ambition ! Dès l'origine, j'ai pensé qu'il ne fallait pas limiter l'enjeu à la question « Comment ? », mais s'interroger aussi -et surtout- sur le « Pourquoi ? ». Plus la transformation numérique va produire ses effets (nous n'en sommes qu'aux prémices), plus va se poser la question du sens, de la place de l'Homme dans l'espace numérique. La dimension éthique, sociologique, philosophique est essentielle. Les sciences humaines doivent converger avec les « sciences dures » pour que l'Homme soit le maître du cyberespace et non l'esclave. Le juriste doit avoir une culture scientifique, le scientifique inscrire son action dans une approche humaniste. Confiance, loyauté, solidarité seront, grâce à l'espace numérique, les valeurs en pointe du XXIe siècle. « *Science sans conscience n'est que ruine de l'âme* », écrivait Rabelais. Je suis un rabelaisien inconditionnel ! Paraphrasant Saint Matthieu, j'ajouterai « *Que servirait à l'Homme de gagner le cyberespace s'il venait à y perdre son âme ?* ».

■ Administrations, collectivités territoriales, entreprises, particuliers… La cybersécurité concerne tous les acteurs. Est-il difficile de faire comprendre la nécessité d'une mobilisation générale et d'une « cyberposture » face à ces risques dans notre pays ?

Un enfant ne comprend le danger d'une gazinière que le jour où il s'y est brûlé. Nous sommes tous des enfants ! Mais nous atteignons aujourd'hui l'adolescence, c'est-à-dire la période où l'on découvre la vraie vie. Hier, la cyberattaque ne concernait que les autres… Aujourd'hui, la prise de conscience est manifeste, dans l'administration, les entreprises et même chez les particuliers. Il y a encore une marge de progrès. Mais cette prise de conscience n'est pas toujours suivie d'actions à la hauteur des risques et des enjeux. Les prescripteurs, dont les hommes et les femmes politiques, doivent être les premiers convaincus. D'où la nécessité de rendre obligatoire une formation à la cybersécurité pour l'obtention de tout diplôme d'enseignement supérieur. La formation est la clef. Malgré des initiatives heureuses, de futures « élites » sortent encore des universités et des grandes écoles sans avoir la moindre culture « cyber ». Demain, nous risquons d'avoir un marché de l'emploi déséquilibré, la demande dépassant l'offre. Par exemple, il nous faudra de plus en plus de « datascientists », les transformateurs de la donnée, alors que le nombre de formation diplômantes est encore insuffisant. La mobilisation passe aussi par le développement de la réserve opérationnelle ou citoyenne qui contribue à la cybersécurité en apportant son expertise, mais participe aussi à la « cyberrésilience » par son action au sein de la société. C'est une manière de replacer le citoyen au cœur de la sécurité et de la défense.



■ Plus spécifiquement, comment qualifierez-vous actuellement la place et le rôle de la Gendarmerie Nationale dans la lutte contre la cybercriminalité ?

La Gendarmerie Nationale figure parmi les pionniers. N'oublions pas qu'elle a choisi, il y a plus de trente ans, le « tout numérique » pour ses télécommunications, une grande première dans le monde ! Beaucoup d'officiers et de sous-officiers ont une formation scientifique, ce qui favorise l'acculturation de l'institution. La Gendarmerie Nationale, en charge de la sécurité des personnes et des biens, constate que les menaces glissent du monde réel vers le monde immatériel. En 2007, j'écrivais que la cybercriminalité est « la criminalité du XXIe siècle ». Le prédateur est intelligent : il opère là où, le gain est optimal et le risque pénal le plus faible. Le maillage territorial de la gendarmerie (plus de 3000 brigades) est un atout pour une action de proximité au plus près d'entreprises et de citoyens qui sont souvent désemparés lors d'une cyberattaque. Nous avons un devoir d'assistance et de « rassurance ». Tout militaire de la Gendarmerie Nationale, sans être obligatoirement un expert, doit avoir une culture cyber. J'enseigne la cybersécurité à tous les officiers de l'EOGN, l'Ecole des Officiers de la Gendarmerie Nationale. Son centre de recherche (CREOGN) que je dirige est pleinement engagé dans la réflexion prospective. Nous pouvons encore progresser.

■ Comment les services de la Gendarmerie et de la Police s'organisent-ils pour lutter ensemble contre les cyberrisques ?

Depuis 2000, l'Office central de lutte contre les infractions liées aux nouvelles technologies (OCLCTIC) est un organe mixte police-gendarmerie, dont le rôle est très important, notamment en ce qui concerne le traitement des contenus illicites. La plate-forme PHAROS est d'ailleurs dirigée par un gendarme. En 2004, avec Thierry BRETON, j'ai animé un groupe de travail « Police-Gendarmerie » sur la cybercriminalité. Vous le voyez, on se parle, on travaille ensemble. Aucune des deux institutions ne peut prétendre avoir à elle seule la réponse aux enjeux. Police et Gendarmerie ne sont pas des clones. Chacune a son organisation, sa culture, ses modes d'action propres au territoire dont elle a la responsabilité. Avec sa communauté « Cybergend », forte de plus de 2000 officiers et sous-officiers, la Gendarmerie Nationale a choisi d'irriguer le territoire. La Police a plutôt concentré ses moyens. L'une et l'autre devraient contribuer à l'action de la nouvelle juridiction spécialisée que la loi du 3 juin 2016 vient d'instituer à Paris. La création attendue d'une délégation à la lutte contre les cybermenaces au sein du Ministère de l'Intérieur favorisera les complémentarités et les synergies.

■ Défenseur de l'importance du continuum défense-sécurité dans le cyberespace, trouvez-vous la coopération entre les acteurs privés et publics suffisante en France ?

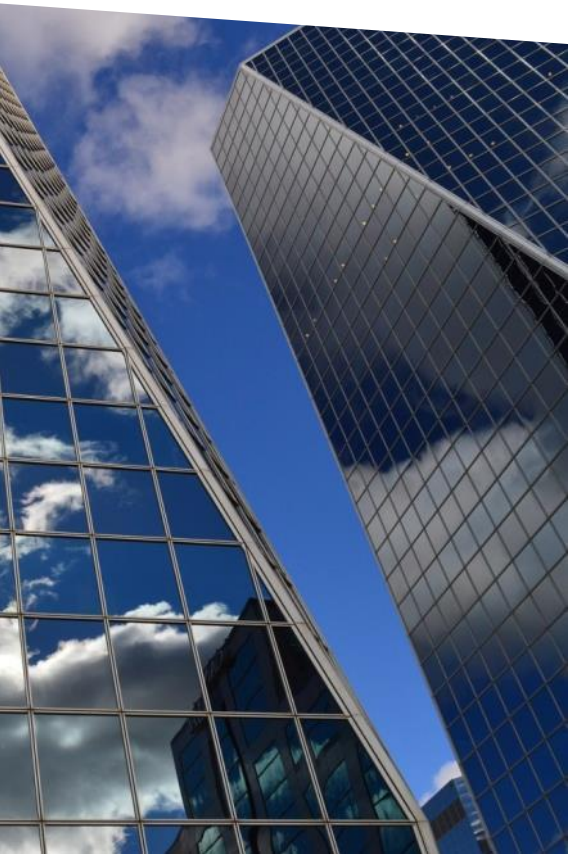
Suffisante, pas encore, mais elle progresse à grande vitesse, ne serait-ce qu'en raison du rôle moteur de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). La protection des secteurs d'importance vitale (sécurité, santé, énergie, transports, télécommunications, etc.) n'est plus une option mais une obligation légale qui implique les entreprises concernées et, par effet de cascade, les sous-traitants. Le dialogue – même si les dispositions normatives s'imposent – est le mode d'action de cette « autorité nationale » en matière de cybersécurité. Les textes sont le fruit d'une concertation, ce qui crée, me semble-t-il, un rapport de confiance. L'ANSSI est d'autant plus audible que sa position est claire quant à toute activité de renseignement ou de cyberdéfense « offensive » qu'elle écarte délibérément de son champ de compétence. Il faut encore renforcer la coopération car, l'action régalienne ne peut résoudre seule les difficultés connues et à venir. Sans renoncer à leur domaine d'attribution (toute fusion serait confusion), les acteurs publics et privés doivent agir ensemble. C'est le cas lors de cyberattaques graves. L'ANSSI intervient et, avec elle, des prestataires de sécurité privés. Nous devons aussi nous rapprocher du monde de l'assurance. Il va jouer un rôle préventif majeur, au fur et à mesure que les risques « cyber » seront couverts sur la base d'exigences, de normes de cybersécurité auxquelles il faudra se plier. La coopération public/privé est au cœur de nombreuses initiatives. J'ai l'honneur d'être le Président du Centre Expert de lutte contre la Cybercriminalité Français (CECyF) qui regroupe des administrations (Gendarmerie, douanes, DGCCRF, services fiscaux), des entreprises (La Poste, Orange, Thalès, etc.), des universités, des grandes écoles et des centres de recherche (UTT de Troyes, EPITA, Université de Montpellier, etc.), en tout plus de 35 partenaires. Nous travaillons ensemble pour développer la prévention au profit des entreprises comme des particuliers. Si vous écoutez nos échanges, vous aurez parfois du mal à identifier celui ou celle qui vient du secteur public ou du secteur privé. Les « gens du cyberespace » sont comme les « gens de mer » : ils se rassemblent parce qu'ils partagent le même milieu physique. S'agissant du continuum défense-sécurité, dont j'ai posé les principes en 1991, il s'applique tout particulièrement à l'espace numérique, ce qui impose une coopération civilo-militaire très poussée. La cyberdéfense ne commence pas là où s'arrête la lutte contre la cybercriminalité. Les deux sont intriquées et agissent en symbiose. La coopération avec les acteurs privés appelle aussi une clarification du « statut du hacker éthique » car, nous aurons de plus en plus recours à des compétences individuelles, capables de tester les systèmes pour mieux en garantir la sécurité, en toute bonne foi, bien sûr !

■ Existe-t-il une culture du web différente entre les organismes publics et les entreprises privées ? Si c'est le cas, cela influe-t-il sur la difficulté à trouver une réponse commune et uniforme face à la menace ?

J'ai le sentiment que les cultures sont proches, tout simplement parce que les outils sont les mêmes. Ce qui distingue les uns des autres ce sont les finalités, les services rendus. Je crois cependant qu'il y a une forte convergence. Les organismes publics, grâce à la transformation numérique, vont davantage regarder « l'usager » comme un client. Le web permet de refonder le service public en garantissant sa continuité, son ubiquité, sa proximité, etc. La donnée est - et sera - au cœur de l'action des acteurs. Les systèmes connectés vont achever le mouvement de rapprochement entre les deux secteurs. On observe par ailleurs une prise de conscience conjointe de la nécessité de changer la gouvernance des organismes publics et privés, de modifier la conception du « travail » selon un mode plus réticulaire, plus distribué. Les organismes vont prendre une forme « galactique » alors qu'ils avaient été construits sur un modèle vertical, en silos, en « Tour Eiffel ». Sans risquer la polémique sur le statut des fonctionnaires, je parie sur une très grande « porosité » entre le public et le privé dans les vingt prochaines années.

■ Au niveau international, peut-on dire qu'il y a un vrai consensus et une réelle coopération efficace en matière de cybersécurité ? Un mouvement européen se met-il en place ?

Il faudrait tout d'abord que l'on s'entende sur la gouvernance mondiale. La Conférence mondiale de l'UIT, en décembre 2012, à Dubaï, a consacré la coupure du monde en deux blocs : il y a ceux qui veulent une gouvernance de l'Internet (pour faire en sorte qu'il fonctionne en garantissant la sécurité, la neutralité, l'égalité, etc.) et ceux qui veulent une gouvernance sur Internet qui ajoute la surveillance des contenus au titre de la sécurité nationale. La cybersécurité accentue les démarches égoïstes car, elle conditionne la souveraineté nationale. Pour autant, on sait qu'une coopération est indispensable. Elle prend du temps à se mettre en marche. La Convention du Conseil de l'Europe contre la cybercriminalité (Convention de Budapest du 21 novembre 2001) n'a été ratifiée que par 49 pays. C'est encore peu mais, le nombre augmente chaque année. Beaucoup de pays africains qui ont signé la Convention de Malabo (Union Africaine) regardent vers la Convention de Budapest – je pense au Sénégal, dont le rôle moteur est manifeste. Il y a une tendance – certes lente – à la coopération. Mais il y aura toujours de mauvais élèves, des Etats « cybervoyous ». Pour progresser dans la coopération, il faut avancer dans la réforme de la gouvernance d'Internet. L'affaire PRISM a mis en exergue la nécessité de réformer profondément l'ICANN, l'organisme qui gère notamment le « .fr » et qui est sous la tutelle du Département d'Etat du Commerce américain. Depuis mars 2016, de nouveaux statuts –encore imparfaits – annoncent une amélioration de la situation, mais il y a encore beaucoup de chemin à parcourir. Quelle belle opportunité pour l'Europe, blessée par le Brexit ! Au lieu de se préoccuper du débit uniforme des chasses d'eau, qu'elle engage notre Vieux Continent dans l'ère numérique ! Elle le fait, mais encore trop lentement. Nous ne remercierons jamais assez la Cour de justice de l'Union européenne, dont, la jurisprudence récente est historique ! Les arrêts sur le transfert transatlantique des données, sur le « droit à l'oubli » font bouger les lignes. Le salut viendra du tandem franco-allemand. Il y a deux ans, au FIC, nous avons reçu le ministre fédéral Thomas DE MAIZIERE. L'ANSSI travaille de conserve avec son homologue. Il faut un rapprochement industriel car, il n'y a pas de cybersécurité sans un tissu d'entreprises « souveraines ». Le couple franco-allemand est le moteur de l'Europe. Qu'il avance, les autres suivront ! N'oublions pas cependant nos amis britanniques – en tout cas ceux qui voulaient rester parmi nous – et qui sont ultra majoritaires dans la communauté cyber qui sait qu'on ne se grandit pas en se repliant, dans un monde désormais hyperconnecté.



■ Vous êtes également le fondateur et le co-directeur du Forum International de la Cybersécurité (FIC). Ces deux jours de rencontres et d'échanges entre les acteurs publics et privés, participent-t-il de cette volonté de maintenir une relation et une coopération forte entre le privé et le public, entre la France et ses voisins internationaux ?

Ce FIC, je l'ai conçu en 2005 et lancé en 2007 pour faire sauter toutes les barrières nationales et internationales. Je peux vous dire qu'à l'époque certains pensaient que c'était ma « danseuse ». Aujourd'hui, les « pères » sont nombreux…Je ne m'en plains pas. L'Europe, grâce au regretté Jacques BARROT était mon partenaire d'origine. Elle m'a abandonné ! Mais elle revient…Le FIC est pour elle, si elle le veut, un extraordinaire vecteur pour faire entendre une voix de l'Europe qui offrirait au reste du Monde une alternative à la seule option qui se dessine : être « américain ou chinois ». Pendant ces deux jours (24 et 25 janvier 2017 à Lille), nous allons réunir plus de 6 000 experts publics et privés, 250 entreprises, venant du monde entier et, bien sûr du Royaume-Uni, de la Belgique, des Pays-Bas, etc. Les administrations vont rencontrer les entreprises. Il y aura du business (ce n'est pas l'objectif premier) mais aussi du contenu avec de très nombreuses interventions (plénières, conférences, ateliers, démonstrations) qui font avancer la conception du Nouveau Monde numérique. J'ai, depuis l'origine, l'ambition de créer le « Davos de la cybersécurité ». Grâce à toute l'équipe autour de Guillaume TISSIER, le FIC a déjà un rayonnement mondial car, il répond précisément à toutes les questions : Comment ?, Pourquoi ? Pour le « Combien ? », je vous laisse traiter directement avec les entreprises… ■

FOCUS SUR LA RÉSERVE CITOYENNE DE CYBERDÉFENSE

Bénédicte PILLIET | Adjoint Rayonnement auprès du Coordinateur National de la Réserve Citoyenne de Cyberdéfense.

■ Est-ce votre parcours professionnel qui vous a amené à faire partie de la Réserve Citoyenne de Cyberdéfense ?

La Réserve Citoyenne Cyberdéfense (RCC) a été créée il y a trois ans et lancée sous l'autorité du Vice-Amiral Arnaud COUSTILLIERE. C'est effectivement parce que dans le cadre de mes fonctions professionnelles, j'animais déjà des communautés et des sujets sur le thème de la cybersécurité que l'Amiral m'a appelé auprès de lui pour participer à la création de cette Réserve. La RCC est désormais le premier réseau spécialisé de réservistes cyber avec 150 membres, de profils très différents, professionnels du sujet avec des compétences complémentaires – juristes, universitaires, communiquants, etc. - La vocation de la RCC est de participer à la création d'un esprit de cyberdéfense-cybersécurité au sein de la Nation, en appui des actions des institutions de l'Etat en charge de ces questions. Il faut bien se rendre compte qu'il y a trois ans lorsque nous avons commencé à travailler sur ce sujet, nous partions de très loin en matière de sensibilisation. Ce n'était pas du tout un sujet sur le devant de la scène comme c'est le cas aujourd'hui.

Actuellement, au sein de la Réserve Citoyenne de Cyberdéfense, je suis en charge du rayonnement et de la coordination des différentes actions qui sont menées à ce titre, afin d'avoir une stratégie globale et une identité de communication sur l'ensemble du territoire national, sur lequel la RCC est présente à travers ses 7 groupes régionaux. Etre membre de la Réserve Citoyenne Cyberdéfense, c'est avoir des compétences et une expertise que l'on souhaite mettre volontairement et bénévolement, dans un esprit citoyen d'engagement, à disposition de la Réserve et au service de la Nation. C'est vraiment un état d'esprit.

■ Quelles sont les missions de ce réseau ?

La Réserve Citoyenne de Cyberdéfense a pour mission principale de mener des actions de sensibilisation sur la cybersécurité, en coordination avec les institutions qui sont en charge de ces questions au sein de la Nation – l'ANSSI, le Ministère de la Défense, le Ministère de l'Intérieur qui sont nos autorités de tutelle. Autrement dit, être membre de la RCC c'est porter l'esprit de cybersécurité au sein de la Nation, et participer ainsi à l'esprit de Défense, afin que chacun appréhende mieux les enjeux et s'approprie cette dimension dans ses activités. L'objectif de la RCC est ainsi de sortir la cybersécurité de cette image parfois trop technique ou trop strictement « militaire », pour montrer que chacun est concerné. Nous travaillons plus particulièrement à destination de certains publics, comme les PME-PMI, les jeunes ou les chercheurs-universitaires, en sciences dures et en sciences humaines. Les membres de la RCC apportent également en cas de besoin leurs expertises sur certains sujets de réflexion, en fonction des demandes des institutions.

Nous avons une démarche très proactive, fondée sur les échanges, le dialogue et la disponibilité. Néanmoins, et c'est un point fondamental, nous sommes là pour apporter un soutien à nos institutions et non pour se substituer à elles dans leurs missions. Ce qui est très intéressant au niveau de la RCC, c'est que nous travaillons en interministériel. Le Ministère de la Défense n'est pas notre seule autorité de tutelle : nous relevons également du Ministère de l'Intérieur et de l'ANSSI. Cette dimension interministérielle est très novatrice et adaptée à la transversalité

caractéristique de la cybersécurité. Elle nous permet d'aborder les sujets dans l'ensemble des secteurs de la Nation qui tous sont concernés. Autre caractéristique qui fait la richesse de la RCC et montre son caractère transverse : nos membres appartiennent à des réserves de l'ensemble des armées, Terre, Air, Marine et Gendarmerie, ce qui là encore est très novateur.

■ Concrètement, pouvez-vous nous citer des actions actuelles ou à venir de la RCC notamment en matière de sensibilisation ?

Ces actions de sensibilisation sont à destination de différents publics. Concrètement, notre première action a été de concevoir et de réaliser des fiches de sensibilisation sur les enjeux de la cybersécurité. Ces fiches sont des infographies simples de compréhension, disponibles gratuitement en téléchargement sur le site du Ministère de la Défense. Elles permettent par exemple à chacun de comprendre comment fonctionnent les différentes cyberattaques - DDoS, phishing, APT, etc – et de disposer de recommandations pour s'en prémunir.

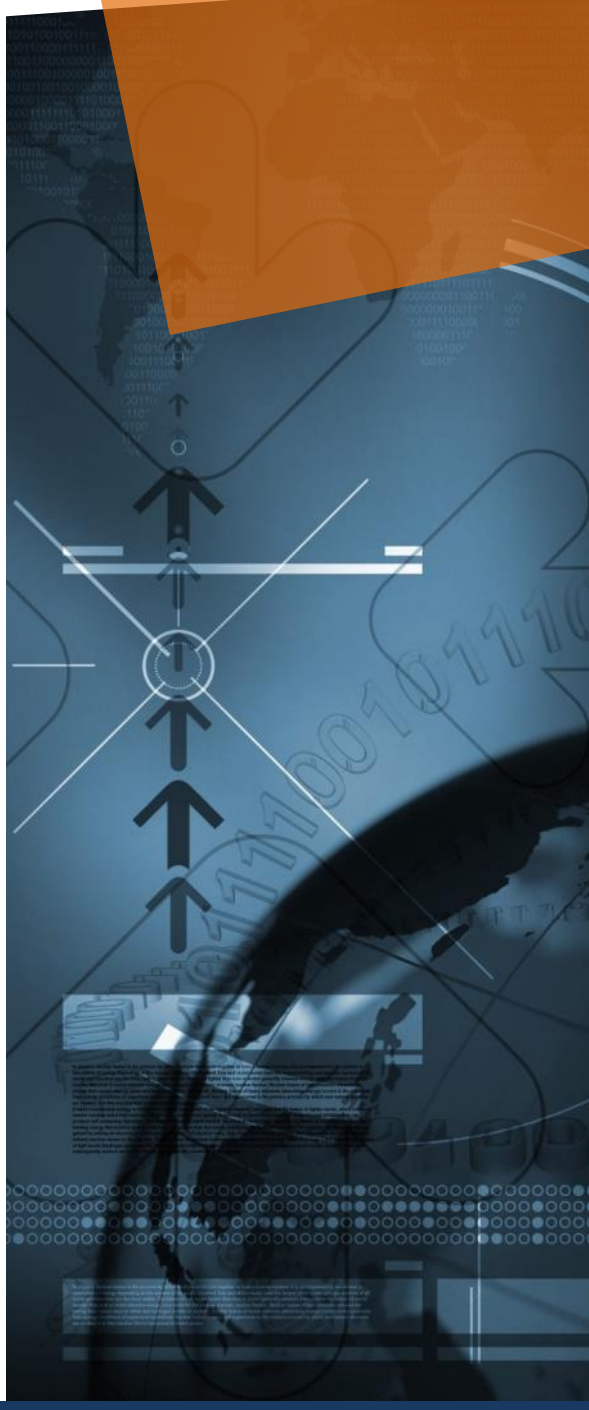
Nous avons également mis en place un module de sensibilisation à destination des PME/PMI, accessible et compréhensible par tout dirigeant. Ce module met en exergue les enjeux de la cybersécurité pour une entreprise de façon très pragmatique, et vise à donner des pistes de réflexion afin de construire une véritable stratégie de cybersécurité. La présentation a été validée par nos institutions de tutelle, ce qui est un point important car, les informations que nous y présentons sont des informations fiables – on entend parfois trop des « spécialistes autoproclamés » qui portent si ce n'est des contre-vérités, au moins des approximations... Nous avons construit cette présentation en une vingtaine de slides qui servent de base à nos réservistes pour aller faire des présentations au sein de colloques, de conférences, de congrès réunissant des PME/PMI et dont les organisateurs acceptent de nous accorder une heure trente.

Disponible à la fin de l'année 2016, nous avons aussi créé un jeu de plateau autour de la cybersécurité-cyberdéfense : « Cyberstratégia ». Ce support nous permet de manière pédagogique et ludique d'expliquer les différents concepts liés à cet univers. Chaque joueur représente un Etat doté de caractéristiques historiques, économiques et sociétales définies, qui doit à la fois renforcer sa stratégie de cybersécurité, se défendre des cyberattaques menées par les autres joueurs, mais également construire une stratégie offensive. Des parties de jeu, « accessibles de 7 à 77 ans » comme on le dit traditionnellement, seront organisées par les groupes régionaux, et je ne doute pas pour avoir participé à des parties test, que l'ambiance sera bonne !

Autre action concrète : nous avons lancé cette année « le Défi RCC : MA THESE 3.0 », un concours à destination des doctorants qui travaillent sur les sujets de cybersécurité, que ce soit en sciences dures ou en sciences humaines. Ce concours permet aux jeunes chercheurs de venir présenter leur thèse en 3 minutes devant un jury de hautes personnalités, co-présidé par le Vice-Amiral COUSTILLIERE et Christophe BONNARD, le Coordinateur national de la RCC. Avec le Défi RCC, nous souhaitons à la fois valoriser ceux qui aujourd'hui travaillent sur ces sujets au niveau universitaire, favoriser les échanges entre eux et la communauté de cybersécurité, et favoriser les vocations. La deuxième édition s'est déroulée en mai dernier à l'Ecole militaire à Paris. Le milieu de la Recherche étant un milieu important pour nous, nous organiserons également en octobre de chaque année une conférence des Chaires qui travaillent sur la cybersécurité. Cet événement permet ainsi de créer un rendez-vous annuel où les chercheurs et l'ensemble des acteurs de la cybersécurité peuvent se rencontrer et échanger, autour de la valorisation des travaux qui auront été conduits au sein des chaires.

Au travers de ces différents exemples, nous retrouvons toujours notre objectif de sensibiliser les différents publics, de créer cette culture de cybersécurité en favorisant les espaces de rencontres et d'échanges entre différents acteurs, et de participer à l'animation de l'esprit de cybersécurité au sein de la Nation.

« Notre objectif est de sensibiliser les différents publics, de créer cette culture de cybersécurité en favorisant les espaces de rencontres et d'échanges entre différents acteurs, et de participer à l'animation de l'esprit de cybersécurité au sein de la Nation »



■ Comment cette Réserve Citoyenne de Cyberdéfense s'organise-t-elle ?

La RCC a été organisée sur Paris selon des groupes de travail thématiques dédiés animés par des chargés de mission. Assez rapidement, il a été décidé de créer également des groupes régionaux de réservistes locaux qui se sont inscrits dans la philosophie et la démarche que je vous ai exposées. En collaboration étroite avec les groupes de travail thématiques, qui par exemple leur fournissent des outils comme le module de sensibilisation ou les fiches pédagogiques, les groupes régionaux mènent un certain nombre d'actions auprès du tissu économique local, notamment des actions en matière de sensibilisation, au plus près des préoccupations des acteurs locaux, là encore en soutien de nos institutions. Par exemple, comme vous le savez, l'ANSSI est en train de déployer des coordonnateurs régionaux. En perspective de cela, les groupes régionaux de la Réserve Citoyenne Cyberdéfense ont vocation à se mettre à leur service.

■ En termes d'organisation, vient d'être créée cette année, une Réserve de CyberDéfense. Pouvez-vous nous en parler et nous indiquer quelle est son rôle en complément de la Réserve Citoyenne Cyberdéfense ?

En effet, cette année a été créée la Réserve de CyberDéfense (RCD). C'est une réserve cyber à vocation opérationnelle. En termes de recrutement, nous recherchons des informaticiens. La RCD sera composée de spécialistes informatiques qui vont accepter de venir travailler avec les différentes institutions (ANSSI, Ministère de la Défense, Ministère de l'Intérieur) et qui pourront être sollicités en cas de crise. Le format qui a été arrêté pour cette réserve est très original. Elle sera composée majoritairement d'étudiants des écoles informatiques et des écoles d'ingénieurs qui auront signé un partenariat avec le Ministère de la Défense. Ce partenariat consiste pour les étudiants à s'engager en soutien des instances institutionnelles en cas de crise cyber majeure. Ces étudiants seront formés et participeront à des exercices. On voit bien ici la philosophie gagnant-gagnant de cette réserve qui permet à la Nation de bénéficier d'un réservoir de compétences en cas de crise cyber, et aux étudiants de bénéficier d'un plus durant la période de formation, tout en participant à l'effort national. Sans oublier les spécialistes et des profils d'encadrement de réservistes opérationnels, professionnels civils qui « basculent » dans le cadre militaire en cas de besoin.

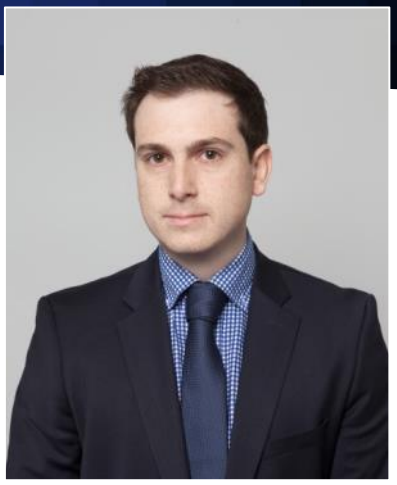
■ A ce propos, j'ai donc lu que la Réserve de CyberDéfense (RCD) souhaite renforcer ses effectifs et compter 4300 cyber réservistes dans ses rangs d'ici 2019. Est-ce vrai ?

4440 plus exactement ! L'objectif est en effet de compter environ 4000 jeunes réservistes cyber à vocation opérationnelle. Nous y ajouterons environ 400 réservistes opérationnels, professionnels dans le civil. En complément, nous compterons sur un état-major d'une quarantaine de militaires qui viendront encadrer l'ensemble du dispositif. C'est cela qui va créer ce dynamisme de gestion de crise pour répondre à une crise cyber majeure. Cela nous permettrait de pouvoir faire face à une menace grandissante et de disposer d'un vivier à mobiliser en cas de crise majeure dans le pays.

■ Vigilance citoyenne, réserve citoyenne… Pensez-vous que cette notion de citoyenneté est la base nécessaire à toute tentative de sensibilisation, d'information et de diffusion de l'esprit de défense et de protection auprès des français ?

Les enjeux de cybersécurité sont tels aujourd'hui au niveau de la défense et de la sécurité nationale que la dimension de citoyenneté est une base indispensable lorsqu'on aborde ces sujets. La cybersécurité concerne aujourd'hui l'ensemble de la Nation et chacun de nous à son niveau a un rôle à jouer. La Réserve Citoyenne de Cyberdéfense est un vecteur très pertinent pour sensibiliser aux enjeux mais il faut être réaliste : cela ne suffit pas. C'est ce que nous disons d'ailleurs lorsque nous faisons de la sensibilisation auprès des entreprises. Nous ouvrons la porte à la prise de conscience. Ensuite, il est indispensable que le dirigeant s'empare du sujet et le monte au niveau stratégique. Cela doit se traduire par des outils et une organisation techniques bien sûr, mais également par des formations dédiées pour les collaborateurs – et là quand je parle de formation, je ne parle pas de formations techniques, mais de formations d'usage aux réflexes à avoir dans son vécu quotidien professionnel, aux fameuses règles « d'hygiène informatique »… « Le maillon faible se situe le plus souvent entre le clavier et la chaise » : il est donc nécessaire d'aller plus loin qu'une simple sensibilisation et de renforcer ses bons réflexes pour éviter, autant que faire se peut, des erreurs de comportement qui peuvent avoir de lourdes conséquences.

La notion de citoyenneté dans la cybersécurité est importante puisque chacun a son rôle à jouer dans la protection globale contre les cybermenaces. Le jour où on aura gagné, c'est le jour où chaque citoyen aura conscience de cela. Chacun peut être victime d'une malveillance cyber, mais chacun peut aussi être un acteur positif en la matière. C'est aussi le sens de l'action de la Réserve Citoyenne de Cyberdéfense. ■



L'ANSSI : BIENTÔT UN NOUVEAU RÉFÉRENT EN RÉGION PACA, RETOUR SUR CE PROJET

Jean-Sylvain CHAVANNE | Adjoint au chef du Bureau Coordination territoriale au sein de l'Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI).

■ Pouvez-vous nous présenter les missions des Observatoires Zonaux de la Sécurité des Systèmes d'Informations (OZSSI) qui étaient mis en place dans chaque zone de défense et de sécurité en France ?

Comme vous l'évoquez, les OzSSI ont été mis en place dans chaque Préfecture de zone de défense et de sécurité. Ils étaient donc rattachés au Préfet de zone. Sous les orientations de l'ANSSI, ils avaient pour missions de soutenir les administrations locales, d'animer les réseaux (et le partage d'expérience) mais également de faire remonter les signaux précurseurs d'incidents. Ils étaient également les relais territoriaux de l'ANSSI notamment auprès des acteurs économiques locaux. La mission des OzSSI a pris fin le 1er juillet dernier pour laisser place au dispositif territorial de l'ANSSI.

■ A partir du 1er juillet 2016, ils passent progressivement le relai au niveau dispositif des référents territoriaux dépêchés par l'ANSSI. Pour le cas de notre région Provence Alpes Côte d'Azur (PACA), quelles seront ses futures missions et son rôle à venir ? Quand sera-t-il nommé ?

L'ANSSI est un service à compétence nationale. Pour remplir au mieux ce rôle, les référents « sécurité numérique » auront la charge de représenter l'Agence au sein des différentes régions, et notamment de la région PACA, auprès des interlocuteurs locaux que l'on a peu l'occasion de rencontrer depuis Paris comme les pôles de compétitivité, les TPE/PME, les mairies etc. Le référent aura donc deux rôles majeurs : en premier lieu, il s'agira d'être l'interlocuteur privilégié des collectivités territoriales, des administrations et des entreprises afin de les sensibiliser sur la mise en place de la sécurité au sein de leurs systèmes d'Information. Mais il s'agira également d'apporter un soutien aux politiques publiques en matière de sécurité économique.

Concrètement, l'ANSSI souhaite participer à la défense des intérêts économiques en prenant en charge l'animation des réseaux pour accompagner les différents acteurs à la sécurisation de leurs systèmes d'Information. Pour cela, le référent « sécurité numérique » de l'ANSSI devra travailler en symbiose avec les différentes dynamiques déjà existantes comme les pôles de compétitivité et les clusters par exemple mais également les syndicats mixtes et les communautés de communes. L'objectif est de renforcer les politiques publiques en cours sans en créer de nouvelle. Pour la région PACA, nous souhaitons nommer le référent très rapidement, si possible avant l'automne car, la demande est de plus en plus grande pour cette région riche et dynamique.

■ Globalement, quel est le profil de ces référents territoriaux ?

Pour représenter l'ANSSI de manière cohérente, les représentants en région sont généralement des ingénieurs qualifiés qui ont un minimum de deux ans d'ancienneté au sein de l'Agence. Cette expérience est nécessaire pour connaître les différents dispositifs de l'ANSSI tels que, les guides de bonnes pratiques à destination des collectivités territoriales et des entreprises, les prestataires qualifiés, les labels etc.

■ Quelle réflexion interministérielle a déclenché la nécessité de ce déploiement territorial et de fait ce renforcement tant au niveau central que local ?

L'expérience positive des OzSSI a démontré que le besoin était présent mais que le dispositif était sous-dimensionné. Une réflexion interministérielle a donc eu lieu entre l'ensemble des services de l'État concernés par la sécurité économique. Cette réflexion a déterminé qu'il devait y avoir une complémentarité entre les missions locales d'intelligence économique et la cybersécurité et que l'échelon régional devait servir de point d'appui de l'action de l'État en matière de sécurité des systèmes d'Information. Dans le prolongement de ces réflexions, l'ANSSI a décidé d'agir en créant son dispositif territorial afin d'offrir un contact de proximité qui saura prendre en compte les particularités locales et ainsi, mieux répondre à la demande en matière de cybersécurité.

■ Ce nouveau dispositif est davantage au contact de l'ensemble du tissu économique local. Vis-à-vis de cela, trouvez-vous qu'en matière de cybersécurité, « l'union fait la force » et qu'il est indispensable aujourd'hui d'agir ensemble ?

En matière de sécurité, il est nécessaire d'être collectif. Quelquefois, nous allons rencontrer des PME qui sont déjà sensibilisées à la notion de protection de leur patrimoine informationnel mais le plus intéressant est de faire partager cette expérience. C'est pour cela que le référent de l'ANSSI va chercher à toucher des associations d'entreprises pour non seulement faire prendre conscience de l'importance de telles mesures mais également pour faire partager des expériences positives et ainsi créer une véritable dynamique commune qui bénéficiera à la compétitivité de l'ensemble des entreprises de la région. ■

Agence Nationale de la Sécurité des Systèmes d'Information

Secrétariat général de la défense et de la sécurité nationale
51, boulevard de La Tour-Maubourg, 75700 Paris 07 SP

www.ssi.gouv.fr

01 71 75 84 05
01 71 75 84 06

« Les référents « sécurité numérique auront la charge de représenter l'Agence au sein des différentes régions »

DIRECTEUR DES SYSTÈMES D'INFORMATION, UN RÔLE DE PLUS EN PLUS CENTRAL DANS LA STRATÉGIE DE L'ENTREPRISE

Christophe DUVAL | Directeur des Systèmes d'Information chez AGATHA PARIS.

■ En poste depuis quelques mois en tant que Directeur des Systèmes d'Information chez Agatha, quels sont les grands travaux qui vous ont été confiés ?

Comme souvent, pour les missions d'un Directeur des Systèmes d'Information (DSI), je possède trois périmètres d'action : le périmètre opérationnel à savoir, la maintenance en condition opérationnelle de l'ensemble des systèmes au sein du siège social (gestion des serveurs, de la messagerie, de l'ERP), le périmètre de la gestion des systèmes d'Information en magasin et le périmètre de la digitalisation rattachée plus ou moins à la Direction Marketing et à la Direction Générale.

Donc, pour répondre à votre question, il y a plusieurs grands projets qui m'ont été confiés dès mon arrivée tels que la mise en place d'une véritable solution de digitalisation des points de vente. C'est le grand projet d'aide à la vente grâce à l'installation de tablettes numériques en magasin. C'est vraiment l'un de nos grands projets en termes de multimédia. Il y a également la refonte totale du site e-commerce de l'entreprise et l'organisation d'une stratégie CRM et d'étude client. Vous voyez donc que la dimension stratégique est déjà belle et bien présente dans ces différents projets impliquant la Direction des Systèmes d'Information au sein de l'entreprise.

■ Le rôle du Directeur des Systèmes d'Information est en pleine évolution. Ressentez-vous cette mutation au niveau de vos missions depuis votre arrivée à ce poste ?

Tout à fait ! Je pense que ce n'est pas une mutation jeune. Elle est en cours depuis une dizaine d'années déjà. Vous savez, il y a encore quelques temps, la Direction des Systèmes d'Information était souvent rattachée à la Direction Administrative et Financière de l'entreprise. Elle était considérée comme de l'administratif ou de la bureautique pure. Heureusement, ce n'est plus du tout le cas aujourd'hui. En effet, les questions et les enjeux relatifs aux systèmes d'Information de l'entreprise deviennent beaucoup plus transverses. Les métiers dépendent systématiquement de l'informatique à un moment donné (échanges d'informations internes ou externes, aide à la vente en magasin, étude des évolutions des gammes et des cycles de vie produit…). Pour prendre cet exemple, les équipes marketing sont parfois démunies car, il y a souvent besoin d'une compétence technique pour formaliser l'information. Toutes ces questions sont forcément liées à un outil informatique qui vient s'interfacer avec les différents métiers. C'est un accompagnement quotidien.

■ Etes-vous d'accord pour dire que le Directeur des Systèmes d'Informations est devenu un véritable acteur de la stratégie de l'entreprise aujourd'hui ?

En effet, je pense que la Direction des Systèmes d'Information devient un acteur à part entière de la stratégie de l'entreprise. Outre ses fonctions initiales, là où le Directeur des Systèmes d'Information a désormais un rôle stratégique au sein de l'entreprise, c'est qu'il peut également être force de propositions. Il peut aller proposer aux différents services des outils stratégiques dans le cadre de l'exercice de leurs fonctions comme des outils pour la restitution d'informations, pour le CRM ou l'ERP de l'entreprise.

Globalement, au sein d'Agatha, cela commence à devenir plus prégnant dans les esprits. L'approche a commencé à évoluer avec le temps. Néanmoins, il arrive encore parfois que les différents métiers de l'entreprise ne pensent pas forcément à me solliciter. Nous ne sommes pas encore suffisamment pris en considération. Cela s'explique simplement par le fait que les membres de la Direction des Systèmes d'Information sont encore un peu vus comme de simples acteurs au service de la bureautique de l'entreprise. Or, nous avons la capacité légitime de proposer de très nombreux services et outils d'aide à la décision qui sont stratégiques de fait. Dans le cadre de mes fonctions, c'est donc une réelle volonté et un fort positionnement que de placer la Direction des Systèmes d'Information en tant que partenaire stratégique de l'entreprise du fait des projets auxquels nous participons.

■ Stratégique, le DSI doit l'être également vis-à-vis des diverses transformations numériques qui se jouent dans son environnement de travail. Comment vous adaptez-vous à cela quotidiennement au sein du groupe Agatha ?

Pour s'adapter à la transformation numérique qui se joue inévitablement dans toute entreprise aujourd'hui, Agatha porte un grand projet de digitalisation des points de vente. Je vous en ai parlé tout à l'heure. Là, nous sommes purement sur un projet liant la Direction des Systèmes d'Information à la stratégie de l'entreprise. Comme pour beaucoup d'entreprises actuellement, l'objectif est d'être présent de plus en plus multi et cross canal. Nous souhaitons que chacun de nos clients soit identifiable en point de vente comme sur le site Internet. Tout cela, nous le voulons perméable aux différents environnements techniques que sont l'encaissement traditionnel, le site internet, la visibilité des stocks en entrepôt, etc. Initialement, c'est un projet interne qui proposait la création d'un catalogue des articles de l'entreprise dans le but d'une économie de papier. Pour moi, il était évident dès le départ que ce projet devait aller beaucoup plus loin que cela. J'ai donc apporté quelques évolutions pour aboutir à ce projet que je vous présente ici. Désormais, il mêle les acteurs de la Direction des Systèmes d'Information, de la Direction Marketing, de la Direction client et de la stratégie même de l'entreprise. De nouveau, ce projet illustre donc bien la dimension transversale des missions imposées à la DSI et son lien stratégique avec les ambitions de l'entreprise en termes de développement, de croissance et de compétitivité.

■ Considérez-vous que la démarche de virtualisation informatique soit une des solutions efficaces possibles pour optimiser la sécurité, maîtriser vos ressources et permettre un gain de compétitivité et d'économie ?

Pour cette question, il est vrai que nous sommes davantage sur des questions d'infrastructures des outils informatiques. Il est évident que la partie mobilité est complètement cloudée. C'est bien sûr un long débat. Le web de la même façon. Concernant, le cloud de la partie bureautique, c'est pour moi l'un des gros chantiers de l'année 2017. Selon moi, l'avenir des systèmes d'Information passera inévitablement par le Cloud. L'objectif est de ne plus avoir de serveur dans une entreprise. Nous essayons d'ores et déjà d'en supprimer le plus possible. En effet, cela demande des investissements massifs, des licences nombreuses aux mises à jour conséquentes et une infrastructure technique importante. De plus, avec cette organisation informatique, l'accessibilité aux données est directement liée à l'entreprise physiquement. A la différence, lorsque l'entreprise commence à travailler, via le Cloud, les données sont hyper-accessibles et ultra partageables entre les collaborateurs, sauvegardées de manière automatique. Je fais souvent le comparatif suivant. Il y a cinquante ans encore, une entreprise avait son propre groupe électrogène. Or, vous en conviendrez tout comme moi, cela ne nous viendrait plus à l'idée aujourd'hui. Pour l'informatique, c'est la même chose. Il faut laisser la partie liée à l'exploitation serveur aux grands opérateurs qui, en mutualisant tout cela, font nettement mieux et à plus faible coût. Selon moi, la démarche de virtualisation informatique est d'une efficacité à toute épreuve et un gain de compétitivité énorme. Cela dégage l'informatique de sa mission d'exploitation pure et dure qui d'ailleurs n'est pas sa grande force en matière de valeur ajoutée.

Vis-à-vis des enjeux liés à la transformation numérique, la Direction des Systèmes d'Information doit aujourd'hui passer davantage de temps sur des projets et des problématiques beaucoup plus stratégiques pour l'entreprise. ■

Visitez leur site Internet et contactez les sur :

www.agatha.fr

AGATHA
PARIS

« La démarche de virtualisation informatique est d'une efficacité à toute épreuve et un gain de compétitivité énorme »

QUAND LE MONDE BANCAIRE MONTE DE FRONT CONTRE LA CYBERCRIMINALITÉ

Anne-Laure COUCHOT | Responsable Risques Opérationnels et Responsable de la Sécurité des Systèmes d'Information - Banque Populaire Provençale et Corse.

■ Pouvez-vous me présenter vos fonctions au sein de la Banque Populaire Provençale et Corse ?

Le secteur d'activité bancaire et financier est astreint à un important niveau de sécurité des systèmes d'Information. Ma fonction en tant que Responsable de la Sécurité des Systèmes d'Information (RSSI) consiste essentiellement à veiller à la bonne application des règles de sécurité liées au système d'Information de notre entreprise. Le RSSI assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte.

■ En quelques grandes lignes, comment qualifieriez-vous la politique de sécurisation des systèmes d'Information du Groupe Banque Populaire ?

Je dirais qu'elle est à la fois réaliste, soutenable et adaptée aux enjeux. Elle est réaliste parce qu'elle est le fruit d'un travail collectif entre la filière Sécurité des Systèmes d'Information et les opérationnels de l'informatique. Elle est soutenable et adaptée aux enjeux parce qu'elle est entièrement fondée sur une approche par les risques et qu'elle fait l'objet d'une révision régulière.

■ Cryptogramme dynamique, machine learning, authentification par biométrie vocale… Aujourd'hui, le milieu bancaire rivalise d'innovation pour contrer des hackers toujours plus ingénieux. Quel serait le « plus » du Groupe Banque Populaire pour faire face à ces risques multiples ?

Avant toute chose, il me semble nécessaire de préciser que le terme hacker désigne originellement la personne qui analyse, décortique, découpe un système informatique pour en comprendre le fonctionnement et en découvrir les éventuelles vulnérabilités, et pas nécessairement d'ailleurs à des fins malveillantes. Quoi qu'il en soit, le hacker est donc avant tout un technicien qui va chercher à exploiter ses compétences pour mener des opérations frauduleuses sur un système d'Information.

Pour importante qu'elle soit, ce n'est que l'une des menaces auxquelles sont confrontées les banques et leurs clients particuliers ou entreprises : phishing, ingénierie sociale, etc. C'est pourquoi, il convient plutôt de parler de lutte contre les fraudeurs que de lutte contre les seuls hackers. Dans ce contexte, les dispositifs techniques tels que ceux que vous évoquez et qui sont effectivement en cours d'expérimentation dans le Groupe, ne sont qu'un élément de la réponse. Ils doivent nécessairement être complétés par des moyens de détection des fraudes ou des tentatives de fraudes en amont et en aval. Ils doivent aussi s'accompagner d'actions récurrentes de sensibilisation et de rappel des bonnes pratiques auprès de nos collaborateurs et surtout auprès de nos clients. C'est sur l'ensemble de ces axes que travaille le Groupe.

■ En tant qu'Opérateur d'Importance Vitale (OIV), les banques devront mettre en place au 1er juillet prochain des dispositifs de sécurité informatique renforcées. Que pensez-vous de cette nouvelle mesure ?

Il ne s'agit pas à proprement parler de nouvelles mesures mais plutôt du renforcement ou de l'extension de mesures déjà existantes. Le monde bancaire est un des domaines d'activité les plus matures en termes de sécurité. Cette précision étant faite, je pense que cette disposition témoigne de la prise en compte tant au niveau européen qu'au niveau national de la réalité et de l'importance de la menace cyber quelle qu'en soit l'origine. Elle traduit la volonté des autorités de définir un cadre homogène et cohérent applicable à l'ensemble des Opérateurs d'Importance Vitale (OIV) pour se prémunir de cette menace et réagir en cas de détection d'événements. Elle fait totalement écho au renforcement des moyens de l'Etat en matière de prévention et de lutte contre la cybercriminalité.

■ L'arrivée des services bancaires en ligne a changé la donne et a bouleversé la nature de la relation bancaire. Selon vous, l'augmentation des attaques cyber contre les banques est-elle en partie due à la transformation digitale qu'elles sont en train de vivre ?

Là aussi il convient d'appréhender le problème dans sa globalité et plutôt que d'attaques cyber ciblant les seules banques, il convient plutôt de parler de menaces cyber. Et effectivement, le phénomène est lié assez directement à la digitalisation de l'économie en général et même plus globalement à ce que j'appellerais la numérisation de la vie sociale. Les réseaux sociaux sont une mine inépuisable d'informations pour les fraudeurs. Par ailleurs, la presse se fait très régulièrement l'écho de vols parfois massifs de données personnelles incluant souvent des identifiants et des mots de passe. Les auteurs de ces vols ne sont pas simplement à la recherche de l'exploit et n'utilisent pas forcément eux–mêmes ces données mais les mettent en vente notamment sur ce que l'on appelle le dark web. A côté de l'économie numérique « légale » se développe une économie parallèle tout aussi numérique mais frauduleuse avec ses propres règles, ses propres services, ses places de marché, etc. Cependant, même si la menace ne doit être ni négligée, ni minimisée, il reste néanmoins possible de réduire son exposition et les conséquences en adoptant au quotidien quelques bonnes pratiques comme par exemple ne pas utiliser un même mot de passe pour plusieurs services sur Internet ou ne jamais communiquer sur Internet des données bancaires (n° de carte, code de connexion à la banque en ligne) sur une simple sollicitation par email fût-elle apparemment émise par sa banque. ■

Les réponses ont été apportées en collaboration avec la filière SSI Groupe

BANQUE POPULAIRE PROVENÇALE ET CORSE

Visitez leur site Internet et contactez les sur :

www.provencecorse.banquepopulaire.fr

« A côté de l'économie numérique « légale » se développe une économie parallèle tout aussi numérique mais frauduleuse avec ses propres règles, ses propres services, ses places de marché… »

SÉCURITÉ DES SYSTÈMES D'INFORMATION DANS LE DOMAINE MEDICAL

Philippe TOURRON | Responsable de la sécurité des systèmes d'Information – à la Direction des Services Numériques au sein de l'Assistance Publique Hôpitaux de Marseille (AP-HM).

■ Pouvez-vous nous éclairer sur les missions d'un RSSI dans un complexe médical comme l'AP-HM ?

Dans le contexte de l'AP-HM, le rôle du RSSI est avant tout d'être un lien entre les professionnels de santé (leurs besoins et leurs contraintes) et la sécurité du système d'Information pour éclairer les prises de décision que ce soit au niveau de la Direction Générale ou au niveau de la Direction informatique. Son rôle consiste à identifier, évaluer et gérer les risques. Que risque-t-on à mettre une application en ligne pour nos patients ou nos professionnels de santé ? Quelle est la probabilité de survenance du risque et quel est l'impact de ce risque potentiel ? Face à cela, l'idée est de proposer des mesures de sécurité en cohérence avec des solutions répondant aux besoins.

Le rôle du RSSI demeure dans l'analyse et le conseil afin de prendre les bonnes décisions et d'éviter de prendre des risques. Et, dans le cas, où nous devrions en prendre, de le faire en connaissance de cause et de les limiter à un niveau acceptable. Le management des risques est donc le cœur de son activité dans un contexte où, les réglementations se durcissent et la technologie et les usages évoluent sans cesse.

L'AP-HM est le centre hospitalier le plus important en région PACA. En quelques chiffres, c'est :

4 hôpitaux et 3 500 lits

environ 15 000 salariés dont 3 000 médecins

8 500 postes de travail et une centaine de collaborateurs au service informatique.

■ En 2015, on a vu le nombre d'attaques au rançonnage exploser dans les hôpitaux. Selon vous, qu'est ce qui explique que les hôpitaux soient aujourd'hui devenus une cible privilégiée des pirates ?

Il est vrai qu'il y a encore deux ans, les hôpitaux n'étaient pas les cibles premières des attaques. Nous étions plutôt des victimes collatérales. Cela a changé aujourd'hui. Il y a deux raisons selon moi. La première raison est que la donnée de santé représente une valeur qui attire les personnes malveillantes. Elle vaut désormais beaucoup plus cher qu'une donnée bancaire sur les marchés parallèles de revente d'informations. La seconde raison est que la donnée de santé peut être à l'origine d'un chantage à deux niveaux différents. Un cybercriminel peut menacer l'hôpital de diffuser des informations comme il peut le menacer de paralyser le système et donc d'empêcher la structure d'utiliser les données des patients. Dès lors, il peut aussi priver le patient de ses soins. Aujourd'hui, les données médicales sont des informations propices aux chantages.

■ Tous les acteurs de santé ne sont pas de taille identique et ne disposent pas des mêmes moyens pour analyser les risques et mettre en place des moyens adaptés. Pensez-vous que cela joue sur l'augmentation du nombre d'attaques cyber envers le milieu de la santé ?

Plus la structure est petite, plus il y a une surface de risque importante. Moins ces structures sont préparées, plus elles vont être des cibles. Dans le cas du chantage, pour reprendre cet exemple, il y a deux mesures principales à mettre en place. Ce sont deux remparts indispensables à toute structure hospitalière. La première mesure de protection réside dans la mise en place d'actions de communication, de sensibilisation et de formation afin de permettre de bons réflexes d'utilisateurs. La seconde mesure est une mesure de protection par le biais d'un plan de sauvegarde et de reprise ou continuité d'activité qui nécessite souvent une infrastructure technique importante.

Un établissement de taille moins importante peut donc avoir plus de mal à mettre ces mesures en place par rapport à un établissement plus structuré où, la sécurité est présente à tous les étages de l'organisation.

■ Mise à part ce risque, y-a-t-il d'autres risques cyber qui vous préoccupent ?

Les risques sont malheureusement nombreux. Nous avons plus ou moins de parades pour les limiter. Néanmoins, je dirais que la préoccupation principale des établissements de santé aujourd'hui repose sur le couplage de la notion de disponibilité et de confidentialité des données. Dans le domaine de l'information informatisée, c'est une prise de conscience assez récente. Auparavant, il y a encore cinq ans, la disponibilité des données était privilégiée. Tout était mis en œuvre pour que la donnée soit disponible facilement et immédiatement. C'est toute la complexité du monde hospitalier : concilier cette disponibilité de la donnée avec la nécessité de confidentialité. A l'heure actuelle, le monde hospitalier est en train de rééquilibrer cette balance « disponibilité – confidentialité » pour gérer notamment des habilitations adaptées aux métiers de chacun. Il y a un effort important mené sur cette question en cohérence avec la CNIL, et les établissements de santé s'attachent de plus en plus à nommer des CIL (Correspondant Informatique et Libertés).

Pour notre cas, je travaille régulièrement depuis 5 ans en binôme avec un correspondant CNIL, médecin de profession, pour trouver des moyens techniques et des manières de faire qui permettent le respect et le maintien de cet équilibre. A mon sens, il est très important que ce soit une personne du métier pour bien comprendre cet équilibre complexe à trouver. C'est toute la spécificité de notre environnement que de réussir ce mariage-là.

ANSWER, un partenaire du SECEM 2017

■ Vous parlez justement de votre relation avec la CNIL et son correspondant. De fait, face à l'importance de garantir la confidentialité et la protection des données de santé, comment sécurisez-vous ce patrimoine informationnel que l'on vous confie chaque jour ?

Par la mise en œuvre de tous les composants techniques de sécurité classiques (Pare-feu, anti-virus, détections et filtres divers de menaces et intrusion, …) mais, au-delà de ces fondamentaux, par l'amélioration des pratiques des utilisateurs. Nous avons redéployé plusieurs éléments de notre politique de sécurité des systèmes d'Information ; en particulier, une charte utilisateur vient d'être remaniée et intégrée à notre stratégie sécuritaire. C'est une mesure écrite indispensable puisqu'elle indique les droits et les devoirs de chacun vis-à-vis de l'information. Une politique d'habilitation vient compléter les règles concernant les droits d'accès aux données.

Au niveau national, nous disposons aussi d'une politique de sécurité transmise par le Ministère de la Santé. Nous la déclinons au niveau de notre établissement. Cela nous amène à régler toutes les manières de faire dans les différentes phases de vie du système d'Information (achat – installation – exploitation – gestion des incidents– arrêt). Je dirais néanmoins que la force d'une politique de cybersécurité vient de ceux qui l'appliquent. Nous pouvons avoir de nombreux documents bien écrits avec de belles intentions. Il faut tout de même qu'elles soient applicables et appliquées. La condition de réussite d'une politique de cybersécurité demeure la force et la rigueur des acteurs qui sont amenés à la déployer mais aussi à la respecter.

■ Et pour cela, comment travaillez-vous avec l'ASIP Santé ?

Nous travaillons avec l'ASIP Santé à deux niveaux complémentaires : l'un méthodologique avec l'élaboration de la Politique de sécurité ; l'autre plus opérationnel. ASIP Santé nous accompagne et nous propose des solutions techniques pour amener de la sécurité dans nos établissements. La première brique technique demeure la « Carte de Professionnel de Santé » (CPS) mise en place et intégrée dans notre architecture technique depuis 2012 sur des périmètres critiques. C'est une carte à puce qui permet l'authentification et la signature des professionnels de santé. Elle est accompagnée par la « Carte de Professionnel d'Etablissement » qui est le versant pour le personnel non médical. La seconde brique est la mise en place de la « Messagerie Sécurisée de Santé ». C'est un outil incontournable de la dématérialisation pour permettre un échange sécurisé notamment avec la médecine de ville et l'ensemble des acteurs partenaires de l'établissement. La troisième et dernière brique est la signature numérique, l'ASIP Santé fournit un certificat de signature embarqué dans la CPS, qui a pour but de prouver la garantie de la provenance, l'authentification du document, de son signataire et de son intégrité. La signature numérique est un gage de confiance. Et, vous savez tout comme moi, combien la confiance est importante dans la relation numérique.

Toutes ces briques intégrées à notre système d'Information et notre architecture informatique permettent petit à petit d'aller vers la dématérialisation des données de santé tout en les protégeant.

■ Je vais justement rebondir sur cette notion de confiance dont vous me parlez. En interne, vis-à-vis de vos collaborateurs, quel niveau placez-vous votre démarche de sensibilisation et de formation du personnel aux bonnes pratiques de sécurité informatique ?

Depuis plus de trois ans, nous avons entrepris une démarche de communication sur la sécurité avec plusieurs composantes. Le but est de permettre aux acteurs du monde de la santé de s'exprimer quand ils ont un doute au travers d'une hotline et d'une boite aux lettres qui leur sont réservées. Ils peuvent rediriger tout message douteux afin que le personnel du service informatique essaie d'adapter le filtrage pour voir si un message malveillant a déjà agi sur un poste. Cette démarche de communication et ce système de réaction en chaine sont donc en place depuis plusieurs années.

En matière de formation, nous devons prendre en charge plus de 15 000 salariés. Nous avons donc réfléchi à la manière d'arriver à former l'ensemble des collaborateurs sur ces questions de sécurité. Il aurait été impossible de les réunir ou les rassembler en petit groupe. Nous avons donc mis au point un outil de e-learning dédié à la sensibilisation et à la formation aux questions de sécurité. J'ai eu la chance de piloter ce projet avec une équipe de collègues RSSI hospitaliers et soignants afin de réaliser un outil de plateforme de contenus adaptés aux professionnels de santé. Conçu il y a deux ans, cette plateforme contient une cinquantaine d'activités sous différentes formes qui vont permettre d'expérimenter les bonnes pratiques dans les différentes phases de l'usage de l'informatique et de l'information au sein de l'hôpital. L'objectif est de familiariser les collaborateurs aux bonnes pratiques en mettant en scène avec pragmatisme les problématiques qui peuvent se poser tous les jours sans les sanctionner et dans la bonne humeur.

Nous souhaitons faire comprendre à nos collaborateurs que l'informatique à l'hôpital, ce n'est pas comme à la maison. C'est volontairement équivoque puisque, nous sommes autant susceptibles d'avoir des virus chez soi que sur son lieu de travail. Or, la grande différence, ce sont les conséquences et les impacts. La propagation d'un virus informatique dans le système d'Information de l'hôpital, c'est par exemple priver un patient d'un examen au scanner dont, il aurait pourtant eu besoin au plus vite ou perdre une partie de ses données par cryptage.

■ « L'informatique à l'hôpital, ce n'est pas comme à la maison ». Par rapport à cela, pensez-vous que le phénomène de « Bring Your Own Device » (BYOD) puisse devenir un risque particulièrement dangereux et coûteux pour le secteur médical à long terme ?

Pour moi, le BYOD est un risque inéluctable. Phénomène nouveau issu de l'évolution des usages, nous pouvons difficilement aller contre. A mon sens, mieux vaut utiliser la force de l'autre pour essayer de gagner le combat. C'est le rôle même du RSSI que d'être capable d'identifier les risques potentiels du BYOD et, pour certains usages, de les encadrer avec des moyens techniques. Techniquement, nous savons le faire. Nous pouvons aujourd'hui sur un matériel personnel exécuter une application dans un mode conteneur ou protégé afin de s'assurer que la donnée est sure et qu'elle ne va pas fuiter. Les outils existent sur le marché pour permettre de gérer cette question. Par contre, le BYOD reste encore expérimental sur certains aspects. Des questions restent à résoudre, notamment, la responsabilité juridique en cas d'incident. Est-ce la responsabilité de l'établissement qui est engagée ? Ou est-ce la responsabilité du propriétaire de l'outil personnel utilisé ? Assimile-t-on cela à du télétravail ? Une réflexion est d'ores et déjà en cours dans le cadre de groupements d'hôpitaux pour statuer sur les dispositifs à mettre en œuvre. Je pense que le BYOD doit être encadré techniquement et juridiquement pour éviter d'être un risque dangereux et coûteux à long terme.

■ Pour conclure, quels sont vos grands chantiers à venir au sein de vos missions de RSSI de l'AP-HM ?

La mobilité au sens large, avec la dématérialisation mais aussi les objets de santé connectés qui sont en pleine expérimentation et évolution aujourd'hui ; nous utilisons déjà des dispositifs médicaux de ce type. Dans ce contexte d'ouverture du système d'Information hospitalier nous avons besoin d'une rigueur d'autant plus importante ce qui nous a conduit à suivre une démarche de certification ISO 27001 (de management de la sécurité) s'appuyant sur une certification ISO 9001 déjà obtenue et sur nos agréments d'hébergement de données de santé.

Par ailleurs, le défi ou chantier permanent qui fait la spécificité des établissements de santé est la diversité des applications et des éditeurs d'applications. Plus il y a une diversité importante, plus le niveau de sécurité des applications est hétérogène. La protection, la confidentialité, les habilitations, la sécurité dans le développement sont de réels enjeux. Nous avons un parc applicatif de plusieurs centaines d'applications différentes aux éditeurs très nombreux. Cela amène donc un effort considérable à entreprendre au niveau des éditeurs pour obtenir un socle minimal en termes de sécurité et de confidentialité dans les applications. C'est un enjeu extrêmement important pour l'avenir qui pourra peut-être là aussi passer par un label sécurité des logiciels. ■

Visitez leur site Internet et contactez les sur :

www.fr.ap-hm.fr

« La préoccupation principale des établissements de santé aujourd'hui repose sur le couplage de la notion de disponibilité et de confidentialité des données »

LE RENSEIGNEMENT PRÉDICTIF, TECHNOLOGIE AU POTENTIEL DE DISRUPTION MAJEUR

Jean-Paul PINTE | Docteur en Sciences de l'Information et de la Communication - Maître de conférences – Université Catholique de Lille et cybercriminologue.

Dans le cadre de l'étude Technologies-Clés 2020[1], mandatée par le Ministère de l'Economie, de l'Industrie et du Numérique ont été identifiés quatre technologies clés au potentiel de disruption majeur : nanoélectronique, Internet des objets, technologies de valorisation des données massives et infrastructures de 5ème génération. En effet, les technologies de valorisation des données massives, leur maîtrise et leur collecte représentent aujourd'hui un enjeu majeur du XXIème siècle. Les données personnelles ont une valeur économique. Les détenir et être capable de les analyser est devenu un critère de puissance mondiale à l'heure d'une société menacée par la cybercriminalité et le (cyber)terrorisme.

Je veux parler ici de disruption car, il y a comme une cassure, une brisure qui fait que nos systèmes sociaux arrivent toujours trop tard pour s'emparer des évolutions technologiques. Tout va de plus en plus vite. Dans le domaine de la physique nucléaire, de la magnétohydrodynamique et de la physique des plasmas, on appelle depuis longtemps disruption comme « *l'apparition brutale d'instabilités magnétohydrodynamiques dans la chambre de confinement* ». Il semblerait que ce soit le cas en ce qui concerne le renseignement où, à chaque fois qu'il se passe de nouveaux évènements qu'ils soient criminels, terroristes ou autres on remet toujours en cause les méthodes utilisées et leur décalage avec la réalité. Il faut dire aussi que les modes opératoires de ces (cyber)criminels évoluent au fur et à mesure qu'on les renseigne sur la façon dont, ils sont surveillés !

Le Web 2.0 et le Web 3.0 quasiment inexplorés et pourtant…

Il est utile de le rappeler qu'Internet a d'abord été un outil permettant la lecture de contenus (Web 1.0). Il a migré ensuite vers une capacité d'y ajouter soit même des contenus en tant qu'utilisateur donc permettant la bidirectionnalité des échanges (Web 2.0). Puis, est venu l'ère du web aux contenus intelligents, un web capable de comprendre les contenus et de réagir en conséquence (Web 3.0). C'est déjà l'Internet des objets connectés qui se profile (Web 4.0) sans parler de l'intelligence artificielle qui commence à pointer son nez dans beaucoup de domaines (Web 5.0).

[1] *http://www.entreprises.gouv.fr/politique-et-enjeux/technologies-cles-2020*

Voilà où nous nous sommes rendus. Tout cela sans qu'une grande partie des internautes, des entreprises et des services de renseignement n'aient pu en mesurer réellement les potentialités de fouilles ni, la profondeur des recherches possibles dans le cyberspace. Et ce, dans tous les domaines de notre société. Le cyberespace exige aujourd'hui pour nos services de renseignement une nouvelle forme d'intelligence « dite de la donnée » avec, en même temps une certaine intuition dans le discernement des données collectées.

Tout se passe aujourd'hui comme si l'on s'adaptait aux évènements et nouveaux modes opératoires des acteurs de la cybercriminalité pour cyber-investiguer sur le Net sans précéder réellement l'évènement. Plus de 300 sites-outils permettent aujourd'hui de mener une veille sur la toile pour y trouver par tâtonnement et par le biais d'ontologies [2] des signaux faibles comme des interactions possibles avec des évènements ou encore des inter-relations avec des concepts. Le tout est de mener cette cyber quête dès qu'il y a des indices et bien avant que l'ADN numérique de la personne ou du sujet ne soit pollué par les internautes eux-mêmes.

Des algorithmes qui nous gouvernent, chiffrent et prédisent le monde.

La masse d'outils de surveillance évoquée ci-dessus fonctionne à partir de gros calculateurs et d'algorithmes qui correspondent à des séries d'instruction permettant d'obtenir un résultat à partir de masses de données (Big Data) ou de nos métadonnées. Bien manipulés, ces algorithmes sont de puissantes entités, qui contrôlent, gouvernent, trient, réglementent et façonnent toute notre société. A partir de ces derniers, on peut établir aujourd'hui la réputation d'une personne ou d'une société. En scrutant plus loin encore, on peut aussi prédire par les traces via la technologie du machine learning. CookieViz (développé par la CNIL) en est un bon exemple. Il permet de visualiser les données de l'utilisateur lorsque, croyant se connecter à son site préféré, l'internaute ne fait qu'envoyer en réalité des informations à des sites plus ou moins obscurs dans le monde. Il y a donc de quoi innover pour nos services de renseignement avec ces méthodes surtout quand, on sait que les algorithmes vont aussi scruter nos applications et les objets connectés que nous ne manquerons pas de porter ou de véhiculer sans en prendre réellement conscience. On peut citer ici à titre d'exemple le réseau maillé MESH. Il correspond à un ensemble d'appareils communicants reliés entre eux de manière distribuée sans fil, ni hiérarchie centrale.

De l'urgence de revoir en général le renseignement en France.

En ce qui concerne les entreprises, l'agence européenne pour la sécurité de l'information et des réseaux (ENISA)[3] soulignait encore, début janvier, dans son rapport sur l'année 2015, l'importance du renseignement sur les menaces pour améliorer les postures de sécurité. Ainsi, 91% des professionnels interrogés voudraient recevoir des renseignements sur les menaces. Or, ils ne sont que 63% à être prêts à en partager. Et encore, sous condition, ils ne le feraient que via un système privé et sécurisé. Près d'un quart des personnes interrogées reconnaissent leur méconnaissance du sujet et 21% craignent que les informations partagées ne soient susceptibles de permettre d'identifier leur organisation.

Pour le terrorisme aux termes de six mois de travail, la Commission d'enquête parlementaire sur l'action de l'Etat face aux attentats de janvier et novembre 2015 a rendu son rapport le mardi 5 juillet 2016. Ce document de 300 pages se nourrit notamment des auditions de quatre Ministres et des Directeurs des services de renseignement. Cet important travail de synthèse aboutit à 39 propositions. Le rapporteur de la Commission, le Député parti socialiste Sébastien PIETRASANTA et son Président, le Député LR Georges FENECH signalent tout deux que « *nous sommes sur des schémas qui datent des années 1980, à une époque où, le terrorisme n'était pas ce qu'il est aujourd'hui. Il faut une ambition bien plus importante pour rationaliser notre renseignement et le coordonner véritablement au niveau européen* » tout en signalant un criant manque de coordination. Le rapporteur propose donc la création d'une Direction générale du renseignement territorial, placée auprès du Ministre de l'Intérieur et intégrée au premier cercle de la communauté du renseignement. Tout ceci est en vue d'améliorer la détection « des signaux faibles ». Sébastien PIETRASANTA, quant à lui, suggère ainsi de redynamiser le renseignement de proximité.

Un espoir qui viendrait de l'Europe et d'une loi sur une République numérique.

L'Union Européenne s'attaque sérieusement à la cybercriminalité. Les entreprises européennes sont systématiquement gênées par la criminalité informatique. Pour lutter contre ce phénomène, la Commission européenne conclut un partenariat public / privé avec des pouvoirs publics et des entreprises. Cette collaboration prévoit d'investir 1,8 milliard d'euros dans la cybersécurité d'ici 2020. De son côté, l'OTAN lors de son dernier sommet, qui s'est déroulé les 8 et 9 juillet à Varsovie, a confirmé plusieurs décisions dont, celle de se doter d'une unité dédiée au partage de renseignements entre les Alliés. Mais, l'espoir ne viendrait-il pas de la loi pour une République numérique. Son texte final devrait être promulgué au début du mois d'octobre 2016. La fouille de textes et de données (text data mining) pour les scientifiques et les chercheurs y est envisagée. Cela serait un bon point pour relancer la veille stratégique dans tous les domaines de la société. En effet, la donnée n'est pas donnée[4] et il faudra de plus en plus apprendre à la chercher. ■

[2] *Modèle de données représentatif d'un ensemble de concepts dans un domaine, ainsi que des relations entre ces concepts.*

[3] *https://www.enisa.europa.eu*

[4] *http://www.editions-kawa.com/home/157-la-donnee-n-est-pas-donnee-strategie-big-data.html*

CYBERSÉCURITÉ : ENTRE L'ESPACE NUMÉRIQUE ET L'ESPACE MARITIME

Capitaine de Frégate NICOLAS | Officier sécurité et systèmes d'information de la Marine Nationale.

Le CF Nicolas sert dans la Marine Nationale depuis près de 20 ans. Après avoir navigué sur tout type de navires comme chef de service SIC (Systèmes d'Information et de Communication) ou à des postes de commandement, il s'est spécialisé dans la cybersécurité. En plus d'être diplômé de l'École Navale et de l'École de Guerre, il détient un mastère en Réseaux de télécommunication et le titre d'expert SSI (Sécurité des Systèmes d'Information) de l'ANSSI (Agence Nationale de la SSI).

■ Pouvez-vous expliquer à nos lecteurs ce qu'est la « Marétique » dans le milieu maritime ?

Du latin « mare », la mer et du français « informatique », la « Marétique » est l'ensemble des systèmes informatiques et électroniques utilisés dans la gestion et l'automatisation des opérations relatives aux activités maritimes, fluviales et portuaires. Ce terme rend compte du croisement entre deux secteurs d'activité très porteurs : le maritime et le numérique.

■ Quelles sont les forces et les faiblesses de la Marétique en matière de cybersécurité ?

La marétique s'est construit très vite avec des objectifs de rentabilité très forts à une époque où, le risque cyber n'était pas encore ancré dans les consciences. Il y a donc un existant qui n'est pas toujours sécurisé à la hauteur des menaces actuelles. C'est en 2010 que tout a basculé avec la révélation de l'attaque Stuxnet. Cette attaque ciblait des automates industriels et notamment leurs systèmes de contrôle et de commande qui servaient à piloter des centrifugeuses utilisées pour enrichir de l'uranium à Natanz, en Iran. Cette attaque informatique a permis d'endommager des centaines de centrifugeuses au prix très élevé, avec pour conséquence un retard dans le programme nucléaire iranien. La Marétique repose en grande partie sur des automates similaires à ceux qui se trouvaient à Natanz. C'est la raison pour laquelle, le milieu maritime regarde les capacités offensives des cyberpirates d'un autre œil depuis cette date. Malheureusement, le coût des infrastructures existantes ne permet pas toujours de les remplacer rapidement. Il y a donc un existant qui n'est pas toujours sécurisé à la hauteur des menaces actuelles.

Cependant, le secteur maritime est très agile pour se mobiliser très vite et pour faire évoluer la situation grâce à des associations professionnelles comme le Cluster Maritime Français (CMF) ou à des organisations internationales comme l'Organisation Maritime Internationale (OMI). On peut aussi s'appuyer sur une des grandes forces de la Marétique : son orientation très marquée résultat. Si le besoin opérationnel est d'avoir plus de cybersécurité, les entreprises maritimes et informatiques qui contribuent à construire chaque jour la Marétique ont une capacité d'adaptation suffisante pour y répondre.

■ On se souvient tous du film américain « Speed 2 » dans lequel un terroriste prenait le contrôle d'un paquebot de croisière par le piratage de son système informatique. Est-ce un scénario possible dans la réalité à l'heure actuelle ?

Le déroulement du scénario exactement comme dans le film peut paraître incroyable. Pourtant, il peut exister des interconnexions entre des réseaux servant à la propulsion et à la barre du navire et d'autres réseaux dédiés aux loisirs ou à l'Internet. Ce type de configuration ne se trouve heureusement pas sur tous les navires et il appartient à chaque armateur de faire auditer la sécurité de ses systèmes d'Information embarqués. On va d'ailleurs vers une sanctuarisation des systèmes d'Information dédiés à la propulsion et à la barre, en interdisant ou en limitant l'interconnexion des réseaux. Idéalement, il faudrait que physiquement, il n'existe aucun lien informatique entre les moteurs, la barre et le reste des réseaux (réseaux de messagerie, liens avec la terre, Internet à des fins professionnelles ou de détente de l'équipage ou des passagers). Cependant, lorsque un lien doit subsister, notamment pour la supervision à distance ou la télémaintenance des moteurs, il est nécessaire d'utiliser des outils de sécurité comme des pare-feux (firewall dans le jargon) et des sondes de sécurité (IDS) pour n'autoriser que les flux numériques légitimes et détecter les tentatives d'attaque.

■ Quelle sont les initiatives émergentes et les solutions innovantes qui apparaissent actuellement pour lutter contre ces menaces de plus en plus fortes ?

La prise de conscience dans le secteur s'accélère, notamment grâce à des initiatives comme les rencontres parlementaires sur la cybersécurité dans le monde maritime ou les ateliers cyber du Cluster Maritime Français. Au-delà de la sensibilisation, on va vers la mise en place de véritables formations sur le risque cyber au profit des acteurs du monde maritime. Les constructeurs ont également un rôle majeur à jouer en proposant des navires et des infrastructures portuaires associées étant cybersécurisés « by design ». En effet, il est pertinent d'investir sur la cybersécurité dès la conception car, il est très coûteux de sécuriser un système a posteriori.

Pour la Marine, la cyberdéfense est un domaine de lutte à part entière, rattachée aux opérations. Elle se prépare en permanence pour anticiper et si besoin déjouer des cyberattaques. En 2015, une chaire industrielle de cyberdéfense navale a été créée par la Marine Nationale car, la recherche a un rôle fondamental en la matière. Par ailleurs, les assureurs commencent à considérer le risque cyber et pourraient avoir très prochainement des exigences sur la mise en place d'outils de protection pour couvrir ce risque. Enfin, la France et plusieurs pays de l'Union Européenne ont déposé une soumission à l'Organisation Maritime Internationale (OMI) visant à accentuer la prise en compte de la cybersécurité par la flotte mondiale.

■ La cybersécurité maritime, est-ce pour vous l'un des enjeux majeurs pour les années à venir ?

Assurément. De la même manière qu'au vingtième siècle, on a énormément investi pour protéger les navires contre le risque de naufrage (compartimentage, détecteurs de voie d'eau…) ou d'incendie (détecteurs, moyens d'extinction fixes et mobiles puissants…), le vingt et unième siècle va connaître une course à la sécurisation des systèmes d'Information maritimes. ■

www.defense.gouv.fr/marine

« Les assureurs commencent à considérer le risque cyber et pourraient avoir très prochainement des exigences sur la mise en place d'outils de protection pour couvrir ce risque »

LES SYSTÈMES CONNECTÉS ET EMBARQUÉS DANS LE TRANSPORT MARITIME, UN RISQUE EN MATIÈRE DE CYBERCRIMINALITÉ ?

Frédéric MONCANY DE SAINT-AIGNAN | Président du CLUSTER Maritime Français.

■ Quel est le rôle du Cluster Maritime Français actuellement dans la prise de conscience du cyber risque dans le milieu maritime ?

Le Cluster Maritime Français compte au sein de ses adhérents des leaders de la cybersécurité, d'une part et d'autre part des entreprises qui comme n'importe quel acteur du monde économique sont vulnérables aux attaques informatiques. Alerté par ses membres, le CMF a décidé dans un premier temps d'envoyer un de ses chargés de mission au sein d'une formation de haut niveau au Centre des Hautes Etudes du Cyberespace (www.checy.org), puis de préparer une série d'ateliers de sensibilisation à la cybersécurité maritime pour ses adhérents.

■ Pour représenter un peu ce risque à nos lecteurs, quelles menaces cyber rôdent autour des entreprises du secteur maritime ?

Déjà, les mêmes menaces qui pèsent sur des entreprises dont, les sièges sociaux sont basés à terre : vol de données, ransomware, déstabilisation des systèmes d'exploitation et des automates, espionnage industriel. Mais en mer, les risques sont plus élevés car, les navires sont des systèmes industriels complexes, possédant des SCADA qui automatisent la conduite de la propulsion, de la direction (gouvernail), des systèmes d'alarmes, des commandes et contrôles de divers systèmes dont électrique, gestion du carburant, etc. Ces outils informatiques et automates sont de plus en plus standardisés et surtout interconnectés, et donc soumis aux mêmes vulnérabilités que les systèmes déployés à terre dans des environnements industriels. La prise de contrôle à distance d'un système vital pour le navire est un véritable risque. Enfin, les ports et entreprises de la logistique maritime sont également des cibles potentielles des cyberattaques. Des faits récents montrent que le suivi de la marchandise transportée par voie maritime intéressent les malfaiteurs.

■ Certains jugent le niveau de cybersécurité « faible voire inexistant ». Etes-vous d'accord ou bien est-ce en réalité un jugement trop sévère ?

Ce constat a été particulièrement fait dans le rapport de l'ENISA (European Union Agency for Network and Information Security) en décembre 2011. Même si le secteur maritime reste très en retard en matière de cybersécurité, de nombreuses initiatives sont mises en place : création d'une chaire cyberdéfense à l'Ecole Navale, sensibilisation des navigants à l'hygiène informatique et à comment réagir en cas d'attaques, réflexions menées à l'Organisation Maritime Internationale (OMI)

En quelques chiffres, le secteur maritime, c'est plus de 90% des marchandises sont transportées par voie maritime, 300 000 emplois directs et 70 Milliards d'euros de valeur de production.

Cluster Maritime Français
Le Faire-Savoir Maritime
The Maritime Voice

Le Cluster Maritime Français (CMF) est une organisation créée en 2006 par et pour les professionnels du secteur maritime afin de rassembler tous les acteurs de l'économie maritime.

De l'industrie aux services, elle est composée de plus de 410 membres : entreprises de toutes tailles, pôles de compétitivité, fédérations et associations, laboratoires et centres de recherche, écoles et organismes de formation, collectivités et acteurs économiques locaux, ainsi que de la Marine Nationale.

www.cluster-maritime.fr

pour une nouvelle normalisation, mise en place d'unités « cyber » dans les grandes entreprises. Les mentalités sont en train d'évoluer !

■ Vous avez formé des groupes de travail et des ateliers à ce sujet. Vous avez également participé à un groupe parlementaire sur le sujet. Pouvez-vous m'en dire plus et l'objectif de telles initiatives ?

Le CMF a effectivement participé aux 2ème Rencontres Parlementaires « Cybersécurité et milieu maritime », organisées par le CyberCercle, aux côtés de partenaires comme le Groupement des Industries de la Construction et Activités Navales (GICAN), d'Armateurs de France, de DCNS et de l'ANSSI. Ces rencontres permettent de faire le point sur les problématiques de sécurité numérique auxquels, les acteurs du maritime sont aujourd'hui confrontés, d'échanger sur ces sujets et de rencontrer les acteurs de la filière cybersécurité, publics et privés, à même de les accompagner dans leurs démarches.

De son côté, le CMF a décidé de mettre en place une série d'ateliers de sensibilisation à la cybersécurité maritime, en faisant intervenir des experts de haut niveau à destination des représentants de nos membres, cadres opérationnels et supérieurs. Une première réunion a eu lieu en mai sur la cyberdéfense. La seconde s'est tenue mi-juin sur les risques économiques. Une autre réunion est programmée pour septembre où nous parlerons des SCADA.

■ Regrettez-vous l'absence réelle de mesures pour lutter contre cela autant au niveau national qu'européen ?

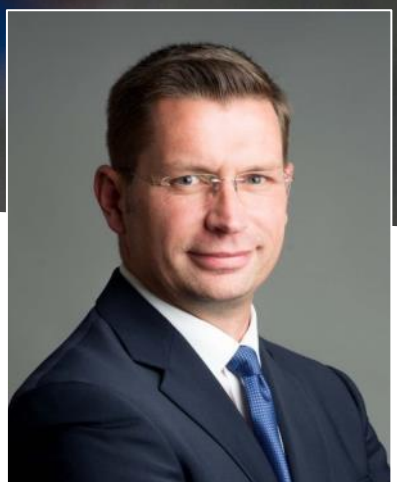
Au niveau national, au-delà des mesures mises en place par les entreprises elles-mêmes, tant au niveau de leur politique de cybersécurité qu'au niveau des modifications apportées à leurs systèmes informatiques, il faut saluer les travaux menés par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) pour sensibiliser les professionnels. Un guide de bonnes pratiques dans le secteur maritime devrait voir le jour prochainement. Au niveau européen, en dehors des travaux de l'ENISA déjà évoqués, on peut noter que l'ECSA (European Community Shipowners' Associations) a recadré les thèmes de son maritime Security Working Group qui couvrira aussi le champ de la cybersécurité. Cependant, malgré l'important travail fait par la délégation française auprès du l'OMI (Organisation Maritime Internationale) il faut être honnête, le chemin est encore long vers l'adoption de mesures très concrètes et de normes pour les opérateurs.

■ Peut-on dire que la cybersécurité maritime est en train de s'organiser et de s'imposer comme l'un des enjeux majeurs pour les années à venir ?

Les initiatives professionnelles se développent. On a parlé de la Chaire de Cyberdéfense de l'Ecole navale, des rencontres parlementaires, des groupes de travail des diverses organisations professionnelles. De toute façon, la cybersécurité et le cyberespace tout court sont des enjeux éminemment majeurs pour aujourd'hui comme pour demain ! Nous sommes au cœur de la transformation numérique du monde, et cela se passe à vitesse exponentielle.

Un dernier exemple : en janvier 2016 un groupement composé du Bimco, Clia, ICS, Intercargo et Intertanko (les principales organisations armatoriales mondiales) a publié un guide pour évaluer la menace d'attaques informatiques sur les systèmes des compagnies maritimes. Ce guide donne également des lignes directrices à suivre pour se prémunir contre les cyberattaques et pour y réagir. Parmi ces lignes, on peut noter la recommandation de développer une norme pour l'entretien et la mise à niveau de tout système électronique programmable. Ces recommandations seront portées auprès de l'OMI pour que bougent les lignes, c'est un bon début. ■

« Nous sommes au cœur de la transformation numérique du monde, et cela se passe à vitesse exponentielle »



SÉCURISATION DES POSTES DE TRAVAIL, UN ENJEU EN MATIÈRE DE CYBERSÉCURITÉ

Anthony HIE | Directeur des Systèmes d'Information et du Numérique au sein de l'Institut Catholique de Paris.

■ Quelles sont selon vous les règles élémentaires de sécurité pour un poste de travail en entreprise ?

La sensibilisation de nos collaborateurs vis-à-vis des risques et autres menaces potentielles me parait un prérequis indispensable voire prioritaire aujourd'hui. Un des points d'attention particulier pour nous est la messagerie électronique. En effet, face à la recrudescence du « phishing » et plus récemment des « ransomware », il est important que nos collaborateurs comprennent qu'il faut analyser le contenu et vérifier la provenance d'un email avant de cliquer dessus. En ce qui concerne la confidentialité, nous avons vraiment sensibilisé nos collaborateurs à verrouiller chacun de leurs postes de travail dans le cadre d'une absence prolongée avec un mot de passe qu'ils changent régulièrement. Ces bons réflexes viennent se mêler à l'installation de moyens techniques centralisés pour protéger l'ensemble du réseau et en cas de risque avéré, limiter la propagation.

■ Un poste de travail mal protégé peut donc mettre en péril non seulement les informations qui sont traitées sur le poste mais également les systèmes auxquels il se connecte. Plus précisément, quels risques cela peut-il prévenir ?

Les risques sont divers et variés. Ils peuvent être liés à l'intégrité des données. Ils peuvent entrainer une perte quasi-complète d'informations voire aussi une altération de l'information à travers les réseaux. Autre menace importante actuellement, ce sont ce que l'on appelle « Un Cheval de Troie ». Ce genre de menace offre la possibilité de récupérer à distance des informations stratégiques et confidentielles sur l'entreprise. Néanmoins, en termes de sécurisation des postes de travail, la démarche de protection est inévitablement liée au comportement que le collaborateur va tenir et appliquer sur son poste de travail et dans son utilisation quotidienne des outils informatiques et Internet.

■ Quel est selon vous la meilleure méthode pour parvenir à une implication et une mobilisation de tous aux bons gestes de sécurité informatique ?

Une Politique de Sécurité des Systèmes d'Information permet d'adapter le niveau de sécurité aux enjeux de l'organisation. Elle sera donc utilisée comme un outil de communication, d'action, de reporting et d'audit régulier pour sensibiliser les collaborateurs aux bonnes pratiques. A mon sens, il y a globalement trois messages concernant la cybersécurité à faire passer aux collaborateurs de l'entreprise. La première chose, c'est que la sécurité n'est pas l'unique responsabilité de la Direction des Systèmes d'Information (DSI). C'est l'ensemble de l'organisation qui doit être sensibilisée et mobilisée pour mieux appréhender les risques potentiels. La seconde chose importante c'est que la sécurité est souvent perçue par les collaborateurs comme une contrainte. Or, il est possible de transformer cette contrainte en véritable valeur ajoutée pour l'entreprise. Enfin, le dernier message que je tente chaque jour de faire passer, c'est que vouloir un système d'Information sécurisé à 100% n'est pas possible. C'est pourquoi, un suivi et un contrôle régulier de l'activité sur les postes de travail est nécessaire ainsi que des audits réguliers tout en prenant compte de l'ensemble des nouveaux risques liés au phénomène de digitalisation en entreprise. ■

Visitez leur site Internet et contactez les sur : www.icp.fr

CLOUD ET BIG DATA, DEUX PRÉOCCUPATIONS MAJEURES ET DEUX DÉFIS POUR LES DIRECTIONS DES SYSTÈMES D'INFORMATION

Jean-Claude BURTIN | Directeur de la Stratégie, de la Qualité, du Soutien et des Développements rapides - Direction des Systèmes d'Information chez ORANGE France.

Jean Claude BURTIN est en charge de la stratégie, de la qualité et du soutien du Système d'Information France.

Il est Centralien et Ingénieur des Mines et est entré en 1979 à France Télécom où, il a fait quasiment toute sa carrière.

Il a participé aux nombreux défis de l'entreprise : de l'équipement téléphonique de la France, l'arrivée du mobile, de l'internet. Il a alterné de nombreux postes de management opérationnels, plusieurs fois Directeur Régional et Territorial où, il a encadré jusqu'à 6500 salariés, avec des postes de Directeur de projets nationaux. Il a conduit au cours de ces 4 dernières années, le redressement de la qualité du système d'Information et a été en charge pendant 2 ans d'un crash programme d'amélioration de la sécurité des données clients à Orange France.

Il est actuellement en charge du déploiement de l'agilité, du devops, des API, du cloud et l'amélioration de l'efficacité de la DSI d'Orange France.

■ Comment qualifieriez-vous les trois axes de réussite de la transformation numérique du Groupe Orange ?

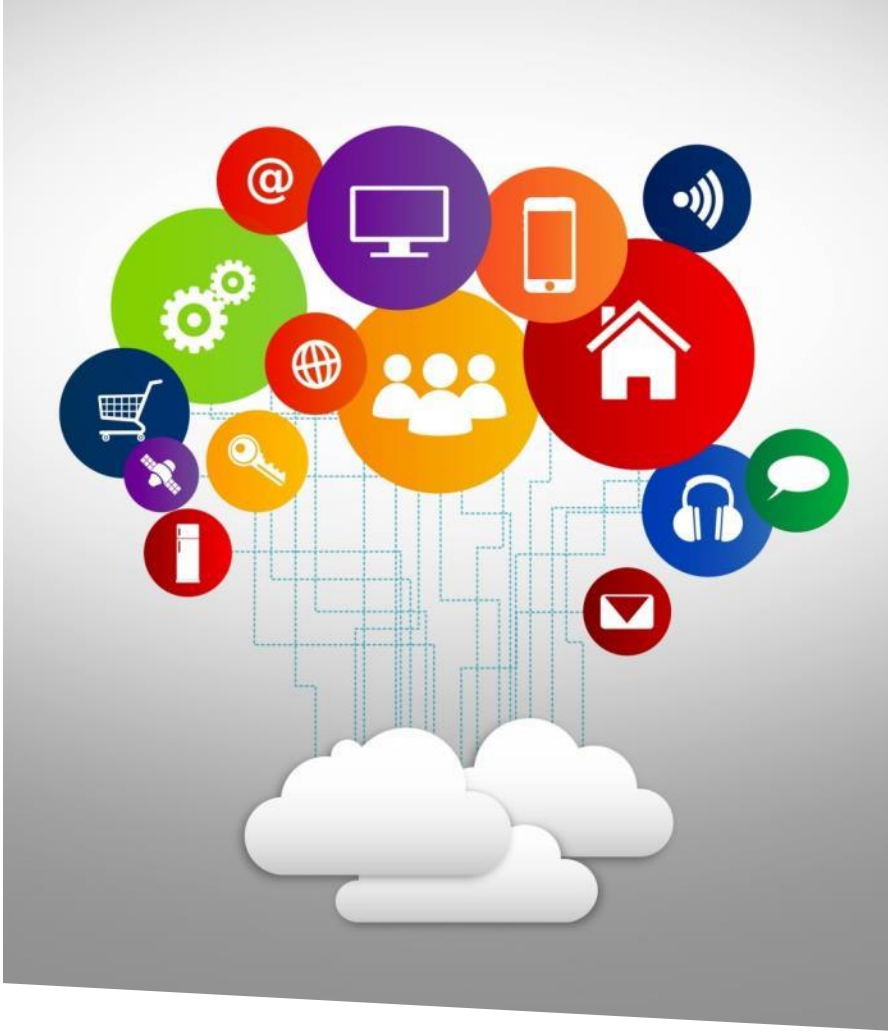
Dans le contexte de transformation digitale que nous vivons, le Groupe Orange a un rôle particulier puisqu'il accompagne ses clients-entreprises professionnels et particuliers, et poursuit sa propre transformation numérique. Nous sommes à la fois leader digital auprès de nos clients et pour nous-mêmes puisque, dans le domaine informatique, nombreuses sont les ruptures technologiques en cours dans l'entreprise.

Big Data, Cloud, méthodes agiles... Autant d'évolutions que nous prenons en compte au sein de la Direction des Systèmes d'Information. C'est toute l'importance de l'évolution informatique qui se joue actuellement dans un contexte client qui se digitalise à grande vitesse. Chez Orange, nous sommes véritablement et de plus en plus sur une relation digitalisée avec nos clients. Certes, nous communiquons de manière déjà traditionnelle avec eux via le web. Mais depuis, les smartphones, les tablettes, les réseaux sociaux ont fortement développé ce mode de relation. Ce sont de nouveaux modes de communication avec nos clients via ces terminaux ou les moyens de communiquer qui changent profondément les usages et notre façon de travailler. Cela oblige l'entreprise et la Direction des Systèmes d'Information (DSI) à travailler différemment. Selon moi, les entreprises ont tout intérêt à s'occuper de ces nouvelles formes de communication et d'échanges pour être là où sont leurs clients. Le mouvement de la transformation numérique est quasiment devenu un impératif pour une entreprise à l'heure actuelle.

Pour reprendre votre question, la grande force d'Orange au sein de la transformation numérique est d'avoir installé une relation sur le digital avec ses clients et su adapter son système d'Information. Nous sommes en plein cœur des transformations numériques principales qui se jouent dans l'entreprise à savoir, celle de la relation avec les clients, de l'efficacité interne de l'entreprise grâce aux systèmes d'Information.

■ Le Cloud représente aujourd'hui 7% de la dépense informatique française totale. Pensez-vous que la transformation digitale et numérique passera forcément par le Cloud et le Big Data ?

Le Cloud fait partie du paysage des solutions possibles et à prendre en compte. Néanmoins, ce n'est qu'une partie émergée de la problématique de la digitalisation. La rupture provient surtout du Big Data qui offre maintenant la possibilité de stocker et d'utiliser de façon économique des quantités énormes d'informations. Le Big Data a fait diminuer de façon drastique les coûts de stockage et de conservation des données pour l'entreprise. Or, à l'heure actuelle, les entreprises n'utilisent que très peu leurs données propres. Si l'on rajoute à cela, les données partagées sur les réseaux sociaux et celles des objets connectés, on arrive à un flot d'informations aujourd'hui en majorité inexploité. Il est désormais possible avec des outils d'analyse sophistiqués de mieux connaître ses clients et de mieux travailler en termes d'efficacité interne. Le problème est que beaucoup d'entreprises manquent de moyens pour analyser les informations qu'elles ont en leur possession. La révolution du Big Data n'est pas une problématique de stockage mais l'enjeu et la difficulté résident dans la capacité d'analyse pour en tirer des bénéfices. Un lien plus étroit doit se mettre en place entre le SI et les parties prenantes dans l'entreprise.



« La rupture provient surtout du Big Data qui offre maintenant la possibilité de stocker et d'utiliser de façon économique des quantités énormes d'informations »

Orange développe deux axes majeurs d'approfondissement autour du Big Data. Le premier a pour ambition la compréhension et l'amélioration de l'expérience client. Le second est positionné sur les recherches d'efficacité interne en utilisant au mieux le panel des données à disposition et évidemment dans le cadre d'une charte d'utilisation de toutes ces données.

■ Par les quantités faramineuses de données produites partout et à tout moment, cela s'impose comme un réel défi pour les entreprises. Est-ce votre cas ?

Il va de soi que c'est un enjeu majeur pour toute Direction des Systèmes d'Information. Je ne pense pas qu'aujourd'hui une Direction de SI, de taille conséquente, ne puisse pas en tenir compte. Selon moi, le Big Data est un changement majeur dans l'entreprise. Cela demande d'avoir une certaine maîtrise technique inhérente à ces nouvelles technologies, de voir émerger des compétences voire des métiers nouveaux et de développer une proximité plus forte et plus agile avec l'ecosystème de l'entreprise. La Direction des Systèmes d'Information est au cœur de ce défi. Elle est naturellement légitime pour maîtriser ces techniques et les proposer de manière proactive aux décideurs des entreprises et aux services marketing, financier ou opérationnel. La DSI doit se positionner de plus en plus en proactif par rapport à ces métiers, être force de proposition et de valeur dans l'entreprise. Cela fait évoluer ses missions et ce que l'on attend d'elle..

■ Maitriser le Big Data, c'est aussi sécuriser les données qui s'y trouvent. Quelle est la force d'Orange dans ce processus de sécurisation ?

Le Big Data reste en effet un puits de données qui accentue l'importance de la sécurité. C'est donc inévitablement une question très importante dans le contexte actuel de cybercriminalité qui se développe également. Nous voyons tous ô combien la donnée est devenue un vrai capital et a de la valeur pour l'entreprise. Pour sécuriser les données qui nous sont confiées, le Groupe Orange s'est doté d'une charte sur les données de ses clients depuis 2014. Pour Orange, la sécurité des données constitue un élément essentiel de la confiance avec ses clients. Enfin, nous avons l'obligation et la responsabilité de protéger ces données clients. Nous avons mis en place donc tout un programme de sécurité des données clients structuré et très important chez Orange pour être à la hauteur de ces enjeux.

■ Selon vous, face à l'accumulation de ces données, quels enjeux vont s'imposer aux Directions des Systèmes d'Information dans les mois voire les années à venir ?

Je dirais que le Big Data pose aujourd'hui l'enjeu du développement et de la maîtrise de ces technologies d'une part, au niveau technique mais surtout en ce qui concerne les capacités d'utilisation. Quant au Cloud, cette nouvelle utilisation pose des enjeux grandissants en matière de développement et de sécurité, tout comme le Big Data. L'explosion des données sous toutes ses formes (texte, image, son, vidéo, structurées ou non structurées…) demeure aussi un véritable défi. C'est une révolution qui démarre et qui n'en est qu'à son début. Globalement, pour moi, les trois piliers – les trois enjeux pour les DSI sont le Cloud et sa maîtrise, le Big Data et son utilisation et la Sécurité. Vis-à-vis de cela, la force d'Orange, c'est notre capacité d'innovation et d'adaptation. Nous sommes au cœur même de cette transformation numérique qui touche la société dans son ensemble. Nous avons un rôle à jouer au niveau du marché sur ces sujets et qu'en tant que Direction des Systèmes d'Information, nous avons aussi l'obligation d'être exemplaire dans ce domaine. ■

CLOUD : ALERTE DU CESIN SUR LES DANGERS D'UNE EXTERNALISATION MASSIVE DES DONNÉES DES ENTREPRISES

Alain BOUILLE | Président du CESIN – Club des Experts de la Sécurité de l'Information et du Numérique.

■ Selon les résultats du baromètre Cesin-Opinion Way, 85% des entreprises stockent leurs données dans le Cloud. Face à l'adoption massive de cette nouvelle pratique, qu'est-ce qui vous apparait comme fondamental en matière de sécurité ?

Avant tout, je tiens à préciser que nous ne parlons pas ici de l'intérêt d'aller dans le Cloud ou non, nous évoquons ici la gestion des risques inhérents à l'usage du Cloud public. Nous sommes vecteurs de préconisations avant la prise de décision et chargés de leur mise en œuvre une fois que celle-ci est prise. Ce qui est fondamental est d'évaluer la valeur des données à externaliser et ce qu'elles représentent pour le patrimoine informationnel de l'entreprise. Prenons le cas des collectivités locales. Le Ministère de l'Intérieur et le Ministère de la Culture estiment, que ce qu'elles manipulent, relèvent du « Trésor d'Etat ». Par conséquent, les « Trésors d'état » ne peuvent sortir de la France. De fait, si les collectivités locales souhaitent héberger leurs données dans le Cloud alors, il faut qu'elles choisissent un Cloud souverain et non un Cloud étranger. Cela illustre bien l'importance d'évaluer la valeur des données. C'est le véritable point de départ. Ensuite, une fois que l'analyse de risques et de valeur établie, il est primordial de mettre en place nos recommandations en matière de sécurisation des données une fois la décision prise d'externaliser.

CESIN

Le CESIN a été créé en juillet 2012. C'est un lieu d'échange de connaissances et d'expériences qui permet la coopération entre experts de la sécurité de l'information et du numérique et entre ces experts et les pouvoirs publics.

Il réunit plus de 270 membres issus de tous secteurs d'activité publics et privés : des membres actifs, responsables de la sécurité de l'information dans leur organisation, des membres associés, représentants de diverses autorités en charge de Sécurité de l'Information au plan national, des juristes, experts de la sécurité IT.

Les 10 Recommandations du CESIN face aux projets Cloud ?

Issues de la réflexion et du partage d'expériences des membres du CESIN et d'un panel de spécialistes, dont l'ANSSI, la CNIL et des juristes spécialisés.

1 ■ Estimez la valeur des données que vous comptez externaliser ainsi que leur attractivité en termes de cybercriminalité.

2 ■ S'il s'agit de données sensibles voire stratégiques pour l'entreprise, faites valider par la DG le principe de leur externalisation.

3 ■ Evaluez le niveau de protection de ces données en place avant externalisation.

4 ■ Adaptez vos exigences de sécurité dans le cahier des charges de votre appel d'offre en fonction du résultat du point 1.

5 ■ Effectuez une analyse de risque du projet en considérant les risques inhérents au cloud comme la localisation des données, les sujets de conformité et de maintien de la conformité, la ségrégation ou l'isolement des environnements et des données par rapport aux autres clients, la perte des données liée aux incidents fournisseur, l'usurpation d'identité démultipliée du fait d'une accessibilité des informations via le web, la malveillance ou erreur dans l'utilisation, etc. Sans oublier les risques plus directement liés à la production informatique : la réversibilité de la solution et la dépendance technologique au fournisseur, la perte de maîtrise du système d'information et enfin l'accessibilité et la disponibilité du service directement lié au lien Internet avec l'entreprise.

6 ■ Outre ces sujets, exigez un droit d'audit ou de test d'intrusion de la solution proposée.

7 ■ A la réception des offres analysez les écarts entre les réponses et vos exigences.

8 ■ Négociez, négociez.

9 ■ Faites valider votre contrat par un juriste. Si vous êtes une entreprise française, ce contrat doit être rédigé en français et en droit français.

10 ■ Faites un audit ou un test d'intrusion avant démarrage du service (si cela est possible) et assurez-vous du maintien du niveau de sécurité de l'offre dans le temps.

■ Plus précisément, contre quelles dérives, le CESIN a-t-il récemment pris la décision de mettre en garde les dirigeants d'entreprises ?

Plusieurs types de problèmes peuvent se poser. Par contre, il faut bien comprendre qu'ils varient selon le service qu'une entreprise souscrit dans le Cloud. Acheter du IaaS (Infrastructure as a Service), du PaaS (Platform as a Service) ou du SaaS (Software as a Service) pose des problématiques différentes. Souscrire du IaaS ou du PaaS est moins problématique en termes d'expositions des données. Les services de SaaS sont différents. Cela peut aller de la souscription à quelques services non stratégiques pour l'entreprise à l'externalisation massive de données de clients (CRM) ou de bureautique.

« Les questions de gestion des droits d'accès et de gestion des habilitations sont des sujets fondamentaux à l'heure actuelle »

Dès lors, il faut prendre en considération des problématiques d'habilitation. Lorsqu'un utilisateur est habilité à accéder à une application sur le web, il est nécessaire de prendre en compte un certain nombre de préconisations. En effet, le jour où un utilisateur quitterait l'entreprise, malgré la coupure de son accès à distance, le service SaaS fonctionnerait quant à lui toujours. Il aurait toujours un navigateur et il pourrait toujours y accéder de chez lui. Ces questions de gestion des droits d'accès et de gestion des habilitations sont des sujets fondamentaux à l'heure actuelle. Sans parler des risques démultipliés d'usurpation d'identité lorsqu'on utilise un mode d'authentification simple pour accéder à ces services, ce qui est malheureusement encore trop souvent le cas.

Autre sujet qui entre en ligne de compte est la question de la supervision. Nous avons besoin désormais de plus en plus de savoir qui fait quoi, où et comment. Or, paradoxalement, tout utilisateur peut se connecter n'importe où, n'importe quand et dans n'importe quel service aux quatre coins du globe. Réintégrer les évènements de supervision afin de ne pas devenir aveugle vis-à-vis des attaques dont, les utilisateurs et les données pourraient être la cible apparait être un second challenge, peut-être plus difficile à adresser que le premier.

Enfin, le troisième élément pose l'autorisation d'auditer le fournisseur du service en question afin de contrôler si, les données sont correctement protégées. Cela va poser problème aux grands fournisseurs multi clients de services Cloud. Et, bien sûr, on peut les comprendre. S'ils autorisaient cela à tous leurs clients, ils passeraient leur temps à être auditer. La consigne en vigueur reste donc de leur demander de faire faire un audit eux-mêmes et de transmettre les résultats. Or, bien évidemment, nous savons bien que les résultats seront les plus édulcorés possibles.

Pour résumé, globalement, nous sommes sur une phase de perte de maîtrise de l'entreprise face à la sécurisation de ses données. La grosse difficulté reste la gestion de la donnée et des accès aux utilisateurs.

■ Prenons l'exemple d'une entreprise française qui serait liée aux obligations d'une entreprise américaine vis-à-vis du Patriot Act. Quels sont donc les risques existants ?

Les risques sont clairs aujourd'hui depuis l'épisode Snowden. Si une entreprise est de nationalité américaine, quel que soit son implantation dans le monde le Patriot Act s'applique. Néanmoins, le problème que pose le Patriot Act est connu et souligné depuis des années déjà. C'est un argument prégnant dans la tête de chaque RSSI lorsqu'un projet d'externalisation vers une solution américaine se fait jour. Il fait partie intégrante de l'analyse des risques. Or, cela n'a pas empêché une immigration massive vers le Cloud. Peu de chefs d'entreprises refusent d'aller vers le Cloud par rapport à cela. Mais ils y vont désormais en toute connaissance de cause. De mon sentiment personnel, je ne pense pas que le Patriot Act ait fait infléchir significativement les décisions d'immigration dans le Cloud.

■ Le recours au Cloud modifie le paysage de la sécurisation des données. Quelles interrogations et réflexions nouvelles amènent cette migration ?

Nous voyons bien comment tout cela évolue depuis quelques années. Dans les années 2000, les premiers projets d'externalisation ont commencé à voir le jour. Des entreprises ont pris le parti de confier à d'autres, ici et là, la réalisation d'applications programmées. Par exemple, on souhaitait confier l'hébergement de sa salle informatique à un grand acteur plutôt que le faire soi-même en interne. Néanmoins, jusqu'à cet avènement du Cloud, nous étions restés sur un système d'externalisation maîtrisée, auditable et surtout dédiée. En effet, nous savions où se trouvaient exactement nos données. De fait, nous pouvions avoir une garantie de sécurité par rapport à cela. Aujourd'hui, le Cloud pose le corollaire de l'impossibilité de localisation de ses données. Nous vivons depuis trois ans une vague d'externalisation massive vers le Cloud. Or, lorsqu'un chef d'entreprise signe un contrat dans le Cloud, il décide volontairement d'externaliser par exemple sa bureautique, sa messagerie et tout ce qui va avec. Ce n'est pas rien. Il faut en avoir conscience. Là, ce sont des téraoctets de données qui partent de l'entreprise. Ce n'est plus seulement quelques fichiers mais bien tout le patrimoine bureautique de l'entreprise.

Nous en sommes donc là. Je crois qu'à termes nous allons nous retrouver avec des systèmes d'Information totalement externalisés. Il est évident que certains cas font encore exception. Il est clair que les formules de calcul des salles de marché d'une grande banque française n'iront pas demain s'externaliser sur du Cloud. Ce sont les « Trésors de l'entreprise ». Malgré tout, je pense que nous allons vers une tendance de généralisation et par conséquent vers une complète dispersion des données. L'interrogation n'est plus de savoir où se trouvent les données. Le plus gros challenge pour l'entreprise et le RSSI est d'en assurer une protection la plus homogène possible. La problématique de la protection est prégnante de bout en bout. Il faut que ce soit cohérent. Nous pouvions nous contenter d'une certaine incohérence lorsque tout se passait en interne. Les risques étaient moindres puisque, cela restait dans le cadre et l'organisation interne de l'entreprise. Or, demain, tout cela va se promener sur le Cloud.

Selon moi, le maître mot de tout ça reste la cohérence. Arriver à avoir un niveau de protection qui soit homogène et cohérent tout au long du cycle de vie de la donnée est le challenge de la prochaine génération des RSSI. ■

Prochain Congrès annuel du CESIN les 6 et 7 décembre 2016 à Reims.

Pour les contacter :

CESIN - Club des Experts de la Sécurité de l'Information et du Numérique
14 rue Champfleury - 78730 Saint-Arnoult en Yvelines

contact@cesin.fr

www.cesin.fr

« L'interrogation n'est plus de savoir où se trouvent les données. Le plus gros challenge pour l'entreprise et le RSSI est d'en assurer une protection la plus homogène possible. »

COMMENT LA LÉGISLATION FRANÇAISE ET EUROPÉENNE S'ADAPTE-T-ELLE AUX NOUVEAUX RISQUES VIRTUELS ?

Maître Geneviève MAILLET | Avocat et Bâtonnier Elu.

■ Maître, en tant que première femme Bâtonnier de Marseille, vous avez divers objectifs notamment celui de numériser la Maison de l'Avocat afin d'en simplifier les accès et usages. Pouvez-vous nous en dire plus ?

La révolution numérique est véritablement prise en compte pour nous au niveau institutionnel. Il y a différents projets à l'étude aujourd'hui. Le premier est un projet national avec le Conseil National des Barreaux (CNB). Il a pour but de nous permettre d'avoir une forme de maîtrise technologique et un usage certes, facile, démocratisé sécurisé par le justiciable. Un Groupement d'Intérêt Economique (GIE), réunissant pour le moment un certain nombre de bâtonniers, étudie cette question de l'innovation de la relation entre les avocats et les relations clients. Nous avons une consœur qui a reçu le 17 mars dernier le « Prix du Public 2016 de l'Innovation des Avocats – Relation client » organisé par le site Village de la Justice. Elle a en effet crée une plateforme web dédiée à la fiscalité des non-résidents. Nous sommes au cœur d'une recherche de numérisation constructive. Globalement, je dirais que nous sommes ancrés dans une sorte de révolution à deux vitesses. La première vitesse est d'avoir un centre de droit des personnes démocratisé afin que tout un chacun puisse avoir accès aux grands thèmes. Ensuite, la seconde vitesse est d'avoir des sites internet plus spécialisés afin que nous puissions accompagner nos clients dans des questions plus adaptées aux cas pratiques.

■ Parmi vos nombreuses passions, il y a celle que vous portez aux technologies. Puisque c'est ici notre dossier, que pensez-vous de l'ubérisation massive du digital de notre société, de cette volonté du « tout connecté » ?

J'affectionne en effet un fort intérêt pour les technologies et les innovations de notre temps. Je travaille notamment avec Marseille Innovation depuis vingt ans. Ils ont été les pionniers en matière de startup et d'accompagnement aux pépinières d'entreprises. Aujourd'hui, le terme d'innovation est dans le langage courant. Pourtant, Marseille Innovation porte cet état d'esprit sur notre territoire depuis déjà vingt-cinq ans.

L'ubérisation du droit est une tendance lourde. Le conseil juridique est réservé aux avocats ce qui interdit en théorie aux sociétés commerciales de le pratiquer. Jusqu'à quand dans la mesure où la Commission européenne est profondément hostile aux règlementations professionnelles interdisant le libre accès à certaines activités sauf si ces règles sont édictées dans l'intérêt du consommateur. Un sondage américain aurait estimé insatisfaits à 80 % les besoins de droit des consommateurs. Actuellement, les prestations délivrées en ligne par les « legal startup » sont privées de la valeur ajoutée de la prestation d'un Avocat. Si on peut envisager que les solutions numériques puissent s'affiner, en revanche le respect des règles contrôlé par notre Ordre et le label de l'Avocat, protègent le justiciable avec une exigence forte, permanente et assurée.

Sur cette question du « tout connecté », l'Observation de l'ubérisation est aujourd'hui au carrefour de l'économie du partage, de l'innovation numérique, de la recherche de compétitivité et de la volonté d'indépendance des français. Il a fait l'objet d'une étude pour savoir comment cela allait petit à petit impacter tous les secteurs de l'économie traditionnelle de service. Le numérique est l'évolution majeure équivalente à la révolution de comportement née de l'imprimerie. En effet avant l'imprimerie, la population entretenait une tradition de

communication orale. Ensuite, il y a eu les caractères et leur transmission avec tout ce que cela a entrainé en termes d'accès à la connaissance. Aujourd'hui, nous sommes vraiment dans la mondialisation de l'information à la vitesse instantanée. L'Homme a raccourci l'espace. Il est passé de la marche à pied au cheval ; puis de la voiture à cheval à l'automobile puis au train, à l'avion, à la fusée. Dès lors, l'Homme ne peut plus raccourcir l'espace. Alors, il raccourcit le temps. Il n'y a pas si longtemps encore nous recevions le courrier à l'heure du facteur. Désormais, nous recevons des mails en permanence provoquant même souvent un phénomène de saturation. La manière de communiquer est si expéditive qu'automatiquement la relation instantanée est facilitée.

La France est en tête de ce digital pour tous en Europe. L'essentiel repose en fait sur un système de confiance et sur des communautés qui transforment notre façon de vivre. Nous travaillons. Nous créons de la valeur. Cela correspond à l'économie collaborative de nos jours.

Or, cette économie collaborative suit bien sûr une logique lucrative. Nous faisons intervenir des prestataires qui veulent gagner leur vie en rendant un service au consommateur final. Plus il y a cette forme intermédiaire de commissions, moins nous avons le sentiment de payer quelque chose. Si l'objectif de ce phénomène est louable, ne passe-t-il pas par un business qui place le consommateur au cœur d'un système afin de répondre à des demandes toujours insatisfaites ? Ne créent-ils pas pour autant un obstacle aux entreprises traditionnelles qui sont encouragées à évoluer en suivant les pas de modèles disruptifs ? Dans le Droit des Affaires, mon souci est d'accompagner mon client qui voit son modèle de rentabilité bouleversé. Ainsi, l'essentiel de la difficulté qui tient à l'ubérisation, et plus généralement, à cette numérisation de l'économie est la survenance d'une forme de destruction d'emplois. De la même façon, au XIXe siècle, lorsque nous avons mis en place les industries mécaniques, les couturières ont très vite compris qu'elles n'avaient pas leur place dans ce phénomène. Pour autant, la qualité n'est pas dans le low-cost.

J'ai prêté serment l'année de l'abolition de la peine de mort voyez-vous. J'avais donc conclu mon concours d'entrée dans la profession en disant qu'il y a un éternel problème entre « un droit qui n'est plus » et un « droit qui n'est pas encore ». Ici, pour notre propos, j'ai envie de dire que c'est toute la difficulté entre un « droit qui n'est plus tout à fait » et un « droit qui est en cours d'être ». On le voit bien avec l'ordonnance du 10 février 2016 sur la modification du droit des contrats du régime général et de la preuve des obligations comme on le voit dans les dispositions en droit du travail applicables au 1er août 2016 concernant les juridictions prud'homales.

Objectivement, ce phénomène du « tout connecté » est largement engagé. Nous n'avons plus que le temps de nous y adapter. Il est vrai qu'il y a une forme de répulsion du législateur qui voit la remise en cause de ses principes traditionnels. Or, comme vous le dites si justement, il n'est plus possible de faire machine arrière. Pour moi, l'économie marseillaise a déjà évolué de l'industrie lourde vers les technologies numériques. Je pense qu'aujourd'hui si, nous avons la prétention d'avoir légitimement une French Tech ; c'est que nous sommes en mesure de faire face à cette révolution et d'y prendre part.

■ Dans une société telle que la nôtre où, le numérique règne en maître, les entreprises n'échappent pas aux risques cyber existants. En tant qu'Avocat spécialisé dans le Droit des Affaires, sur quels types de risques les accompagnez-vous ?

Le 4 juin 2013, aux côtés d'Alain JUILLET, ancien Haut Responsable de l'Intelligence Economique et Fondateur de l'association « Sécu Tic », d'experts et de représentants de la Gendarmerie Nationale, nous avions présenté à la Maison de l'Avocat une réunion d'informations sur le thème suivant « Les nouvelles frontières du Droit pénal et commercial en matière d'économie numérique. » Nous n'étions pas visionnaires puisque c'était déjà une évidence.

Dès que vous allumez votre ordinateur, sans prendre aucun risque objectif particulier, vous êtes susceptible de vous retrouver en situation de dangerosité potentielle. Lorsque j'étais jeune, ma grand-mère me disait souvent « si tu sors, ne fais pas de mauvaise rencontre ». Or, vous voyiez combien ce risque est possible. Néanmoins, c'est un phénomène actif. C'est moi qui sors et qui décide de la ruelle que je prends. A la différence, avec le risque de cybercriminalité, vous appuyez sur le bouton de démarrage mais vous n'êtes pas sorti, vous ne savez pas quelle est la ruelle et vous ne savez pas qu'elle est sombre. En tant qu'Avocats, nous avons entre autres missions celle de participer à prévenir et guérir les difficultés du justiciable quel qu'il soit. Prévenir, c'est envisager le numérique comme un outil de modernisation qui engendre des risques anticipés dans la maîtrise des spécialités comme le Droit maritime, le Droit commercial, le Droit de l'environnement par exemple. Nous protégeons nos clients tout en participant à l'élaboration de pratiques nouvelles. Prévenir, c'est anticiper. Faire un audit est un réel moyen de

Journal quotidien d'information numérique

Destimed
5, rue Menpenti, Bât. O
13010 MARSEILLE

www.destimed.fr

connaitre ses risques juridiques afin de pouvoir les couvrir au mieux et assurer ce qui apparait comme le plus important. Guérir, c'est le travail de recherche actuellement mis en place par les théoriciens du droit, les praticiens du droit, et même les compagnies d'assurance pour participer à une réponse réparatrice face à ce problème. Et comme l'affirme l'Observation de l'ubérisation, nous nous posons la question suivante actuellement : comment ne plus subir mais être éveillé, réfléchi, inclusif ? C'est sur ce point que le rôle du droit français est fréquemment critiqué pour son manque de dynamisme par rapport aux pays de Common Law.

« La cybercriminalité serait plus lucrative que les trafics de cocaïne et d'héroïne confondus »

■ A l'échelle nationale et européenne, que met-on en place pour lutter contre la cybercriminalité et quelles sont les difficultés qui se posent ?

Le Conseil de l'Europe a amorcé ce combat à l'international en adoptant une Convention sur la cybercriminalité en 2001. C'est un traité adopté par les Etats-Unis et considéré comme une réponse potentielle à cet enjeu. L'Union Européenne s'est introduite dans cette lutte avec un règlement sur la protection des données à caractère personnel. Il y a des développements internationaux supplémentaires en cours.

En France, nous avons des dispositions législatives qui ont largement dépassées le cadre de départ de notre modèle sécurité / liberté. Aujourd'hui, les textes sont repris et ont été mis en relief par la Commission Européenne qui a affirmé que la cybercriminalité touchait chaque jour plus d'un million de personnes dans le monde et coûtait plus de 400 milliards de dollars à l'international. Pour vous donner un ordre d'idée, la cybercriminalité serait plus lucrative que les trafics de cocaïne et d'héroïne confondus. Le problème est que le champ géographique ne se limite pas à des frontières. Le principe de territorialité pour déterminer la compétence juridictionnelle et les règles applicables est très difficile à adapter à ce type d'infraction. Nos dispositions législatives nous permettent effectivement de porter des procédures pénales. Or, une fois que vous avez porté plainte contre le responsable qui est à un endroit intouchable, comment répare-t-on le dommage concrètement ? La difficulté est qu'il n'y a pas toujours d'indication du lieu d'où vient la personne qui a commis l'infraction la plupart du temps.

Par contre, nous savons bien qu'il y a des risques protéiformes. En cela, nous devions apporter une sorte de réponse lors de la réunion du Barreau en disant que, pour nous Avocats, nous restions tout de même dans une recherche perpétuelle pour envisager une nouvelle approche des questions pratiques et des solutions juridiques afin de mieux connaître les fléaux que représentent cette cybercriminalité et mettre en œuvre des éléments de défense par rapport à nos clients. L'idée est donc de proposer des contrats adaptés qui créent des responsabilisations acceptées entre les professionnels sous condition, à mon sens, d'avoir un minimum de sécurité au départ. Dans tous les cas de figures, peu importe la taille de l'entreprise, ayant intégré des mesures préalables de sécurité et des mesures de garantie, il faut prévoir une clause conventionnelle qui délimite qui sera responsable de quoi en cas de quelque chose. C'est du cas par cas, c'est du coût par coût. Je crois que là nous avons un véritable enjeu de sur mesure.

■ Dernière question, une législation universelle est-elle une solution possible pour lutter contre ce fléau du cyber risque pénal ?

Je pense effectivement que face à la mondialisation de la criminalité c'est un véritable enjeu. Je me souviens quand j'étais adolescente, je m'interrogeais fréquemment sur le feuilleton «Les Brigades du Tigre » où, les policiers de l'époque poursuivaient en vélo des voleurs qui eux roulaient en traction avant. J'ai donc l'impression que tant que nous n'aurons pas l'équivalent de la « traction avant du XXIème siècle » : il sera difficile d'être à armes égales face à des délinquants ou des malveillances qui n'ont de cesse d'avoir un coup d'avance sur les acteurs et les victimes

de la société. Je ne veux pas simplement faire des citations. Mais, j'ai encore un exemple flagrant de ce vers quoi nous allons demain. Dans le film, tiré d'une histoire vraie « Attrape-moi si tu peux », le personnage réel interprété par Leonardo DI CAPRIO était une personne qui se trouvait dans une situation délinquantielle au départ. Or, elle est devenue un si grand spécialiste de l'expérience de la fraude que finalement, les services de la CIA l'ont recruté pour sa compétence et mettre le doigt sur les principales faiblesses du système (une forme de Vidocq). Je crois donc que c'est vers cela que nous allons tendre. Des hackers seront sans doute recrutés pour aider dans cette lutte contre la cybercriminalité.

Il y a une autre question sur laquelle j'ai demandé que l'on se penche aussi. C'est celle de la robotisation. Faut-il un Droit pour les robots ? Nous parlons beaucoup de numérique, d'innovation, d'ubérisation, de virtuel. Or, c'est une vraie question car, la robotisation sera peut-être demain gérée par des systèmes numériques à distance. Or, nous allons être dans une mécatronique de machines humanoïdes que la plupart du temps nous ne voyons pas. Prenons l'exemple tout simple du GPS. Il faut bien sûr au préalable de toute utilisation le régler sans vous tromper. Alors, est-ce que la robotisation ne sera pas demain de laisser le véhicule choisir la destination et nous y amener sur une simple instruction verbale et subjective ? A ce moment-là, je vous pose la question. Qui sera responsable de l'erreur ? Et dans le cas où quelqu'un piraterait le système pour faire un kidnapping ? Ne serait-ce en effet pas plus simple à orchestrer et efficace que de payer deux hommes en cagoule et un chauffeur ? La robotisation est une grande question à venir remplie d'enjeux.

■ Le mot de la fin Maître Maillet ?

Je pense que l'imagination, l'innovation et la création ont toujours été la solution du progrès et de l'évolution. J'ai joué aux échecs contre des robots et ils m'ont battu, je le confesse. Or, je pense que je n'ai pas été assez imaginative, créatrice, ni suffisamment entrainée. D'une certaine façon, je dirais que l'humain doit s'adapter plus vite que la technologie. Et toute numérique que soit cette révolution, elle est tout de même faites à preuve du contraire par des hommes et pour eux. La machine n'a pas précédé l'Homme.

Nous avons tous les moyens d'agir collectivement et dans l'intérêt de tous. ■

Pour contacter le Cabinet d'Avocat :

SELARL MAILLET-DOSSETTO
69, Rue Saint-Ferréol, 13006 MARSEILLE

04 91 55 06 18

« La robotisation est une grande question à venir remplie d'enjeux »

VOITURE CONNECTÉE, UNE RÉVOLUTION DE L'INTERNET DES OBJETS À SÉCURISER

Laura GUILLAUME | Directrice commerciale B2B – Groupe TRAQUEUR

En quelques chiffres, le Groupe TRAQUEUR c'est :

Près de 9 voitures sur 10 géolocalisées en moins de 24 heures en moyenne.

Plus 7 000 affaires de vols résolues depuis sa création.

Plus de 130 millions d'euros économisés en valeur d'achat de véhicules retrouvés.

■ Pouvez-vous nous préciser vos fonctions au sein du Groupe TRAQUEUR ?

Je suis Directrice Commerciale de la division B2B du Groupe TRAQUEUR. Nous délivrons nos services aux professionnels de la petite à la moyenne entreprise jusqu'aux grands groupes. Nous sommes positionnés sur la France et sur l'international. Nos différents secteurs d'intervention sont ceux de l'industrie, des travaux publics, de la location pour n'en citer que quelques-uns.

■ On parle beaucoup en ce moment de la « voiture folle » ou autrement dit, du piratage et de la prise de commande à distance d'une voiture connectée. Selon vous, est-ce un risque grandissant ou à l'inverse une menace plus médiatisée que de raison ?

Il est vrai qu'il y a de plus en plus d'affaires relatées dans l'actualité démontrant que les voitures désormais connectées et informatisées peuvent présenter des failles de sécurité. C'est une menace existante, généralisée je ne pense pas, mais, il faut la prendre sérieusement en compte.

■ Quelles sont les nouvelles méthodes des voleurs et comment y adaptez-vous vos solutions ?

Selon les chiffres du Ministère de l'Intérieur, il y a eu 110 000 vols de véhicules en France en 2015. Ce chiffre est en augmentation de 2,3% par rapport à l'année précédente. Cela représente 300 vols de véhicules par jour. Pour vous donner une idée, en perspective de ces chiffres sur le parc TRAQUEUR, la cellule « Opérations vols » a traité plus de 800 vols en 2015, soit près de 70 vols par mois, témoignant d'une capacité d'intervention unique en France. Mais les méthodes de vol évoluent et diffèrent. Nous parlons aujourd'hui beaucoup du « mouse-jacking », aussi appelé le « vol à la souris » en français, qui consiste à pirater les systèmes électroniques d'une voiture pour la voler. C'est une nouvelle méthode qui est en très forte augmentation. Nous avons d'ailleurs réalisé quelques statistiques sur cette façon de procéder qui représente aujourd'hui près de 70% des vols de véhicules car, il s'agit d'une méthode plus discrète et plus facile à préparer à distance.

Le Groupe TRAQUEUR est le leader de l'après-vol en France avec 80% de parts de marché. Nous ne proposons pas des solutions anti-vol mais bien des solutions d'après-vol. Si le vol est commis et avéré, nous sommes capables de récupérer le véhicule 9 fois sur 10 dans les 24 heures. Quelle que soit la méthode de vol, l'important pour le Groupe TRAQUEUR est moins d'empêcher celui-ci que de récupérer le plus rapidement possible le véhicule dans les meilleurs délais et le meilleur état.

■ Plus spécifiquement, en 2015, le Groupe TRAQUEUR lance Nano, la première balise mobile dédiée à l'Internet des Objets. En quoi consiste-elle ?

La balise Nano est une balise autonome, de petite taille, sans fil. C'est comme une petite boite noire. Elle est facilement et rapidement installable ce qui est très important pour ne pas perturber la productivité d'une société. Nano n'est jamais installée aux mêmes endroits sur les véhicules, ce qui est un gage de sécurité supplémentaire pour lutter contre le vol. En effet, les voleurs potentiels ne savent jamais où est placée la balise et donc où la chercher. La balise Nano n'émet de signaux qu'à des moments très furtifs. Elle est donc difficile à détecter et extrêmement difficile à brouiller. C'est vraiment une très belle solution pour assurer la récupération après le vol même en cas de brouillage, méthode d'opération phare des voleurs, qui empêche toute localisation géographique du véhicule par GPS. En effet, Nano intègre différentes technologies qui permettent de contourner ces limitations. La particularité de Nano, c'est qu'elle communique via le réseau Sigfox, réseau opérationnel pour l'Internet des Objets. Ce réseau est conçu et structuré pour pouvoir supporter les connexions de bon nombre d'objets. La balise Nano va autant s'adresser à des objets roulants (voitures, engins de chantier, camions, utilitaires) qu'à des objets non roulants dont, le chef d'entreprise souhaiterait conserver la traçabilité. Avec Nano, le Groupe TRAQUEUR assure le suivi de tout ce qui roule et plus généralement de tout ce qui peut être déplacé.

Nous aidons nos clients à lutter contre le vol mais aussi contre l'escroquerie. Par exemple, pour assurer la sécurisation d'un véhicule, nous avons également des solutions d'identification gérables à distance. Cela permet de bloquer le démarrage d'un véhicule par des codes d'activation. Ce qui est un point fort en matière de cybersécurité des véhicules connectés pour le Groupe TRAQUEUR.

■ Vous êtes aussi partenaires depuis plus de 10 ans de PSA Peugeot Citroën pour la distribution de nouveaux services connectés à bord des véhicules de leur marque. Pouvez-vous m'en dire plus ?

Ce partenariat est en effet complémentaire dans le cadre de cette même ligne directrice et stratégique qu'est la récupération du véhicule après le vol. Le Groupe TRAQUEUR propose un service après vol mais, il propose également des services télématiques très complets. Nos solutions permettent le suivi des véhicules, la remontée temps réel des positions, les historiques cartographiques, la consommation, etc. Autrement dit, la remontée de toutes les données du véhicule à partir du boitier électronique du constructeur. Pour les autres constructeurs, nous sommes en mesure de proposer la mise en place d'un boitier TRAQUEUR et d'intégrer les données sur une plateforme unique proposant le même service et opérant de la même manière. L'ensemble de nos clients peuvent ainsi gérer des zones de geofencing, recevoir des alertes, produire des tableaux de bords, etc.

■ Comment évalueriez-vous le niveau de sensibilisation à l'importance des données présentes dans les voitures connectées aujourd'hui et donc l'importance de tels dispositifs ?

Comme vous le disiez précédemment, il y a des cas médiatisés qui viennent alerter les acteurs du marché. Les chefs d'entreprises y sont sensibles parce qu'il s'agit d'un risque, dans la mesure où, le véhicule représente un actif important de la société. Et si vous êtes un loueur de véhicules, un transporteur de biens ou de personnes… Le parc automobile représente le cœur de l'activité de la société. Au vu de ces constats, anticiper et gérer le risque de vol est extrêmement important. C'est un impératif, pour éviter la perte conséquente de la valeur d'un véhicule mais également du service qu'il rend. Les 800 vols traités par le Groupe TRAQUEUR en 2015 représentent une valeur en biens de 18M€. C'est pour ces raisons que nous avons une écoute assez forte de la part de nos clients BtoB y compris des assureurs qui recommandent d'installer des traceurs basés sur un système de GPS permettant de localiser les véhicules. C'est un mouvement qui a démarré depuis un certain temps et qui ne cesse de s'accélérer.

■ Dès lors, vous pouvez donc dire que vous participez en quelque sorte à la protection des actifs matériels de l'entreprise ?

Tout à fait ! Nous en assurons le patrimoine et nous en prévenons les risques. Nous réduisons le risque financier, le risque de dégradation du véhicule et la perte de productivité puisque, nous le récupérons avec beaucoup de réactivité, le plus souvent dans la journée. Aussi, au-delà d'un diagnostic simple du positionnement de la voiture, nous pouvons faire jouer certaines technologies particulières qui nous permettent de géolocaliser et de retrouver le véhicule lorsqu'il est positionné en sous-sol ou caché dans un garage, dans un box ou dans un conteneur par exemple.

■ En matière de cybersécurité des véhicules connectés et dans ce genre d'investigations plus poussées, un partenariat public – privé s'opère-t-il pour plus d'efficacité ?

En effet, nous avons pour cela un partenariat avec les forces de l'ordre. Quand un client subit un vol ou une escroquerie, il peut solliciter un recours juridique auprès des forces de l'ordre. Sur dépôt de plainte, nous allons pouvoir géolocaliser le véhicule et faire une recherche fine pour obtenir un maximum de précisions sur sa situation. Dans ce cas, les forces de l'ordre collaborent avec nous pour valider la propriété du véhicule volé, le récupérer et le restituer à son propriétaire. Ce qui est intéressant ici, c'est que c'est un véritable partenariat gagnant-gagnant. Les forces de l'ordre nous permettent d'avoir un arsenal légal d'autorisations notamment pour pouvoir pénétrer dans une propriété privée ou intervenir dans un endroit clos. A l'inverse, les forces de l'ordre peuvent grâce à nous, démanteler des gangs. Cela est souvent arrivé. En effet, les voleurs peuvent être des personnes isolées comme de grandes organisations plus structurées et organisées. Globalement, grâce à ce partenariat, une forte relation de confiance et de légitimité s'est instaurée entre le Groupe TRAQUEUR et les forces de l'ordre.

■ Globalement, quelle est la force du Groupe TRAQUEUR pour détecter et barrer la route à de potentielles tentatives de piratage et de prise de contrôle à distance d'un véhicule par un tiers ?

Le Groupe TRAQUEUR est au cœur de la problématique du vol et de la fraude. Nous possédons les capacités technologiques, techniques et matérielles qui nous permettent d'assurer la recherche et la récupération du véhicule en cas de vol ou d'escroquerie. C'est une vraie force puisque, cela nous permet d'accompagner nos clients jusqu'au bout de la démarche. La réactivité, la confiance et la proximité sont vraiment les valeurs essentielles du Groupe TRAQUEUR. ■

GROUPE TRAQUEUR
APRÈS-VOL - INTELLIGENCE EMBARQUÉE

Visitez leur site Internet et contactez-les sur :

www.traqueur.fr

« Nous possédons les capacités technologiques, techniques et matérielles qui nous permettent d'assurer la recherche et la récupération du véhicule en cas de vol ou d'escroquerie»

QUELLE POLITIQUE DE PROTECTION DES DONNÉES MARSH MET-ELLE EN PLACE POUR LUTTER CONTRE LA CYBERCRIMINALITÉ ?

Didier PICUT | Directeur Régional Sud Est chez Marsh S.A.

■ En tant que Directeur Régional de la région sud-est, trouvez-vous que les entreprises de notre région sont particulièrement sujettes aux risques cyber ?

Toutes les entreprises sont touchées aujourd'hui par les cyber attaques, des TPE aux grands groupes internationaux ! Le cas le plus fréquent rencontré par nos clients est la cyber extorsion : des hackers cryptent les données de l'entreprise et exigent une rançon pour donner la clé de décryptage. Dans ces cas-là, il faut savoir réagir et adopter les bons réflexes pour gérer la crise. Une PME du Béarn a brisé l'omerta il y a quelques semaines en racontant la mésaventure qu'elle a connu sur ce sujet.

■ Selon une récente étude menée par Marsh en Europe, 68 % des entreprises n'ont pas évalué l'impact financier d'une cyberattaque. Trouvez-vous qu'en France également vos clients sous estiment l'impact en termes de risques et de dommages d'une telle attaque ?

De moins en moins car, malheureusement, les attaques sont de plus en plus fréquentes. Nos clients comprennent bien que le risque est réel et que la question n'est plus de savoir si une entreprise va être attaquée, mais quand cela va se produire. En revanche, évaluer l'impact financier est un exercice compliqué et c'est pourquoi Marsh propose des outils d'aide à la quantification de ce risque.

■ Face à la multiplicité des menaces cyber et leur rapidité d'évolution, les solutions d'assurance traditionnelle suffisent-elles à appréhender l'intégralité des cyber risques ?

Les polices traditionnelles (RC, Dommages…) ne constituent pas une réponse adaptée à la menace cyber. En revanche, les assureurs proposent une solution de services dédiés qui permettent de combiner le volet « assurance » pour l'indemnisation des conséquences financières, avec un volet « assistance » pour aider les entreprises à réagir de façon rapide et adaptée en cas de sinistre cyber. Par exemple en cas de cyber extorsion, les assureurs mettent à disposition de l'assuré un expert en négociation avec les hackers ou encore un expert informatique pour tenter de « cracker » le code malveillant. A notre sens, ces deux volets sont complémentaires et indispensables pour les PME qui n'ont pas les moyens de faire face à une crise cyber. Nous proposons même depuis quelques mois d'y ajouter un volet « prévention » qui vise à apporter à l'assuré des conseils simples pour mieux sécuriser son SI. Les assureurs jouent alors pleinement leur rôle d'acteurs, véritable moteur de l'amélioration de la sécurité des entreprises et donc de la sécurité nationale !

■ Concrètement, quelles solutions innovantes et quelles gammes de couvertures mettez-vous en place pour couvrir les risques cyber ?

Fort de notre position de leader sur le marché cyber en France, nous challengeons les assureurs au quotidien sur ces risques. Nous mettons régulièrement à l'épreuve les assureurs sur les aspects suivants qui répondent au besoin de nos clients :

- Simplicité de souscription (les questionnaires sont trop complexes à remplir),
- Etendue des garanties,
- Garantie « assurance » : déploiement d'une police d'assurance cyber rédigée par Marsh,simple et complète, écrite dans l'intérêt de nos clients et non des assureurs (unique en France),
- Garantie « prévention » inédite,
- Garantie « assistance » éprouvée et sans franchise,
- Optimisation des conditions tarifaires (capacités, primes, franchises).

Nous avons bâti des partenariats avec des assureurs qui répondent à ce cahier des charges.

■ Marsh offre la possibilité d'évaluer son profil de risque cyber via un questionnaire en ligne et l'édition d'un rapport assez précis. Pouvez-vous nous en parler ?

Nous proposons effectivement à tous les acteurs d'évaluer gratuitement en ligne leur exposition spécifique au risque cyber au travers d'une série d'une trentaine de questions (www.marsh-stresstest.eu). Le rapport généré après avoir rempli ce questionnaire sert alors de base pour aborder plus en détail le risque cyber qui est différent pour chaque client en fonction de son organisation, son activité… C'est donc plus un point de départ qu'un aboutissement. ■

« Les polices traditionnelles ne constituent pas une réponse adaptée à la menace cyber »

MARSH

Tour Ariane - 5, Place des Pyramides - 92800 Puteaux

Visitez leur site Internet et contactez-les sur :

www.france.marsh.com

SERIOUS GAME : QUAND LA GAMIFICATION GAGNE LE DOMAINE DE LA CYBERSECURITÉ

Thibault RENARD | Responsable Intelligence Economique à CCI France.

■ Jeux de plateau ou vidéo sur la cyberguerre, sur la formation à la sûreté des informations, sur la sensibilisation à l'e-réputation. Qu'est-ce qui vous motive aujourd'hui à promouvoir et encourager les Serious Game en matière de cybersécurité ?

A l'origine, le Serious Game était une réflexion que nous avions sur tout ce qui avait attrait aux Business Game, et notamment ce que des évènements de type « murder party », de par leur dimension d'investigation, pourraient apporter en matière de sensibilisation à l'Intelligence Economique. Assez rapidement, nous sommes très vite intéressés de manière plus générale aux Serious Game, sachant que les CCI en avaient déjà créé un dans le passé sur la création d'entreprise, et s'appétait à en lancer un sur l'intelligence économique.

En fait, les Serious Game existent depuis bien longtemps déjà. Néanmoins, ils prenaient essentiellement la forme de jeux de rôles ou de jeux de plateaux. Aujourd'hui ils existent essentiellement sous la forme de jeux vidéo, mais pas que. C'était quelque chose que l'on observait donc, mais de loin. Il n'y avait pas eu véritablement de réflexion globale sur le sens même de l'utilité de ces outils dans nos professions. Etait-ce pertinent d'utiliser les Serious Game dans le domaine de la sécurité ou de l'Intelligence Economique par exemple ? Telle était la question. Nous nous sommes donc tout naturellement lancés dans un référencement précis des jeux existants, exposant divers questionnements (spécificités, objectifs recherchés, types de scenario, etc.).

CCI Intelligence Économique

Un jeu vidéo gratuit, interactif et pédagogique sur l'IE.

www.jeu-ie.cci.fr

Sois net !

Protège ton image numérique, ta réputation sur Internet.

Gratuit et destiné à un public jeune (11-13 ans).

www.mediapolice.ch

Nous nous sommes rendu compte assez naturellement que les Serious Game étaient de plus en plus utilisés. Aujourd'hui, on voit bien combien c'est un outil prometteur. Ils sont « à la mode » si je puis dire car, outre qu'ils bénéficient de la démocratisation des jeux vidéo et de leur généralisation à tous les supports numériques, ils s'inscrivent dans le phénomène plus vaste de la « gamification ». Néanmoins, la mise en place de Serious Game n'est pas coordonnée. En réalité, chacun prend une initiative indépendante, selon le secteur, le public ou le message à faire passer. On se retrouve donc avec des Serious Game qui fleurissent dans certains domaines comme la sécurité et d'autres où ils sont quasiment inexistants.

Netwars, la guerre sur le net

Jeu documentaire d'Arte s'appuyant sur les discussions politiques actuelles entre les puissances mondiales.

Gratuit et tout public.

http://future.arte.tv/fr/netwars

Info Sentinel de Getzem

Elu meilleur « Learning game » d'Europe en 2014, destiné à la formations des personnels à la protection de l'information.

Destiné aux entreprises (100€ / an)

www.info-sentinel.com

Cryptris, de l'INRIA

Comprendre la cryptographie.

Gratuit et destiné aux étudiants

inriamecsci.github.io/cryptris/jeu.html

■ Les utilisateurs sont confrontés à des situations à risques, tels de véritables collaborateurs de l'entreprise. Quelles sont les bases d'un bon « Serious Game » selon vous ?

Il faut tout d'abord noter qu'il y a deux styles de jeux. Il y a le jeu en ligne sur le Net et le jeu utilisé en entreprise, dans le cadre d'un jeu vidéo installé sur le poste de travail, ou d'un jeu de rôle, de type simulation par exemple, impliquant plusieurs personnes. On peut donc difficilement avoir des retours véritables d'un jeu en ligne utilisé via des connexions externes. Par contre, on sait que le jeu marche selon le temps d'utilisation de l'internaute via son ordinateur. Si on sait qu'un utilisateur a passé entre vingt minutes et une heure à jouer via le Serious Game alors, on considère que c'est une réussite. D'ailleurs, la plupart des Serious Game ne dépassent pas une à deux heures d'utilisation. Vous savez, aujourd'hui à notre époque où nous sommes en permanence sollicités, cela devient un exploit que de garder l'attention d'une personne plus que quelques minutes. C'est une des problématiques à laquelle répond le Serious Game. En effet, notre société fait que nous sommes de moins en moins attentifs. Tout le monde a une chute de l'attention. En moyenne, une vidéo YouTube à vocation professionnelle (conférence, sensibilisation…) peut difficilement maintenir l'attention de celui qui la visionne au-delà de trois minutes. Désormais, l'unité à laquelle nous sommes confrontés se situe entre la minute et la seconde. Le Serious Game réussit donc cet exploit de regagner l'attention quasi exclusive des utilisateurs et de la maintenir pendant le jeu. C'est pourquoi par exemple, de nombreux documentaires prennent la forme de « jeux documentaires », une catégorie de Sérious Game particulièrement utilisée par les sociétés de productions audiovisuelles car, ils impliquent davantage le spectateur, voire même permettent de fédérer une communauté autour du jeu, là où le téléspectateur reste passif.

Outre être parvenu à « regagner » l'attention, le second impératif de succès du Serious Game est l'existence d'un message persistant dans l'esprit de l'utilisateur. Il faut que ce message « trotte dans la tête » après l'utilisation du Serious Game. C'est cela qui va permettre un recours à une formation, une envie d'en parler autour d'elle, d'abandonner certaines pratiques à risque. Souvent, la personne va se sentir gênée vis-à-vis de certaines de ses pratiques quotidiennes qu'elle sait mauvaise en matière de sécurité. Si de telles réflexions naissent ou si de telles initiatives sont prises, alors, le Serious Game est un succès.

■ Est-ce pour vous un moyen durable de sensibilisation et de formation en matière de cybersécurité ?

Je pense que c'est un moyen très efficace et pertinent en matière de sensibilisation, voir même d'évaluation du degré de sensibilisation de ses collaborateurs. Néanmoins, ce n'est pas un jeu qui va vous former. Je me répète mais, c'est vraiment un moyen de faire persister un message dans l'esprit des utilisateurs. Je dirais que c'est un premier point d'entrée pour amorcer de la formation. Imaginez le cas d'un grand groupe. Il me semble difficile d'organiser une session de formation et de sensibilisation pour un groupe de 50 000 collaborateurs. A la différence, il est possible de mettre à disposition un Serious Game sur les ordinateurs des différents postes de travail. A l'inverse, une PME d'une dizaine de collaborateurs pourrait n'avoir ni le temps, ni les moyens de solliciter un organisme extérieur ou de s'offrir un intervenant pour une session de formation. Là encore, consulter un Serious Game via Internet permet en une heure de temps de sensibiliser le collaborateur.

Cela dit, un Serious Game ne remplacera jamais une réelle formation de dix jours, de six mois, d'un an. Cela permet tout de même de donner quelques bases. Mais, outre cela, ce n'est pas la logique d'un Serious Game que de durer six mois. Tout au plus, le Serious Game peut être idéal pour une formation d'une ou deux journées dans une logique de Business Game et de « Team Bulding » pour renforcer la cohésion et l'esprit d'équipe en entreprise, par exemple en simulant un exercice de crise. Néanmoins, à terme, on peut imaginer l'intégration de Serious Game à des formations longues et en ligne, dans les MOOC par exemple.

■ Comment la CCI France encourage-t-elle ce type d'initiatives ?

Au sein des CCI, nous avons déjà un certain nombre de Serious Game mis en ligne sur plusieurs thématiques : Ma Ch'tite Entreprise sur l'entreprenariat (CCI Grand Hainaut); CCI Intelligence Economique (CCI de Normandie) et tout récemment sur l'industrie du futur (CCI d'Alsace)… Nous donnons également la parole à des créateurs de Sérious Game lors d'interview vidéo diffusées via le Portail de l'IE.

En parallèle de cela, nous mettons également en place des démonstrations gratuites de Serious Game. Nous le faisons assez régulièrement depuis un an maintenant. Cela peut être à l'occasion de rencontres parlementaires cybersécurité, de rencontres sur la cybersécurité ou d'événements Intelligence Economique. Cela fonctionne très bien et nous avons un très bon accueil. Celles-ci captent considérablement l'intérêt et l'attention de l'auditoire. Concernant les jeux payants, nous donnons aussi l'occasion à des éditeurs de faire des démonstrations. Pour une entreprise, l'achat d'un Serious Game reste très accessible puisque, la plupart du temps, les tarifs oscillent entre 10 et 100 euros. Néanmoins, dans un premier temps, notre objectif est avant tout d'encourager le public à se diriger pour découvrir cet univers, vers des jeux qui existent gratuitement sur le net. Puis, pour ceux qui veulent aller plus loin, nous leur indiquons au besoin d'autres Serious Game payants en complément, qui de notre point de vue, semblent les mieux adaptés aux différentes problématiques.

■ Pensez-vous que le phénomène de « gamification » puisse être le futur de la cybersécurité ?

En effet, je pense que la gamification sera à terme de plus en plus incontournable en matière de sensibilisation. Il me semble impossible d'échapper à ce phénomène dans notre société de la dématérialisation et du tout connecté. La gamification permet de s'approprier cette tendance. Il est évident qu'à l'avenir, ce qui va sensibiliser l'utilisateur sera directement connecté à lui via son smartphone, sa tablette, son ordinateur. Certains Serious Game en sécurité sont d'ores et déjà multi plateformes. La gamification est donc l'une des clés de la sensibilisation à la cybersécurité. La question n'est pas là. La grande interrogation est plus de savoir jusqu'où il faut aller ?

Par exemple, l'intérêt d'un Serious Game est d'avoir la possibilité de jouer le « méchant ». Pour faire comprendre qu'il est facile de voler des informations ou d'espionner son collègue de travail, il faut montrer par une démonstration en direct et en quelques minutes. Les Serious Game permettent de se mettre à la place du malveillant afin de faire comprendre à quel point, il est facile d'attaquer et par conséquent facile d'être une victime. Or, en France, nous n'aimons pas trop donner de « mauvaises idées » aux utilisateurs. On sent de la résistance. C'est différent dans les pays anglo-saxons qui sont plus offensifs. Malgré tout, cela commence petit à petit en France, par exemple avec le jeu de plateau développé par la Réserve Citoyenne Cyberdéfense où, les joueurs peuvent adopter des stratégies plus ou moins agressives. C'est l'un des enjeux des années à venir.

Cyberstrategia

Jeu de plateau sur la cyberguerre de la Réserve Citoyenne Cyberdéfense.

Gratuit et destiné aux entreprises

Keep an Eye Out

Serious Game du CIGREF qui propose à chaque joueur de devenir « l'ange gardien » d'un salarié de l'entreprise.

Payant destiné aux entreprises.

Crisis Manager

Serious Game de Crisotech pour la sensibilisation à la gestion de crise (évaluation des compétences des collaborateurs).

Payant destiné aux entreprises

Keep an Eye Out

Jeu d'influence de France 5 qui propose une expérience inédite pour explorer de l'intérieur le monde de la communication de crise

Gratuit et tout public.

http://jeu-d-influences.france5.fr/

■ Vis-à-vis de cela, peut-on dire que la gamification s'impose petit à petit en France ?

Honnêtement, je ne pense pas que la gamification s'impose. Selon moi, le terme est trop fort. Je dirais plutôt qu'elle a tendance à gagner du terrain, par exemple dans les processus de recrutement, et n'en perdra pas. Mais pour l'instant, dans le domaine de la sécurité, seul le jeu de rôle « s'impose » véritablement, pour la gestion de crise notamment. C'est indéniable. Nous n'avons jamais trouvé mieux pour simuler une crise que de faire un jeu de rôle.

Outre cet exemple, nous restons donc pour l'instant sur une logique pionnière. Nous savons que cela marche mais, aucune logique de gouvernance s'appuyant sur les Serious Game n'est mise en place. Il s'agit la plupart du temps d'une « brique » ludique ajoutée à des solutions déjà mises en place. Ce n'est pas un passage obligé. Il y a encore beaucoup de réticences. Il y a toujours un public réfractaire. Dans l'entreprise, beaucoup de collaborateurs pensent encore que jouer est une perte de temps. D'autres assimilent encore le fait de jouer à de l'infantilisation. Ce n'est pas une voie royale qui s'ouvre aux Serious Game. Néanmoins, au vue de réactions positives face à la gamification et au succès grandissant des Serious Game, tous les signaux sont au vert. ■

« Je pense que la gamification sera à terme de plus en plus incontournable en matière de sensibilisation. Il me semble impossible d'échapper à ce phénomène dans notre société de la dématérialisation et du tout connecté»

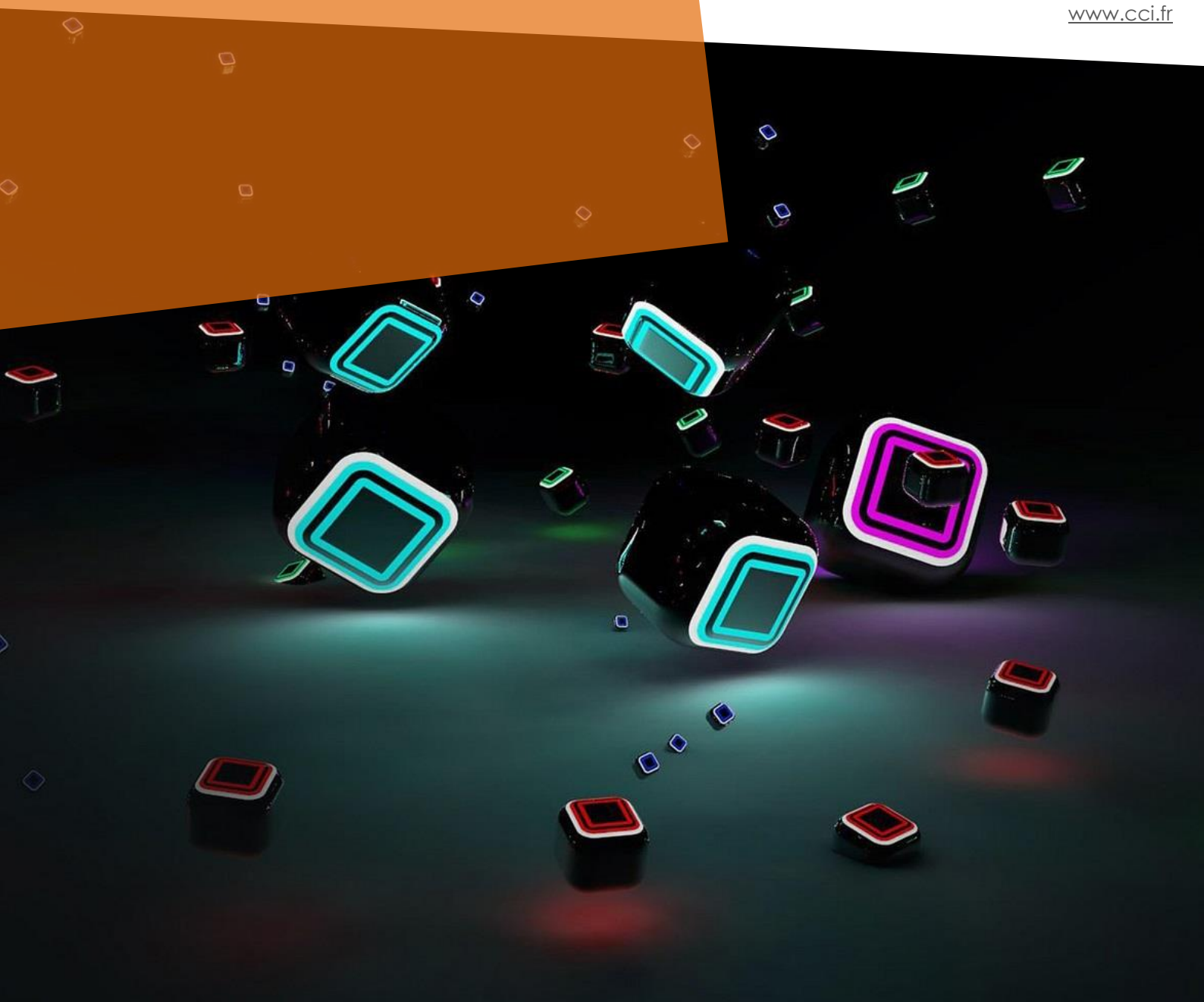
CCI FRANCE

Contact :

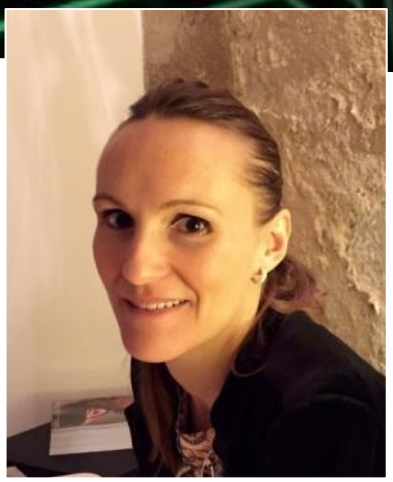
Thibault RENARD
Responsable Intelligence Economique

T.RENARD@ccifrance.fr

www.cci.fr



LES CHEFS D'ENTREPRISES FACE À LA CYBERMENACE : CONSEILS ET BONNES PRATIQUES



Bernadette LEROY | Criminologue et experte en Intelligence Economique et Protection des entreprises. Présidente de la société AESATIS et de l'Association de Criminologie du Bassin Méditerranéen.

Selon la définition du Guide de la Sécurité Economique de la Préfecture de Seine Maritime, le patrimoine de l'information représente « *l'ensemble des moyens actifs et passifs assurant la sauvegarde du patrimoine industriel, informationnel et immatériel de l'entreprise ainsi que ses activités* ». Il est vital pour toute entreprise d'intégrer la protection de l'information dans la stratégie globale de mise en sécurité / sûreté de l'entreprise. Aucune ne peut prendre le risque de mettre en péril les données confidentielles en sa possession et la confiance que l'on lui porte. De plus, une organisation qui met en péril les données de ses salariés ou clients peut en être tenue pour responsable devant la justice si, elle n'a pas mis en œuvre des mesures suffisantes pour les protéger. Ce vif souci et intérêt est d'autant plus décuplé aujourd'hui au regard de la dépendance des entreprises aux moyens de traitements et d'échanges numériques. De nombreuses menaces endogènes et exogènes peuvent porter atteintes et nuire à toute organisation. En effet, aucune entreprise n'est exempte d'attaque. Aucune ne peut se vanter d'être intouchable, inattaquable, inébranlable. Il est établi que le risque zéro n'existe pas. Toute entreprise est une victime potentielle. En entreprise, le niveau de sécurité / sûreté s'évalue à son maillon le plus faible. Négligence, ignorance, méconnaissance des risques, naïveté, malveillance… Les origines des menaces sont grandes. Autant de comportements humains qui ouvrent les portes aux attaques souvent très lourdes de conséquence pour l'entreprise.

Le système d'Information dans une entreprise couvre l'ensemble du périmètre informationnel de l'entreprise. Mais ce serait avoir une vision restrictive de penser qu'il se résume au cybermonde. Le système d'Information numérique est un maillon de la chaîne du patrimoine informationnel de l'entreprise. Or, pour le sécuriser, il est important d'avoir une vision globale du système d'Information de l'entreprise. La mise en place un système de management de la sécurité des systèmes d'Information numériques nécessite donc un système transversal et pluridisciplinaire. Plusieurs phases sont nécessaires pour la mise en place d'une bonne stratégie de sécurité / sûreté du patrimoine informationnel imbriqué au cybermonde de l'entreprise. Elle aura pour effet la mise en place de plusieurs dispositions au travers de diverses actions :

■ Une Politique de Sécurité du Système de l'Information (PSSI) :

Le PSSI reflète la vision stratégique et sécuritaire d'une organisation en matière de sécurisation des systèmes d'Information numériques. Elle constitue un ensemble formalisé des éléments stratégiques, des directives, des procédures, des codes de conduites, des règles organisationnelles et techniques ayant pour but la protection du système d'Information. Il représente véritablement un plan d'actions définies pour maintenir un niveau minimum de sécurité. La démarche de réalisation de cette politique est basée sur une analyse des risques en matière de sécurité des systèmes d'Information.

Le PSSI constitue le principal document de référence en matière de SSI de l'organisme. Elle en est un élément fondateur définissant les objectifs à atteindre et les moyens accordés pour y parvenir. Il doit être diffusé à l'ensemble des acteurs du système d'Information

(utilisateurs, exploitants, sous-traitants, prestataires…). Elle constitue alors un véritable outil de communication sur l'organisation et les responsabilités SSI, les risques SSI et les moyens disponibles pour s'en prémunir. La PSSI vit et évolue avec le système d'Information. Elle doit être contrôlée chaque année.

■ **Un processus de pilotage et de management du Système de Management de la Sécurité de l'Information (SMSI) ainsi qu'une organisation spécifique :**

L'installation d'un Système de Management de la Sécurité de l'Information ne se déroule pas en un temps unique et demande une organisation particulière et surtout la désignation et la mise en place d'un comité de pilotage. Un système d'information vit. Il est en mouvance. Il est donc important de rester en veille permanente. Celle-ci repose sur une homogénéité et une cohésion des différents services de l'entreprise : juridique, assurance, Ressources Humaines, accueil, commerciaux, administratifs... Pour qu'une telle politique puisse vivre, l'adhésion à 100% et la mobilisation totale de tous les acteurs de l'entreprise sont indispensables pour garantir son succès. La protection des systèmes d'Information de l'entreprise passe par une responsabilité de tous les acteurs de l'entreprise. Mobilisation, adhésion et implication sont donc les maîtres mots de cette organisation spécifique à établir dans l'entreprise en signe d'engagement.

■ **Un corpus documentaire de sécurité (référentiels, procédures et instructions, inventaire des actifs, cartographie des risques) :**

Il s'agit de faire un état des lieux de l'entreprise en matière de sécurité. Cela passe par la réalisation d'une analyse des risques qui va permettre à l'entreprise de se situer et d'évaluer son niveau de risque. Il convient donc dans un premier temps et dans un souci de visibilité d'analyser les risques afin de déceler les failles possibles et les vulnérabilités afin de cartographier autrement dit de hiérarchiser les risques dans le but de mettre de mettre en place des dispositifs procéduraux, organisationnels et techniques en adéquation avec le niveau de risque de l'entreprise.

En complément, adopter des règles de conduites simple au quotidien est une solution voire un impératif de la part des collaborateurs aujourd'hui. Ce sont des gestes relevant souvent du bon sens qu'il suffit de connaître afin de les appliquer. Une énumération des bonnes pratiques peut faire l'objet de la rédaction d'une charte éthique et/ou de bonne conduite, d'une charte de sécurité économique ou une charte d'utilisation du patrimoine informationnel de l'entreprise. Cela énumère les principes essentiels et les comportements attendus en interne. C'est un document qui doit de façon claire et synthétique définir le réseau dans son activité, sa composition, ses objectifs, son organisation et ses modalités de participation et d'adhésion de ses membres. La charte est avant tout un outil de cohésion interne. Elle permet de se mettre d'accord à tout moment sur les objectifs, les droits et les devoirs de chacun au sein du réseau. Outre, la mise en place de charte, il est important d'écrire des procédures, de les mettre en place, d'informer et sensibiliser régulièrement les collaborateurs mais aussi de vérifier la bonne application de celles-ci.

Quelques conseils simples

CONTROLER ET SECURISER LES VISITES ET SEJOURS EN ENTREPRISE

-Contrôler l'identité des visiteurs,
-Port de badge obligatoire du personnel,
-Eloignement du standard de la salle d'attente,
-Organisation de parcours de visite,
-Encadrement du personnel non permanent.

SE MEFIER DES INTERLOCUTEURS INCONNUS AU TELEPHONE

-Vérification d'identité préalable et de la finalité de l'appel,
-Demande d'envoi de la demande par mail ou courrier (preuve écrite),
-Eviter de donner beaucoup de détails par téléphone lors de la conversation.

RESTER VIGILANT LORS DES DEPLACEMENTS PROFESSIONNELS

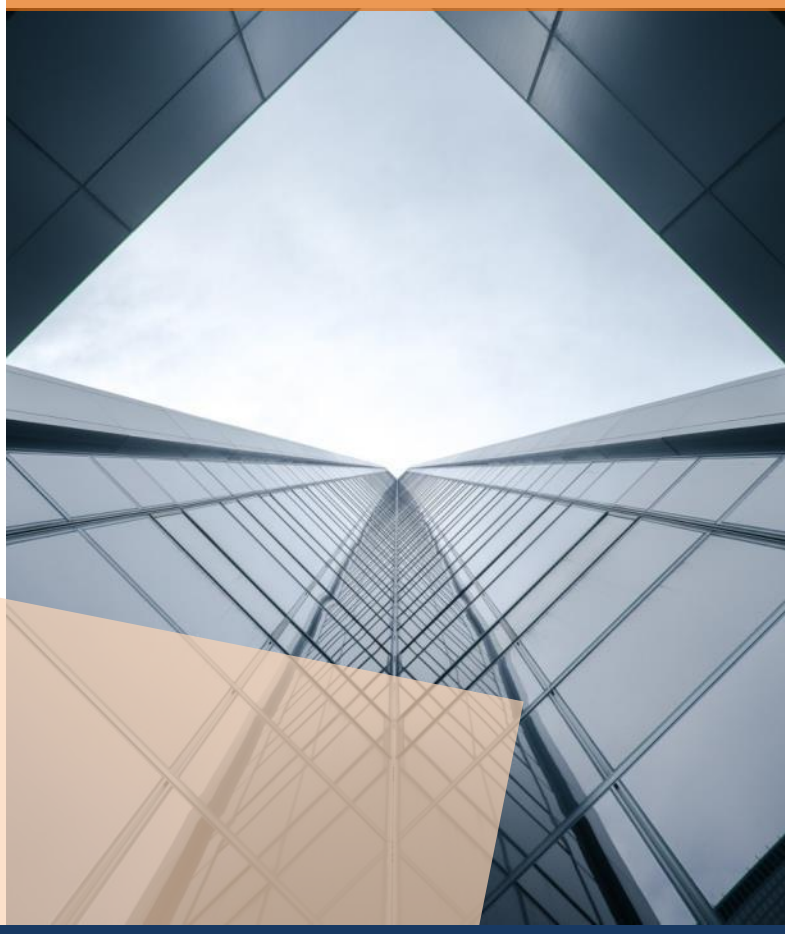
- Eviter d'avoir des conversations professionnelles dans les transports en commun et les lieux publics
- Eviter de sortir des documents confidentielles ou stratégiques de l'entreprise hors de celle-ci
- Ne pas se connecter au réseau wifi gratuit des hôtels
- Prévoir un ordinateur réservé exclusivement aux déplacements qui sera vide avant chaque départ

CONNAITRE LES BONNES PRATIQUES DE SECURITE INFORMATIQUE

-Choisir des mots de passe de huit caractères alphanumériques et les renouveler régulièrement,
-Stocker les informations sensibles sur un poste non connecté à Internet,
-Mettre à jour régulièrement les antivirus, firewall et anti-spams,
-Détruire les documents sensibles et ne pas les jeter tels quels,
-Effacer la mémoire des photocopieurs après usage.

RESPECTER LES REGLES DE SECURITE DE L'ENTREPRISE

-Vérifier les diplômes et expériences des candidats lors de recrutement,
-S'assurer du bon fonctionnement de la fermeture des locaux,
-Regrouper et protéger les clés de service,
-Rester discret sur les mesures de protection et les dispositifs d'alarme mis en place.



■ **Une méthode d'analyse et de traitement de risques qui va permettre d'établir un plan d'actions correctives et préventives et une revue des actions :**

Partant du postulat qu'une entreprise est en mouvance perpétuelle, il apparaît évident qu'après avoir analysé ses risques, l'entreprise doit respecter le principe d'une amélioration continue. Le risque zéro n'existe pas, toute organisation a pour engagement d'évaluer ses risques afin de les faire diminuer le niveau de risque à un niveau le plus acceptable possible. Dans cette perspective, établir une réelle méthode continue d'analyse et de traitement des risques apparaît comme tout aussi important que d'établir son plan d'action et de contrôle.

■ **Un suivi d'indicateurs et tableaux de bord d'incident :**

Dans le cadre de notre sujet, un incident serait « *un ou plusieurs événements intéressant la sécurité de l'information indésirable(s) ou inattendu(s) présentant une forte probabilité de compromettre les opérations liées à l'activité de l'organisation et de menacer la sécurité de l'information* » (Définition de la norme ISO 27 000 – sécurité de l'information). Quelle que soit l'approche, il est important en entreprise d'établir un système de suivi organisé des incidents de sécurité informatique et des dispositifs de surveillance. Cette gestion a pour objectif la détection, la compréhension et le traitement des incidents (à priori et à posteriori). Cela permet ensuite de mettre en place des dispositifs de prévention.

■ **Un Plan de Continuité d'Activité (PCA) :**

Un Plan de Continuité d'Activité (PCA) a pour objet de garantir à une organisation publique ou privée la reprise et la continuité de ses activités à la suite d'un sinistre ou d'un événement perturbant gravement son fonctionnement normal. Il a par conséquent pour mission de décliner la stratégie et l'ensemble des dispositions qui sont prévues pour garantir à une organisation la reprise et la continuité de ses activités à la suite d'un sinistre ou d'un événement perturbant gravement son fonctionnement normal. Il a pour finalité de permettre à l'organisation de répondre à ses obligations externes (législatives ou réglementaires, contractuelles) ou internes (risque de perte de marché, survie de l'entreprise, image…) et de tenir ses objectifs.

■ **Un dispositif de surveillance et d'alerte, de traitement et de suivi des incidents de sécurité :**

Etablir une méthode d'analyse et de traitement du risque dans le cadre d'une Politique de Management de la sécurité numérique va permettre de pouvoir être dans une rapidité de réaction afin de limiter les effets néfastes sur l'entreprise.

■ **Un dispositif de sensibilisation et de formation dédié.**

Ces quelques pistes d'action et de réflexion en matière de sécurité du système d'Information et de bonnes pratiques sont totalement inefficaces sans un socle minimum de sensibilisation, de communication et de formation de l'ensemble des collaborateurs de l'entreprise. La sensibilisation est un impératif majeur dans des entreprises 4.0 aujourd'hui où, la digitalisation et la transformation numérique sont au cœur des enjeux stratégiques de l'organisation interne.

La nécessité de sensibiliser et de former les collaborateurs sur les questions de sécurité informatique est aujourd'hui plus que jamais d'actualité. Face à des cybercriminels qui ne cessent de se perfectionner, les collaborateurs de l'entreprise doivent également pouvoir faire face et lutter à armes égales.

Garantir un système d'Information numérique sécurisé et de confiance, c'est garantir la confidentialité, l'intégrité, la disponibilité et la non répudiation des données de l'entreprise. Une politique de sécurisation des systèmes d'Information apparaît donc aujourd'hui comme un engagement, vecteur essentiel de qualité et de communication dans l'entreprise. ■

Bernadette LEROY

ACBM
ASSOCIATION DE CRIMINOLOGIE DU BASSIN MEDITERRANEEN

Association de Criminologie du Bassin Méditerranéen

www.acbm-paca.com

AESATIS

AESATIS – Conseil en sécurité et sûreté des entreprises

04 42 46 20 88
www.aesatis.com

SECEM MAGAZINE

Le magazine sur la Sécurité Economique et la Compétitivité des Entreprises en Méditerranée

Revue numérique éditée par l'Association de Criminologie du Bassin Méditerranéen (ACBM), située 79bis avenue de l'Europe, 13127 VITROLLES.

contact@acbm-paca.com

www.acbm-paca.com

ACBM
ASSOCIATION DE CRIMINOLOGIE DU BASSIN MEDITERRANEEN

Trimestriel sur la Sécurité Economique et la Compétitivité des Entreprises en Méditerranée

ISSN : 2429-5167
Directrice de la publication : Bernadette LEROY
Rencontres et interviews : Claire HANASTASIOU

L'ensemble des numéros sont téléchargeables sur le site www.secem.fr, rubrique SECEM Magazine.

Prochain numéro :

Dossier spécial
Attractivité des territoires

PARTENAIRES

AESATIS

ACSE
ASSOCIATION POUR LA COMPÉTITIVITÉ ET LA SÉCURITÉ ÉCONOMIQUE

Derniers numéros du SECEM Magazine

Numéro 7 ■ Janv. | Mars 2016
DOSSIER SPECIAL INTELLIGENCE ECONOMIQUE
L'intérêt de mettre en place une stratégie d'Intelligence Economique en entreprise

Numéro 6 ■ Nov. | Déc. 2015
DOSSIER SPECIAL FRAUDE
Focus sur la fraude interne en entreprise

Numéro 5 ■ Sept. | Oct. 2015
DOSSIER SPECIAL TERRORISME
Les entreprises, nouvelles cibles du terrorisme

TELECHARGER
LES AUTRES NUMEROS