Cybersecurity Trends

Édition spéciale CMCS 2021



CHARENTE-MARITIME CYBER SÉCURITÉ
— CMCS-CONNECT.FR —

Multiplication des risques : partage des connaissances !

Un congrès atypique et solidaire pour relever les défis actuels et prospecter de nouveaux secteurs : sport, tourisme, agro-alimentaire, sans oublier les territoires…

CHARENTE-MARITIME CYBER SÉCURITÉ
CMCS 2021

CMCS

L'événement du Grand Ouest
dédié à la cybersécurité
des entreprises et des collectivités

Du 11 au 14 octobre 2021 à La Rochelle

CMCS, l'événement grand public sur la cybersécurité, vous donne rendez-vous pour 4 jours de conférences, de tables rondes et de témoignages autour de thèmes aussi variés que la prévention des risques cyber, la protection des données ou la sécurité des systèmes d'informations. Pour cette 4ème édition, des secteurs d'activités seront mis à l'honneur comme le SPORT, en partenariat avec le Comité Départemental Olympique et Sportif, le TOURISME et l'AGRO-ALIMENTAIRE.









Un congrès atypique et solidaire

Pour relever les défis actuels
et prospecter de nouveaux secteurs :

- sport
- agro-alimentaire
- tourisme
- sans oublier les territoires...

Index

3	**Éditorial : CMCS 2021 : nouveaux enjeux, nouvelles méthodes pour un congrès atypique.** Auteur : Didier SPELLA
7	**Préface: Chacun pour tous, tous pour chacun !** Auteur : Gal Marc WATIN-AUGOUARD
9	**Quand le citoyen choisit de devenir un simple objet jetable… Partout dans l'UE, le mépris du pouvoir élu engendre la méfiance envers l'ensemble des services de l'Etat…** Auteur : Laurent CHRZANOVSKI
14	**Quand le numérique nous ramène au paléolithique.** Auteur : Delphine CHEVALLIER
18	**50 nuances d'Identité Numérique.** Auteur : Stéphane GASCH
22	**Savoir communiquer par temps de crise !** Auteur : Jean-Marc BONNET
24	**La cybercriminalité : un problème de management bien plus que de technologie.** Auteur : Nathalie MALICET
28	**Cyberdéfense : mettre l'humain au cœur du dispositif.** Auteur : Dominique MAÏANO
32	**L'agriculture, un secteur stratégique exposé à la cybercriminalité.** Auteur: Stéphane MORTIER
36	**Exemple pratique : cyber-attaque chez Cérèsia (année 2020).** Auteur : Olivier BACON
38	**Acteurs du tourisme : protégez vos données personnelles et celles de vos clients !** Auteur : Lisa CROIZET
40	**Quels business models pour le tourisme de demain ?** Auteur: Stéphane MORTIER
44	**De l'impérieuse nécessité de s'appuyer sur un datacenter vérifié, de confiance et soumis à la législation souveraine de l'État de domicile de ses clients. Interview croisée avec Eric ARBARETAZ et Okan TUREDI.** Auteur : Delphine CHEVALLIER
52	**Risques, cybersécurité et conformité.** Auteur : Benoit LACOUR
55	**Cybersécurité et ISO 27001 : à chacun son parcours.** Auteur : Brice GILBERT
57	**Du DSI au CDO : une gestion stratégique des données.** Auteur : Jacques-Louis KESZLER

Index

59	**L'évolution du poste de RSSI, de responsable informatique à directeur de la cybersécurité…** Auteur : Pierre VENOT
62	**Le CLUSIF, Association de professionnels de la sécurité de l'information, propose son Espace CoTer pour fournir des réponses pérennes aux problèmes rencontrés par les collectivités territoriales et assimilées.** Auteur : Damien ALEXANDRE
64	**Un club des RSSI pour renforcer la protection des Collectivités Territoriales (COTER) face aux cybermenaces.** Auteur : Philippe STEUER
67	**Confiance numérique des territoires : mutualiser pour faire face aux cyber-risques.** Auteur : Benoît LIÉNARD
69	**La prévention de la cybercriminalité au niveau d'un territoire : l'exemple du reseau des référents cybermenaces de Nouvelle Aquitaine.** Auteur : Paul BOUSQUET
72	**Un nouvel impératif académique : faire comprendre aux étudiants les enjeux de la sécurité digitale.** Auteur : Nathan PRUDHOMME
74	**Pour une professionnalisation du traitement des plaintes en matière de cyber criminalité à la Police cantonale de Genève.** Auteur : Patrick GHION
77	**Cybermalveillance.gouv.fr : un concept novateur dédié à la prévention et l'assistance aux victimes de cybermalveillance.** Auteur : Jérôme NOTIN
80	**CROE, le guide pour la cyber-résilience du monde de la finance.** Auteur : Yahya ARROUBAT
85	**L'industrie numérique au cœur de la PFUE.** Auteur : Sébastien GARNAULT
88	**L'antivirus ne vous protège pas. Il laisse des fichiers vous infecter. Du nouveau dans le paysage français : Viruscamp.** Auteur : Stéphane THOREL
91	**Quand le sport abrite le crime : pari sportif en ligne, blanchiment et corruption.** Auteur: Stéphane MORTIER
94	**Vestiaire : nouvel espace de violence.** Auteur : Tristan IZAMBARD
96	**Sport : Les cybercriminels attaquent même les petits clubs ! Les solutions d'Asklépian.** Auteur : Fabien FERNANDEZ
100	**SportTrooper, un produit onepoint transformant les entraînements sportifs.** Auteur : Benoit LACOUR

CHARENTE-MARITIME
CYBER SÉCURITÉ
— CMCS-CONNECT.FR —



CMCS 2021: nouveaux enjeux, nouvelles méthodes pour un congrès atypique.



Auteur : Didier SPELLA

La crise COVID nous a plongé dans une triste réalité que nous avions oubliée depuis plusieurs décennies. Nos sociétés nous avaient construit un monde où la maîtrise du risque semblait totale. En supprimant les mauvaises "surprises", la sérénité était quasi-totale. Certes, le climat commençait à nous poser quelques doutes sur le futur, mais il semblait que nous avions un peu de temps pour régler ces problèmes.



Cette crise a remis en lumière quelques concepts simples : le risque zéro n'existe pas, le risque est un élément qui doit être partagé, etc..

D'autre part, nous avons oublié que, généralement, les crises sont génératrices de crises. Aussi, nous constatons qu'à cette crise sanitaire une crise cyber s'est développée, encouragée par des comportements que nous n'avions pas intégrés, notamment le télétravail poussé à son extrême.

Nos organisations peu ou pas préparées à ces crises doivent être en mesure d'y faire face et surtout d'en limiter les impacts. Pour ce faire, elles doivent être en mesure comme le citoyen que nous sommes, d'identifier les risques liés à chacune de nos activités dont certaines vont être analysées pendant les 4 jours de notre colloque.



En effet, pour la quatrième année consécutive, Charente-Maritime Cyber Sécurité (CMCS) se déroulera à La Rochelle du 11 au 14 octobre 2021.

BIO

Président de Mirat Di Neride, Expert en stratégie des entreprises et en cybercriminalité, Responsable Bureau CLUSIR - Nouvelle Aquitaine Ouest, Didier Spella, ancien officier supérieur de l'Armée de l'Air, est le co-fondateur du congrès PPP Charente-Maritime Cyber Sécurité. Il a vu évoluer les différents concepts qui régissent aujourd'hui le cybermonde. Ses connaissances en sécurité tant analogiques que numériques, son expérience d'analyse de risques et ses expertises auprès d'une compagnie américaine, lui ont permis de se positionner en tant qu'expert en définition de stratégie de sécurité. Confronté aux attaques cyber de plus en plus importantes et intrusives dans nos modes de vie, il étudie spécialement les risques encourus par la population en général et, plus particulièrement, les menaces qui pèsent sur les TPE et les PME.

Comme les années précédentes, nous traiterons avec nos différents intervenants des impacts socio-économiques de la cyber criminalité. Nous avons sélectionné pour cette année trois thèmes, complétés par des problématiques transverses afin de couvrir au mieux nos réflexions.

Afin de mieux communiquer avec nos participants et leur apporter ainsi un éclairage sur ce que seront les débats, nous avons sollicité nos intervenants pour qu'ils rédigent un article concernant soit leur structure et/ou les concepts qu'ils développeront lors de leur intervention.

La plupart d'entre eux se sont prêtés à cet exercice avec beaucoup d'entrain et nous sommes ainsi en mesure de vous proposer en avant-première de CMCS cet ouvrage collectif qui vous permettra de mieux appréhender ce que nous allons vous proposer pendant ces quatre journées.







Les trois domaines que nous traiterons cette année correspondent à des problématiques certes régionaux et nationaux mais surtout qui concernent la majorité de la population : Il s'agit du sport, de l'agro-alimentaire et du tourisme.

Comme vous pouvez le constater, ces domaines ne peuvent que nous interpeler car ils font vraiment partie de notre vie quotidienne. L'agro-alimentaire nous permettra d'aborder ces problématiques de notre alimentation quotidienne. Le sport sera abordé à la fois dans sa dimension activité sportive mais aussi dans ses aspects compétitions et sport de haut niveau. Les enjeux financiers et technologiques qui y sont liés sont des domaines très sensibles aux attaques cyber. Quant au tourisme, là aussi, nous pouvons constater que son évolution se fait au travers de nouvelles technologies numériques et de leur usage.

Cependant, nous ne pouvions pas évoquer ces problématiques sans y inclure le domaine public, notamment au travers des territorialités.

Au-delà des ces thèmes, nous commencerons aussi à réfléchir sur les enjeux sociétaux que nous amène le cyber monde.

Au regard de ce qui se passe aujourd'hui, sommes-nous dans une phase d'évolution ou plutôt allons-nous plus vers une véritable révolution ?

Si nous traitons le cybermonde dans une approche tri-dimensionnelle, à savoir l'Information, la Gouvernance et la Technologie, nous ne pouvons que constater que les deux premières dimensions sont plus dans un aspect de révolution.

En effet, aujourd'hui, l'Information qui a toujours été un instrument de pouvoir, était "générée" par le pouvoir. Or aujourd'hui, grâce aux technologies et usages qui en sont faits, l'Information provient de toute part. Elle permet ainsi à des groupes non constitués de devenir des organes de pouvoir et d'influence. De plus, l'intégrité de cette Information n'est plus garantie car non filtrée et non vérifiée.

Nous pouvons aussi faire la même réflexion concernant la gouvernance qui, là aussi et nous ne pouvons que le constater, échappe aux structures établies. Cette gouvernance se crée naturellement en fonction des réseaux et des communautés sans que pour cela il émane de ces structures une direction et des responsables, au sens où nous l'entendons aujourd'hui. A cela, nous pouvons y ajouter l'absence de territorialité. Cette complexité remet en cause nos schémas habituels.

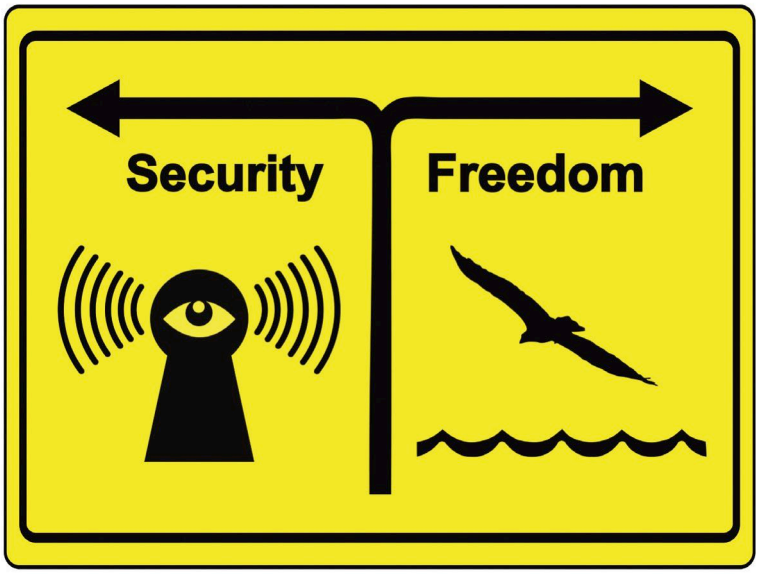
Concernant la dimension technologique, si elle est bien dans un cycle d'évolution, les usages qui en sont faits ne sont pas complètement en accord avec ce qui était prévu. Ces usages mal maîtrisés nous obligent

à revoir comment nous devons vivre dans le cyber monde.

Il reste aussi un problème récurrent qui, là aussi, est en train de positionner nos sociétés. Afin d'assurer que nous évoluions dans un cyber monde à risque maîtrisé, nous devrons nous poser des questions sur un équilibre fondamental entre liberté et sécurité.

Quelle sera notre modèle de société ? Sparte ou Athènes, cette réflexion fera notamment l'objet d'une agora le mardi après-midi.





Ces véritables révolutions nous amènent à réfléchir sur des problèmes que nous pourrions aborder l'année prochaine, tel le thème "ExpertCyber, mythe ou réalité", thèmes qui nous amènera alors à réfléchir sur les formations.

Cette année donc CMCS2021 sera encore un événement atypique par les thèmes que nous y aborderons : par les méthodes que nous utiliserons, par la richesse et la diversité de nos intervenants. Et je vous invite maintenant à lire ces articles et à venir entendre les intervenants à notre colloque du 11 au 14 octobre. ■



Chacun pour tous, tous pour chacun !

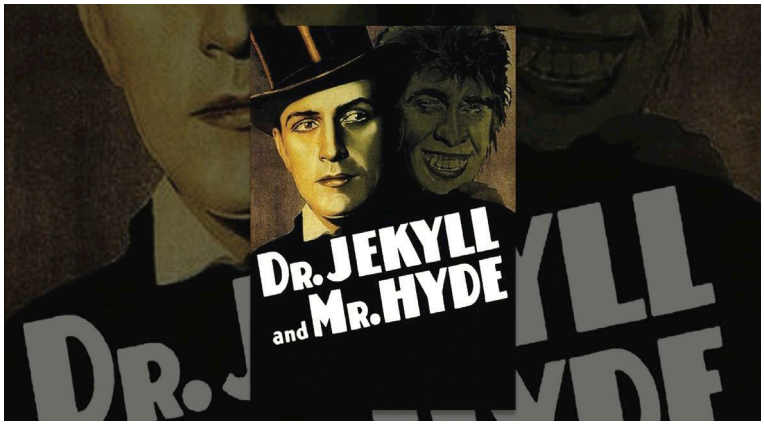


Centre de recherche de l'EOGN

FIC — FORUM-FIC.COM —

Auteur : Marc WATIN-AUGOUARD

La crise de la COVID-19 a mis en lumière la place du numérique dans notre vie quotidienne. Sans internet et toutes ses applications, la pandémie aurait conduit au chaos humain, social et économique. Comment maintenir les liens amicaux et familiaux, comment envisager le télétravail sans le "réseau des réseaux" qui a été un facteur essentiel de notre résilience. Mais le "Docteur Jekyll" vient avec "Mister Hyde".



Le développement des connexions, l'augmentation massives des contenus véhiculés par internet, l'isolement lié au confinement ont libéré l'action des prédateurs. Une toute autre pandémie, illustrée notamment par l'explosion du nombre de rançongiciels, marque une inflexion exponentielle dans la croissance déjà forte du nombre de cyberattaques. Les pionniers de la cybersécurité sont rejoints par les incrédules d'hier, désormais conscients des enjeux, même si beaucoup pensent encore que les cyberattaques n'atteignent que les autres. Le télétravail a obligé nombre d'entreprises, d'administrations ou de collectivités territoriales "atomisées" à revoir en urgence la sécurité de leurs systèmes d'information.

Celle-ci, hier l'apanage des RSSI et DSI, est désormais davantage diffuse au sein des organisations. Espérons que cette prise de conscience se prolonge et s'amplifie ! Pour cela, il faut des "piqûres de rappel", des moments forts qui favorisent la "révélation" et apportent à ceux qui sont convaincus de la matière pour poursuivre leur action "d'évangélisation".

BIO

- Fondateur et Codirecteur, Forum international de la cybersecurité – FIC
- Directeur, Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale (CREOGN)
- Ancien inspecteur général des armées-gendarmerie
- Général d'armée (2008)
- Général de corps d'armée (2007)
- Général de division (2006)
- Commandant, Gendarmerie pour la zone de défense Nord (2005 – 2008)
- Commandant, Région de gendarmerie du Nord-Pas-de-Calais
- Conseiller pour la gendarmerie, Cabinet de Dominique de Villepin (2004 – 2005)
- Général de brigade (2003)
- Conseiller pour la sécurité, Cabinet de Nicolas Sarkozy (2002 – 2004)
- Commandant de la légion de gendarmerie départementale de Champagne-Ardenne (2000 - 2002)
- ENSEIGNEMENT : Chargé de cours en droit, Universités Panthéon-Assas (Paris II), René Descartes (Paris V) et Aix-Marseille III-Méditerranée.



Charentes Maritimes Cybersécurité s'inscrit dans ces moments forts, ces rendez-vous attendus, qui rythment l'année et permettent à la communauté des "gens du cyber" de se retrouver pour partager leurs connaissances, leurs expériences. On ne mesure pas assez l'importance d'un tel événement qui contribue à une véritable mission de service public. CMCS a une vocation régionale, ce qui est loin d'être péjoratif sous la plume du fondateur du FIC, événement devenu la référence en Europe.

L'ancrage dans les territoires est absolument essentiel, car ce sont des espaces naturels pour décloisonner public et privé, pour créer des solidarités, pour construire une trame de résilience. Parler des territoires alors qu'Internet est réputé sans frontière peut paraître paradoxal. Il n'en est rien, bien au contraire. Notre cybersécurité a été construite dans l'urgence, depuis plus d'une dizaine d'années, avec une approche verticale, sectorielle, centralisée. Aujourd'hui, il est nécessaire d'ajouter une démarche horizontale, territoriale, là où se tissent des liens humains, là où la pratique quotidienne invite à ouvrir, voire effacer, les frontières qui peuvent exister et qui ne peuvent plus perdurer, sauf à avancer seul sur un champ de bataille qui élimine les solitaires. Les territoires accueillent nombre de PME, TPE, ETI, collectivités territoriales, établissements publics (hôpitaux par exemple), dont la SSI est limitée en raison de leur taille, de leur capacité financière. Pourtant, ces personnes morales de droit public ou privé sont souvent les premières cibles de prédateurs, notamment en raison de leur fragilité et de leur relative dispersion.



Nous ne pouvons rester indifférents à la multiplication d'atteintes graves qui peuvent annoncer la mort d'entreprises, la mise en danger de patients, la divulgation de données sensibles. Créer les conditions d'un dialogue, d'un partage des expériences est aujourd'hui une ardente obligation. Didier Spella l'a compris. Je suis heureux de l'accueillir chaque année au FIC avec CMCS ; je suis heureux d'envisager une coopération étroite avec l'Institut National pour la Cybersécurité et la Résilience des Territoires (INCRT) que je préside.

Je suis malheureux d'être absent pour cette édition, étant "capturé" par les activités de cybersécurité que je conduis au sein de l'IHEDN. Mais ce n'est que partie remise ! L'année cyber qui s'ouvre sera riche en évolutions. En janvier la France prendra la présidence du Conseil de l'Union européenne (PFUE) et devra accentuer le souffle d'une Europe de la cybersécurité qui commence à se révéler. Nous aurons donc l'an prochain à tirer les enseignements des progrès enregistrés. Nous pourrons avec le recul nécessaire observer les mutations liées à un télétravail qui devrait se prolonger, même en plus faible intensité, modifier l'aménagement du territoire, grâce à l'achèvement du plan France Très Haut Débit, le déploiement de la fibre, de la 5G. L'hyperconnexion est en marche accélérée et très vite vont devenir réalité les smart cities ou smart countries qui vont exiger une cybersécurité collective et collaborative. Encore une raison de plus pour légitimer le CMCS et inciter les acteurs régionaux, dont les partenaires, à le rejoindre, à accompagner et amplifier son rayonnement.

IN.CRT
CYBER – RESILIENCE – TERRITOIRES



Cet ouvrage collectif, dirigé par Laurent Chrzanovski, permet de contribuer à la doctrine, avec le sens positif du terme. Les paroles s'envolent, les écrits demeurent ! cet adage trouve toute sa raison d'être, même à l'heure du tout numérique, car le verbe précède l'action, les idées influencent et structurent les comportements. Cette publication aura un lectorat qui dépasse nos frontières, en particulier en Italie, en Roumanie, en Suisse. C'est bien la preuve du rayonnement de CMCS, bien au-delà du cadre rochelais.

"Chacun pour tous, tous pour chacun", ce slogan pourrait être celui de CMCS. "Chacun pour tous", intervenant ou auteur apporte aux autres le message dont il est le porteur, exprime son "acte de foi" pouvant servir de référence. "Tous pour chacun", telle est la mission que les participants au colloque doivent accepter en ayant la conviction que la cybersécurité ne peut se concevoir avec égoïsme. ■



Quand le citoyen choisit de devenir un simple objet jetable...

Partout dans l'UE, le mépris du pouvoir élu engendre la méfiance envers l'ensemble des services de l'Etat...



Auteur : Laurent Chrzanovski

Relire tous les articles des derniers numéros de notre magazine nous laisse un goût amer. Nous avons l'impression de vivre dans un cercle vicieux sans fin. En bref, tous les points extrêmement importants mentionnés par les meilleurs experts... sont exactement les mêmes que ceux que nous traitons depuis dix ans.

Les menaces sont de plus en plus dangereuses chaque jour alors que, paradoxalement, le défi consistant à sensibiliser à la cyber-sécurité et à l'hygiène numérique ainsi qu'à faire appliquer les nouvelles lois et réglementations, défi qui était déjà très difficile, est devenu presque impossible.

Ce faisant, les Européens passeront très rapidement du statut de citoyen à celui de simple objet modifiable, pas même de sujet, appartenant aux géants de la Big Tech. Cette condition pourrait être bien représentée par le dialogue entre Morpheus et Neo dans The Matrix - un scénario écrit il y a vingt ans...



Morpheus : "La Matrice est partout, elle est tout autour de nous, même maintenant dans la pièce où nous nous trouvons. C'est ce que tu vois quand tu regardes par la fenêtre ou quand tu allumes la télévision. Tu le ressens quand tu vas au travail, quand tu vas à l'église, quand tu payes tes impôts. C'est le monde qui a été mis sous tes yeux pour te cacher la vérité."

BIO

Professeur aux Universités, Laurent est titulaire de la chaire d'archéologie et d'histoire ancienne auprès de l'École doctorale et postdoctorale de l'université d'État "Lucian Blaga" de Sibiu. Il enseigne régulièrement dans plusieurs grandes universités européennes. Il est l'auteur/éditeur de 38 livres, de plus d'une centaine d'articles scientifiques et autant d'articles pour le grand public. Dans le cadre de la cybersécurité, ses principaux domaines d'études sont centrés sur la relation entre les comportements humains et le monde numérique ainsi que sur l'assurance de trouver le juste équilibre entre sécurité et vie privée pour les e-citoyens. Membre du cercle d'experts de l'UIT (ONU). Il a fondé et dirige le triptyque de congrès PPP annuels "Cybersecurity-Dialogues" (Roumanie, Suisse et Italie, en partenariat avec plusieurs des plus hautes institutions nationales et internationales compétentes. Dans ce même esprit de partage, il est fondateur et rédacteur de la première revue trimestrielle gratuite de cyber-awareness pour adultes et dirigeants, "Cybersecurity Trends", publiée 3 versions adaptées aux besoins de leur lectorat respectif (Roumanie, Italie, Grande-Bretagne).

Neo : "Quelle vérité ?"

Morpheus : "Que tu es un esclave. Comme tout le monde, tu es né enchaîné, tu es né dans une prison qui n'a pas de barreaux, qui n'a pas de murs, qui n'a pas d'odeur, une prison pour ton esprit."

Les années de pandémie numérique arrivent maintenant....

Le principal effet des confinements et des mesures prises en période de pandémie est que la plupart des citoyens sont, bien plus qu'avant COVID-19, complètement perdus et confus dans leur relation non seulement avec le monde réel, mais surtout avec l'État et le monde numérique.

Les alertes "rouges" proviennent de toutes les disciplines, de tous les domaines, de tous les pays. Mais pour les géants de la technologie, les jours ne sont que *"business as usual"*, sans limites, sans règles, sans lois pour freiner leurs excès... Alors que c'est exactement le moment où, grâce à la mise en œuvre de la 5G, la quatrième révolution industrielle se met définitivement en place.

Nous allons essayer, dans ce court texte, de présenter brièvement les menaces les plus importantes auxquelles nous sommes confrontés, dans une perspective sociale, humaniste et démocratique. Pour cet exercice, nous nous appuierons sur le rapport annuel des jalons de l'IE Center for the Governance of Change (CGC), *"European Tech Insights 2021"*.





Publié exceptionnellement en deux volumes distincts en raison de la période très particulière que nous vivons (Partie I. *Comment la pandémie a modifié notre relation avec la technologie* & Partie II. *Embrasser et gouverner la perturbation technologique*), le rapport met l'accent sur le fait qu'une grande majorité de citoyens européens ont désormais des réactions, des approches et des compréhensions bipolaires de ce qu'ils attendent du monde numérique.

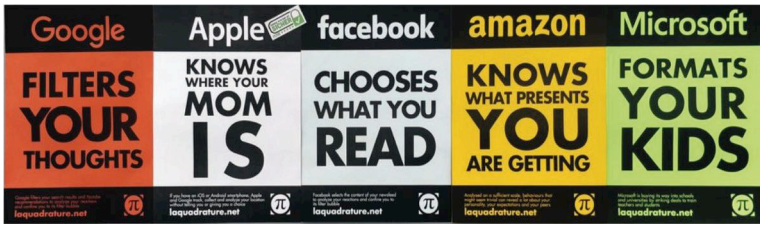
La plus grande menace pour notre système démocratique est que, si nous comparons les résultats sur une même question, nous arrivons toujours au même dilemme. D'une part, une large majorité souhaite des lois pour taxer la haute technologie, des lois pour sauver les emplois humains contre l'automatisation et des règles pour un meilleur contrôle des médias sociaux et des fake news. D'autre part, la plupart des citoyens ne font pas du tout confiance aux institutions qui seraient chargées de promulguer ces lois, impôts et règles. C'est ce que révèle l'enquête du rapport sur les parlementaires/sénateurs de tous les pays européens : *"plus de 50% des Européens sont favorables au remplacement de leurs représentants par des algorithmes. Les jeunes générations y sont particulièrement favorables, avec 60 % des 25-34 ans qui y sont favorables."*

Nous pouvons observer la même situation sur les questions les plus cruciales de cette année.

- **La Santé :** si *"la majorité des Européens est favorable à la construction d'une Union européenne de la santé pour améliorer la coopération dans le domaine de la santé publique"* (65%), les mêmes personnes interrogées *"sont complètement divisées lorsqu'il s'agit de laisser leurs gouvernements partager leurs dossiers médicaux avec des entreprises privées"* (45% pour, 47% contre). Pire, *"la majorité des jeunes Européens de moins de 25 ans est prête à laisser les assureurs collecter des données personnelles sur la santé et l'exercice physique grâce à l'utilisation de wearables de santé"* (46%).



- **La censure des médias sociaux et la propagation des fake news :** *"La perception de Google, Amazon, Facebook et Apple s'est considérablement dégradée : l'année dernière, seule l'Allemagne avait proposé de limiter très sévèrement leurs pouvoirs. Aujourd'hui, tous les pays européens, à l'exception de l'Italie et de la Pologne, sont en faveur d'une limitation du pouvoir des géants technologiques". En outre, "les Européens sont majoritairement opposés à ce que Facebook devienne un géant de la messagerie privée" et il existe un "large*



consensus parmi les Européens sur le fait que les réseaux sociaux ont eu un impact négatif et ont accru la polarisation politique" (56%). Mais pour ces mêmes citoyens, "les fake news sur les réseaux sociaux devraient être contrôlées par les plateformes et non par les gouvernements" (55% contre 27%).

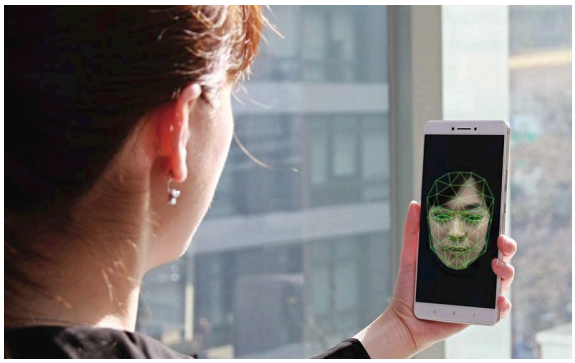
▸ **L'emploi :** *"Une majorité écrasante d'Européens (61%) est prête à payer plus d'impôts en échange d'une augmentation des salaires des travailleurs essentiels". "Une grande majorité d'Européens souhaite que des lois et des taxes permettent de sauver les emplois humains par rapport aux tâches automatisées", et "Il existe un soutien fort et large en faveur de l'introduction d'une "taxe technologique" avec 65% des citoyens en faveur et 15% contre."* Mais dans le même temps, *"un tiers des Européens préféreraient que ce soit une IA plutôt qu'un fonctionnaire qui prenne une décision concernant leurs prestations sociales ou l'octroi d'un visa. Un quart des Européens font également plus confiance à l'IA qu'aux humains lorsqu'il s'agit de négocier et d'accorder des prêts hypothécaires."*



▸ **Les achats en ligne :** le malentendu sur ce qui est souhaité atteint son paroxysme avec l'affaire Amazon : *"la majorité des Européens (50%) pense qu'Amazon nuit aux petites entreprises et aux commerces locaux".* Mais *"jusqu'à 64 % des répondants britanniques, 48 % des Allemands et 47 % des Italiens préfèrent acheter leurs livres via leur plateforme plutôt que de se rendre dans un magasin physique".* En outre, *"plus d'un tiers des Européens (35 %) préfèrent qu'un colis soit livré par un robot plutôt que par un humain..."*



▸ **Les dangers du monde en ligne :** *"la grande majorité des Européens (86 %) pense que la dépendance numérique est un problème" mais "une grande majorité d'Européens souhaite que la démocratie passe au numérique : 72 % préféreraient voter via leur smartphone plutôt que physiquement et seulement 17 % sont contre" et "42 % des Européens sont favorables à l'utilisation de la technologie faciale dans la vie quotidienne si cela la rend plus pratique".*

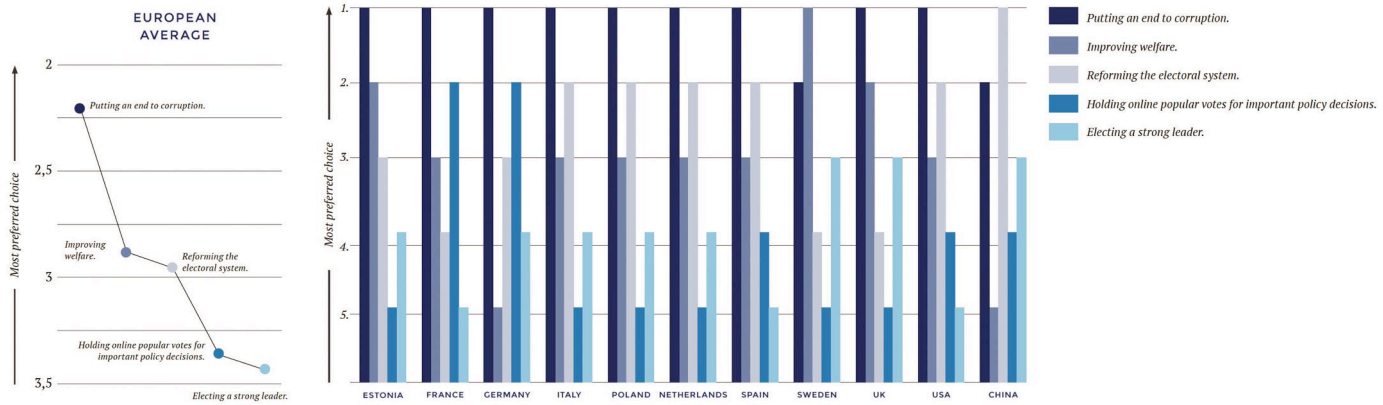


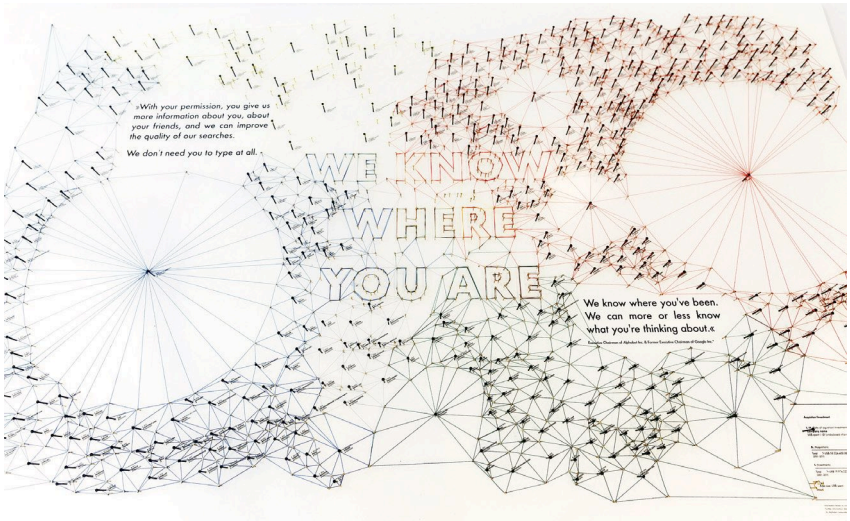
En bref, il y a un manque total de confiance dans l'État élu, qui est aggravé par une mauvaise union de toutes les institutions de l'État en charge de la loi et de l'ordre, sans parler du phénomène répandu de méfiance totale dans le soi-disant *"État profond"* (services secrets). L'incompétence, les administrations surchargées et la bureaucratie (publique et privée) ne sont pas un problème. Même le bien-être vient après la lutte contre la corruption, ou plutôt ce qui est perçu comme corrompu dans chaque Etat, qui est selon les citoyens le principal problème à résoudre pour restaurer la confiance dans la démocratie (une opinion partagée par les Européens et les Américains)...

Les autorités en alerte... sans conséquences

Pendant ce temps, les autorités académiques et spécialisées agitent quotidiennement des drapeaux rouges. Nous avons choisi trois sujets parmi les plus récents et les plus importants de l'immense panoptique des défis culturels et sécuritaires auxquels nous sommes confrontés.

Le premier problème est certainement celui de la reconnaissance faciale en direct. Les citoyens britanniques savent mieux que quiconque de quoi il s'agit puisque le sujet a fait la une de tous les grands médias. Le 18 juin, la commissaire britannique à l'information, Elizabeth Denham, a publié sur son blog institutionnel un article destiné au grand public qui montre très clairement son interrogation sur le fait d'imposer des restrictions urgentes et nécessaires pour contrer la reconnaissance faciale en direct (LFR) par les géants de la technologie[1] et, en même temps, pour permettre aux forces de l'ordre d'utiliser au mieux cette technologie[2]. Nous reproduisons ici la phrase la plus significative de son texte, selon nous : *"Nous devrions pouvoir emmener nos enfants dans un complexe récréatif, visiter un centre commercial ou faire le tour d'une ville pour voir les curiosités sans que nos données biométriques soient collectées et analysées à chacun de nos pas."*





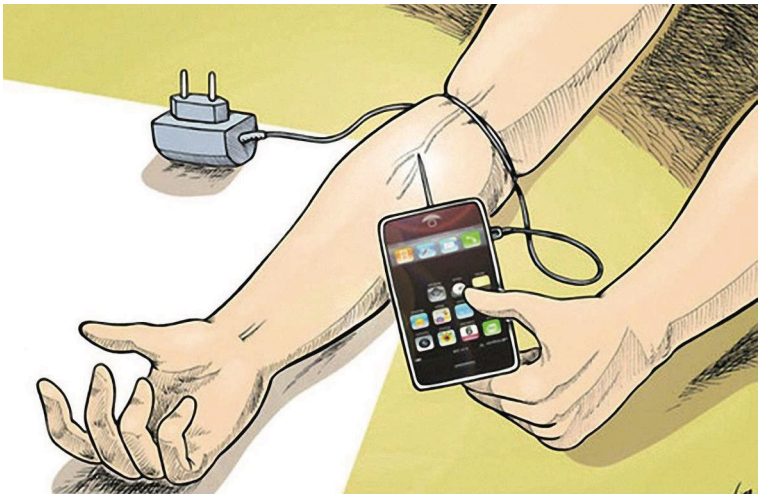
Legenda: L'Alphabet City, œuvre d'art de Tactical Tech et La Loma, réalisée à partir de données ouvertes extraites des GAFAM.

Il va sans dire que si cette phrase est conforme à l'opinion publique que nous venons d'analyser, l'utilisation de la LFR par les institutions policières et, "pire", par les services de renseignement est en totale contradiction avec les résultats de l'enquête que nous avons mentionnée plus haut. Par commodité, les citoyens préfèrent que leur intimité personnelle soit gérée par des applications plutôt que d'être gardée par l'État dont le premier devoir, outre la santé et l'éducation, est précisément de garantir notre sécurité physique et numérique.

Le deuxième dilemme est qu'aucune sensibilisation à l'hygiène numérique ou à la cybersécurité ne sera acceptée si tout cela est considéré comme une entrave au confort de chacun. Et comme la majorité des gens veulent que le smartphone soit de plus en plus utilisé, pour le travail, la vie personnelle, la banque et même maintenant... le vote, les portes de l'enfer sont désormais grandes ouvertes.

Parce qu'il n'y a rien de moins sûr qu'un smartphone. Pire encore, dans la réédition améliorée de son film phare *"The Shallows" : What the Internet Is Doing to Our Brains"*, Nicholas Carr signale un phénomène étudié en profondeur par de nombreux scientifiques lors de traumatismes post-délocalisation : l'abus de smartphones, en plus d'infecter facilement le nuage de tous les virus possibles, réduit drastiquement la membrane externe de notre cerveau, la partie sensible dont la règle est précisément de permettre aux informations de pénétrer dans notre mémoire. Plus tôt les enfants, mais aussi les adultes commencent les excès dans l'utilisation des smartphones, plus leur capacité de mémoire se dégrade, mois après mois, car cette membrane se régénère très lentement et cesse de se régénérer à partir de 50 ans (voir Tanil, Yong 2020 & Liebherr et al. 2020).

Le dernier avertissement, non moins important, est que l'équation HOMME + SMARTPHONE n'est pas seulement le dernier maillon faible de la sécurité, c'est aussi la voie directe vers la mort de la sophistication de nos langues.



Les réformes continues visant à adopter des expressions "e-slang" dans chaque langue européenne sont la mauvaise réponse à l'appauvrissement complet de la capacité linguistique des étudiants que nous pouvons observer dans les universités où nous enseignons, sur tout le continent. Comme il ne faut pas plus de 200 mots pour lire un tabloïd ou une

information mobile de MSM, il va sans dire que les trésors de l'humanité que sont la grammaire et la sémantique propres à chaque langue ou dialecte seront bientôt étudiés comme le grec ancien ou le latin.

L'anglais (ou plutôt le globish) peut se permettre de le faire en maintenant sa version académique pour les universitaires puisque cette langue particulière ne dispose pas d'un organisme unique qui définit son vocabulaire et sa grammaire, comme c'est le cas de la majorité des langues néolatines, parmi lesquelles nous citerons l'Académie française à titre d'exemple.

Et c'est ainsi que l'exemple américain d'acceptation des néologismes électroniques à des fins utiles ne peut être transposé à nos langues, comme l'explique Gretchen McCulloch dans son essai présenté par le Times comme *"une réfutation bien documentée des grammairiens grincheux qui pensent que la technologie transforme les enfants en baveux paresseux et inarticulés"*. Le français, l'italien, l'espagnol et tant d'autres langues ne peuvent pas se permettre ce luxe, ou alors il faudra accepter de passer d'une langue sophistiquée, élaborée et précise à une sorte de "latin médiéval" post-moderne.

Pour en revenir à The Matrix, les pensées de Morpheus correspondent parfaitement à notre époque : *"Tout au long de l'histoire de l'humanité, nous avons été dépendants des machines pour survivre. Le destin, semble-t-il, n'est pas dénué d'un certain sens de l'ironie."*

Et pour conclure avec ironie, ce sont justement les langues utilisées académiquement qui pourraient devenir le dernier outil pour éviter toute censure des Gafam : avec des collègues et, avant tout, avec l'accord de notre homologue cité dans notre texte, nous avons paraphrasé une description qui nous est connue grâce à ce qui est considéré comme une pierre angulaire pour les chercheurs : les quatre volumes de l'ouvrage *A Catalogue of the Lamps in the British Museum* (Londres, 1975-2004) du regretté Donald Michael Bailey.

Nous avons utilisé Twitter, Linkedin, Messenger, Facebook et avons posté : *"our colleague XXX is known to be in congress with selected students"* en joignant une photo de lui avec ses doctorants, dont 99% sont des femmes. Considéré par les algorithmes comme une erreur d'anglais écrite par une personne originaire d'un pays d'Europe de l'Est, notre texte n'a été censuré ni pendant que nous l'écrivions, ni après l'avoir posté, sur aucun des réseaux sociaux mentionnés ! Bien sûr, nous avons immédiatement supprimé tous les messages ainsi que les faux comptes créés pour cet exercice.....



Lampe romaine en terre cuite découverte à Alexandrie, collection Marc Bouvier. Datation : 30-70 apr. J.-C . Fabriquée au moule par un atelier chypriote, puis importée en Égypte. Sur son médaillon, scène érotique identique à celle qui orne quatre lampes contemporaines, manufacturées en Italie et conservées au British Museum, une iconographie décrite par D.M. Bailey comme "a woman in congress with a man on a bed ". (Bailey 1980, pp. 67-68).

Blagues universitaires mises à part, nous considérons nécessaires, indispensables et immédiates la lecture et la mise en œuvre consécutive des conseils offerts par Cal Newport, professeur d'informatique à l'Université de Georgetown, dans son dernier essai, immédiatement traduit en 18 langues - dont nous reproduisons le titre original, qui rend mieux le contenu : *"Digital Minimalism : Choosing a Focused Life in a Noisy World"*. Il existe tellement d'applications et de gadgets qui, vraiment, ne manqueront pas, même à ceux qui les utilisent pourtant frénétiquement... à condition de vouloir raviver le profond côté humain, passionné, intéressé, disponible envers les éléments vraiment importants qui existent en chacun de nous.

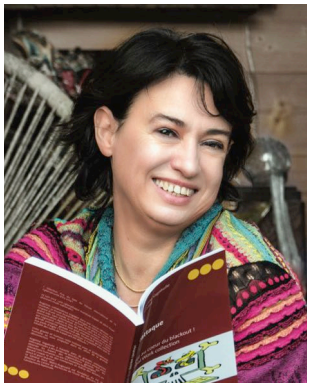
Bibliographie :

- Nicholas Carr, The Shallows : *What the Internet Is Doing to Our Brains* (édition mise à jour), Atlantic Books, Londres 2020
- Cal Newport, *Digital Minimalism : Choosing a Focused Life in a Noisy World*, Penguin Business, London 2019 (version anglaise : *Digital Minimalism. Recentrer votre vie dans un monde plein de distractions.* ROI Editions, Milan 2019)
- Clarissa Theodora Tanil, Min Hooi Yong, *Mobile phones : The effect of its presence on learning and memory,* PLoS ONE 15(8) : e0219233. (https://doi. org/10.1371/journal.pone.0219233)
- Magnus Liebherr, Patric Schubert, Stephanie Antons, Christian Montag, Matthias Brand, *Smartphones et attention, malédiction ou bénédiction ? - A review on the effects of smartphone* usage *on attention, inhibition, and working memory,* Computers in Human Behavior Reports 1, 2020 (https://doi. org/10.1016/j.chbr.2020.100005)
- Gretchen McCulloch, *Because Internet : Understanding the New Rules of Language,* Randomhouse, Londres 2019. ■

1 https://ico.org.uk/media/for-organisations/documents/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf

2 https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf

Quand le numérique nous ramène au paléolithique.



Auteur : Delphine Chevallier

Les acteurs du numérique, que ce soit ceux de l'IA, des applicatifs ou des matériels, nous assènent depuis de nombreuses années que ce qu'ils nous vendent nous augmentent. Et si ceci ne relevait que d'un tour de passe passe marketing[1] ?

Nous ne pouvons pas nier les progrès sans précédent que nous apportent les outils numériques : analyses accélérées, gains de productivité, facilitation et accélération des échanges et des mises en relation. Tout ceci avec une promesse : ces progrès nous permettent de nous éviter les tâches les plus ingrates, besogneuses et répétitives pour nous consacrer à celles les plus agréables, à plus forte valeur ajoutée.

BIO

Delphine a une expérience de plus de quinze ans dans le développement et l'animation de programme de (trans)formations dans les grands groupes internationaux, notamment de conseil. S'appuyant sur son expérience en matière de pédagogie et d'édition, elle a fondé Thalia NeoMédia, pour accélérer le développement des talents en mettant à leur disposition des outils d'apprentissage favorisant le partage d'expérience et l'engagement, plus particulièrement dans le domaine de la cybersécurité. Elle est lauréate Femmes en Vue du concours Vox Femina 2020.



Mais que constatons nous ?

Une hyper dépendance croissante aux outils digitaux qui nous a affaiblis

Les outils digitaux ont pris une telle place dans nos vies personnelles et nos interactions professionnelles que nous nous retrouvons dans une situation de vulnérabilité nouvelle.

Le monde digital a créé un niveau de dépendance sans précédent : s'il n'est pas unique (nous sommes aussi devenus extrêmement dépendants des ressources énergétiques par exemple), il est sans précédent du fait de la rapidité avec laquelle nous avons transformé nos modes de fonctionnements, notre façon de travailler et d'effectuer certaines tâches qui désormais ne se réalisent que grâce aux outils digitaux avec peu d'efforts, dans les organisations mais aussi dans nos vies personnelles.

Quel que soit le vocabulaire utilisé (outils digitaux, systèmes d'information, outils technologiques), il s'agit d'utiliser une machine pour effectuer une action, au lieu d'utiliser nos mains ou des outils présents dans le monde réel voire notre cerveau ! L'utilisation de machines a envahi exponentiellement

1. la communication entre êtres humains désormais 'numérisée',
2. le stockage de données désormais 'virtualisé',
3. le traitement de données désormais 'digitalisé'.

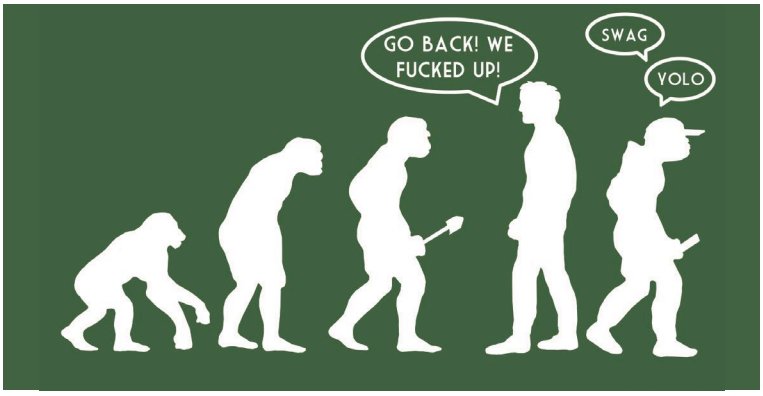
Ces pratiques ont pour conséquence un "désapprentissage" à marche forcée : combien de numéros de téléphone sommes-nous encore capables

de retenir par coeur ? Sommes-nous encore capables de trouver notre chemin dans la rue ou sur la route sans Google Maps ou notre GPS ? Sommes-nous encore capables de lire pendant plus de 15 minutes sans nous arrêter un long texte au lieu de zapper de quelques lignes d'une information à une autre dans le flot sous lequel nous noient les réseaux sociaux ?



Au quotidien, nous nous abandonnons paresseusement aux incitations d'achat, de rencontre ou de trajet recommandés par nos compagnons électroniques. Nous utilisons notre temps de cervelle libéré à regarder des videos de chats ou de congénères qui se dandinent sur les serveurs du net, nous 'scrollons' sans fin le fil d'ariane des réseaux sociaux[2].

Nos capacités intellectuelles sont-elles en train de rétrograder pour revenir au niveau de nos chers ancêtres de cro-magnon ? Avec en moins les capacités à survivre dans un environnement qui risque de nous devenir étranger, l'espace réel.



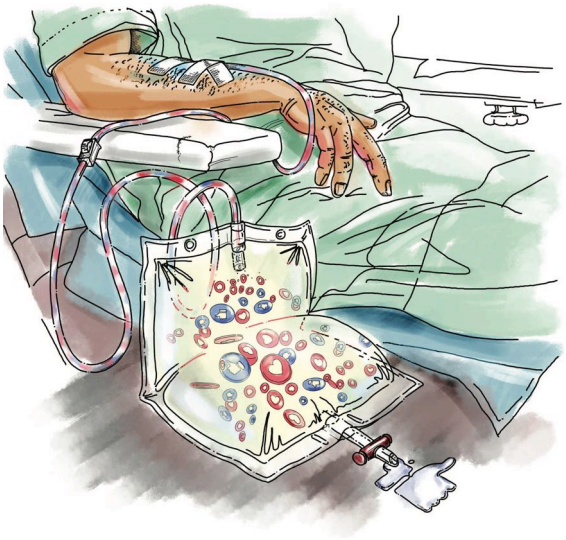
Lorsque nous envisageons le cyber espace, ce nouvel environnement où nous opérons 'virtuellement', par lequel nous transmettons voix, images et données, nos sens sont anéantis et nos réflexes ancestraux semblent avoir disparu. Plus aucune méfiance, plus aucun doute ne nous habitent et nous sommes capables d'échanger avec des individus que nous ne connaissons pas, d'envoyer des documents sensibles ou personnels sans même savoir s'ils peuvent être interceptés : entre mon écran et celui de mon destinataire, c'est comme s'il n'y avait rien dans cet océan d'immédiateté. Nous ignorons, inconsciemment ou non, volontairement ou non, les multitudes de vulnérabilités des matériels et outillages numériques qui ont été mis à notre disposition par des constructeurs ou développeurs qu'ils ont pris soin de nous cacher.

Mais la menace est bien là. Et les attaquants virtuoses de la navigation dans le cyber espace n'ont plus qu'à se régaler de notre naïveté et de nos esprits endormis.

Que se passe-t-il alors lorsque qu'un individu ou un groupe d'individus se trouve brutalement déconnecté des outils numériques ?

Les interruptions informatiques provoquent chez les victimes un niveau de stress extrême

Lorsqu'un incident informatique majeur se produit (comme une cyber attaque ou une interruption de réseau ou un dommage matériel), les individus se retrouvent comme jamais auparavant dans une situation qui les désoriente. Le stress qui en découle atteint de façon surprenante des niveaux extrêmes. Voici quelques paroles que j'ai entendues ces derniers mois de la bouche de celles et ceux qui en avaient fait l'amère expérience : "cela m'a rendu hystérique de ne plus pouvoir accéder à mes données" , "j'étais d'autant plus énervé que mes clients et partenaires continuaient eux à travailler normalement, à s'envoyer des e-mails et moi, j'étais complètement bloqué. Je me suis senti complètement exclu et surtout impuissant", "j'ai perdu deux ans de ma vie", "cela m'a presque rendu fou lorsque j'ai réalisé que je ne pouvais plus travailler" , " je n'avais aucune idée de ce que je pouvais faire pour avancer dans mon travail", "c'est comme si un missile était tombé sur mon entreprise".



Les mots sont particulièrement forts. Comment en est-on arrivé là ?

Lorsque tout s'arrête, que les machines nous jouent un bien sale tour en s'arrêtant de fonctionner, nous voici replongés 'en arrière', dans un monde du "ici et maintenant", bien concret et réel, notre bureau, les

collègues qui travaillent dans le bureau d'à côté, le papier et le crayon. Une réalité avec laquelle nous avons, consciemment ou non, mis une distance avec le développement de ce monde que nous disons "virtuel." et sans lequel nous nous sentons désormais perdu.

Quand il faut se résoudre à traverser le désert digital

Quelle expérience lorsqu'une interruption majeure du fameux réseau ou des fameux systèmes se produit, lorsqu'un logiciel dit malveillant s'introduit pour prendre en otage voire détruire nos données, lorsqu'un bug vient perturber un logiciel ! Comme nous nous retrouvons faibles et perdus lorsque la machine "ne répond plus" car cet événement nous renvoie à la difficulté à réactiver des savoirs faire qui nous paraissent déjà anciens, voire oubliés.

En effet, à l'heure de la soi-disant artificialisation de l'intelligence, on ne peut que constater une rapidité à désapprendre des façons de faire qui avaient, pour certaines, pris des millénaires à être acquises : communiquer, écrire et parler, se souvenir, se concentrer, penser… On pourrait s'en moquer, se dire que les temps changent et que ce processus n'est qu'une nième étape dans l'évolution de notre humanité. Cependant, le pouvoir qu'a pris monde digital sur nos capacités intellectuelles est peut-être bien plus perfide et lourd de conséquences que nous l'imaginons.

Plongés brutalement dans l'inimaginable d'une grande déconnection, les individus n'échappent pas à cheminer dans un processus de transition psychologique dont la durée s'étale sur plusieurs jours. Cette transition démarre par une période d'inaction liée à une sidération et une incompréhension, qui s'accompagne d'un refus de la situation. "Non ce n'est pas possible, les systèmes vont repartir". Pour une majorité d'individus plusieurs jours seront nécessaires pour se remettre en action et une colère monte…

Lorsque la situation sera intimement acceptée, l'opportunité s'ouvre enfin sur une prise de conscience intime de la nécessité de développer des comportements désormais inédits pour se remettre à travailler, en mouvement et en action. C'est dans cette phase que le groupe, face à l'adversité, exprime sa solidarité : lorsque le réseau flanche, le lien humain a une capacité étonnante à se reconstituer. Le retour de la motivation couplée avec la solidarité forme le terreau favorisant le développement de l'ingéniosité, permettant de réapprendre des gestes anciens ou de se débrouiller 'avec les moyens du bord'.







A quelle vitesse sommes-nous capable de réapprendre ce que nous avons si facilement et rapidement désappris ? Quelle énergie devons-nous déployer pour transitionner à rebours vers les gestes anciens ? Ce processus de réinvention, n'est-il pas supérieur à celui d'apprentissage en amont ? Comment garder la main, le contrôle, en toutes circonstances sur ce qui nous permet d'interagir ? C'est bien parce que ce niveau d'énergie demandée est très fort, que face à la machine qui ne fonctionne plus, nombre d'individus peuvent devenir "hystériques".

Ne serait-il pas moins onéreux de conserver ce comportement, ce geste qui a mis de longues années à s'ancrer en nous, en continuant de le pratiquer régulièrement pour assurer la continuité de nos activités ? Comme le souligne Andy Bochman de l'INL Lab[3] : "le seul moyen de (..) se protéger est de faire (..) ce qui peut sembler être un pas en arrière sur le plan technologique, mais qui est en réalité un pas en avant judicieux. L'objectif est de réduire voire d'éliminer la dépendance (..) aux technologies numériques et à leurs connexions Internet. Le prix (..) en vaudra la chandelle par rapport au coût potentiellement dévastateur que nous pourrions payer en continuant comme si de rien n'était."

Le maintien d'une praxis en mode dégradé et la restauration de mécanismes mentaux hors processus digitalisée permettent d'élaborer de nouveaux processus dans un contexte solidaire et de minimiser l'impact de l'interruption de services digitalisée.

Vers l'ère d'une nouvelle indépendance

Pour les organisations, s'assurer de la capacité des individus à traverser sans trop de dommages de telles crises, qui ne manqueront pas d'arriver, est une nécessité vitale. Si les équipes sombrent dans l'inertie en se laissant submerger par le chaos, c'est la pérennité même de l'entreprise qui se joue. Le point de départ est sans nul doute d'accepter sa vulnérabilité et de



refuser la dépendance en identifiant, avec les équipes, les activités pour lesquelles un maintien des savoir-faire manuels ou en mode dégradé sera essentiel pour maintenir la continuité des affaires. Engager toutes les forces vives de l'organisation dans ce processus est indispensable pour que les équipes, à tous niveaux, conservent une capacité minimum à travailler, autant que faire se peut, en cas d'incidents. Pour y parvenir, la meilleure des solutions reste de s'entrainer, de pratiquer, bref de reprendre le contrôle sur les outils numériques que nous utilisons. A nous de les dominer et pas l'inverse.

Rassurée par cette toute nouvelle indépendance, une organisation s'en trouvera renforcée, grâce à ses ressources les plus précieuses, des femmes et des hommes aux capacités réellement augmentées. ■

1 Junk Tech, comment la SiliconValley a gagné la guerre du marketing - Jean-Marc Bailly, Xavier Desmaison, Ed Hermann
2 L'apocalypse cognitive - Gérald Bronner, Ed Puf
3 Harvard Business Review - Avril/Mai 2019

50 nuances d'Identité Numérique.



Auteur : Stéphane GASCH

L'Identité Numérique est une réalité qui est aussi une source de phantasmes divers. 50 nuances sont-elles suffisantes pour effleurer les multiples aspects que ces deux mots recouvrent ? A défaut d'exhaustivité, parcourons ensemble les principaux sujets à comprendre et pour certains à maitriser, sous peine de perdre la maitrise de nos Identités.

Avant toute chose, quelques nuances de définitions de l'identité... L'identité recouvre une multitude d'acceptions en partant de l'angle régalien avec l'identité civile, considérée comme Absolue, à l'angle de La légende du joueur d'un Jeu de Rôle[1], dont éventuellement les compagnons de jeu ne connaissent que le pseudo. Ici, nous évoquons des identités "physiques" alors que le monde numérique nous ouvre d'autres visions de l'Identité depuis le pseudo 3615[2] des années 80 à l'avatar de jeu ou du futur "Métavers[3]". En effet, dans l'espace numérique, l'identité est aussi définie par les "traces" déposées, leur récurrence, leur cohérence et *in fine*, leur recoupement. Dans le monde physique à nouveau, des traces peuvent définir un objet comme l'identité sonore d'un vaisseau parfaitement identifiable quand il navigue[4] ! Le canevas étant tissé, reprenons-les plus en détail et dans l'ordre essentiel de leur mise en œuvre :

Mon Identité, c'est ce que je suis, ce qui me définit et ce qui va être lié à mes actions. Cette définition, perfectible, s'applique aussi bien à un "être" physique que numérique, et dans les deux mondes, il lui sera demandé de démontrer cette identité à partir d'éléments de référence ou bien par une conjonction d'éléments.



Toutefois, lorsqu'il s'agit de transposer l'usage de l'identité du monde physique au monde numérique, se profile alors la question d'une conversion à l'identique dans la sphère digitale de posséder une Identité Numérique. Autrement dit, la capacité de lier cette identité physique à un

BIO

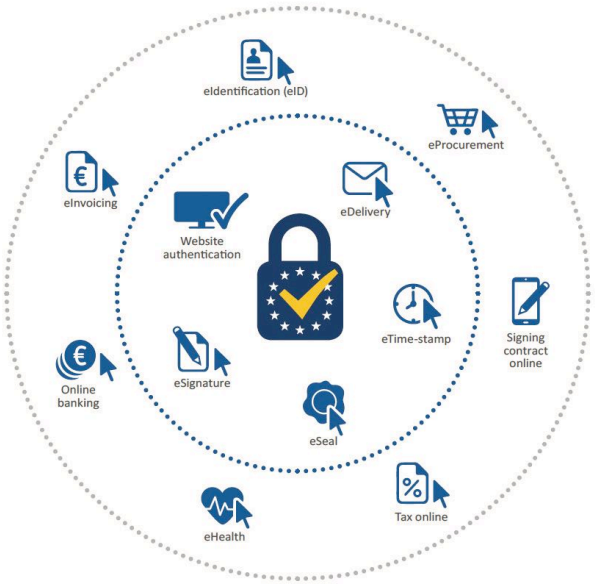
Stéphane a exercé ses activités dans le développement informatique, la conduite de projet, l'audit, le pilotage de business unit et la direction d'entreprises. Spécialiste de la signature éelctronique il est à l'origine de plusieurs réalisations en France depuis la publication de la directive de 1999. Dans l'ensemble de ses actions il a toujours privilégié la normalisation, d'abord en E.D.I. en participant à la création de l'Association EDIFICAS puis dans les travaux de la facture électronique au FNFE ou pour la généralisation des technologies du CEV. Il est aujourd'hui Délégué Général de l'Autorité de Certificat ChamberSign France et travaille sur la généralisation de l'identité numérique et son adoption dans les échanges professionnels. Il est aussi chargé d'enseignements au Master II Tiers de Confiance et sécurité numérique à la faculté de la Rochelle.



moyen d'authentification et créer ainsi une Identité Numérique aussi fiable et sécurisée que celle que nous possédons physiquement !

A l'instar du dieu Janus, l'identité numérique met en évidence deux faces inséparables entre l'identité et le moyen de prouver cette identité : la dynamique d'un cycle débutant par une étape démontrant ou prouvant l'identité, puis l'étape essentielle du lien dans cet enrôlement, mixant contrôle et délivrance certaine du M.I.E ou le Moyen d'Identification Electronique[5].

Le concept du M.I.E. n'est pas unique et existe sous différentes nuances aussi variées qu'un simple pseudo à peine protégé par un mot de passe et pouvant être largement partagé et piraté jusqu'au certificat cryptographique qualifié sur une carte à puce, inviolable et non reproductible. Sous cette dernière forme, le contrôle exclusif de l'identité par son détenteur est obtenu par le respect des règles de délivrance via une qualification des outils et une remise en face à face par une Autorité de Certification.



Entre ces deux "extrêmes", il existe de multiples nuances qui utilisent fréquemment le téléphone mobile, élément très personnel, permettant de recevoir un code pour s'authentifier.



Nous pouvons également distinguer des nuances de fiabilité selon que l'on utilise un simple SMS, fragile car "interceptable", ou une application mobile sécurisée et enrôlée lors du contrôle de l'identité.

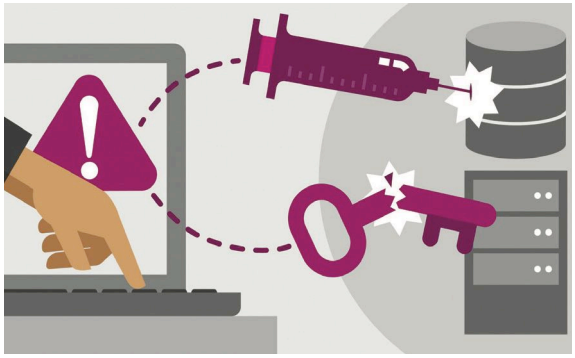
En tout état de cause, la question de la sécurité du M.I.E. est la pierre angulaire de la fiabilité de l'Identité Numérique, car quel que soit le niveau de vérification de l'identité et de la véracité de celle-ci, elle n'existe plus si le M.I.E. est dupliqué ou intercepté à l'insu du titulaire ou avec sa complicité…

Mais pourquoi cette dernière assertion est-elle si importante pour le M.I.E. ?

Prenons l'exemple d'un acheteur peu scrupuleux qui se dirige dans un magasin spécialisé à Nice pour acquérir un ordinateur portable et souscrire à un service complémentaire en validant celui-ci au moyen d'un code reçu sur son téléphone. Simultanément, un

"ami" réalise la même opération à Lyon avec le même numéro et reçoit le code d'activation qui a transité sur le mobile de son complice à Nice. Deux contrats, souscrits théoriquement en présence de la même personne à 600 kms de distance en quelques minutes … Il y a manifestement un problème conceptuel dans l'authentification de l'individu. Incertitude des parties, incertitude du consentement !

Bien entendu, ce type de situation peut exister dans la vie réelle, et de nombreux contentieux sont susceptibles de naitre au regard du contournement de moyens trop simples d'authentification.



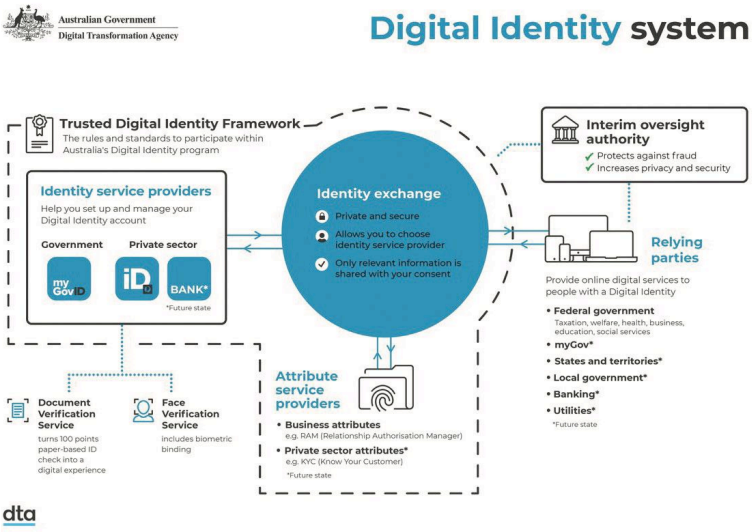
Poursuivons sur ces nuances de M.I.E. et revenons au "Dinosaure" qu'est la carte à puce ou le certificat cryptographique, et observons ensemble une licorne Française : LEDGER, numéro 1 mondial de Wallet électronique sécurisé pour gérer ses cryptoactifs. Quelles différences entre un portefeuille numérique mémorisant ses clefs privées de comptes et une puce contenant ses clefs privées de signatures associées à son certificat d'identité ? Un niveau de qualification, des interfaces utilisateurs et pour le portefeuille, des moyens de recouvrement permettant de récupérer ses actifs en cas de perte de mémoire. Nous observons une certaine permanence des solutions face à la répétition des mêmes besoins.

Puisque nous sommes dans les cryptomonnaies, continuons vers ces nuances extrêmes disruptives du nouveau monde des blockchains et plus précisément des identités décentralisées…

L'approche décentralisée nuance l'identité numérique en structurant le concept d'attributs liés à cette identité et réaffirme le contrôle de l'identité par son titulaire en gérant celle-ci au moyen d'un "Wallet", espace sécurisé et communicant permettant de gérer des identités et de prouver celle-ci au moyen de micro-échanges avec l'environnement utilisateur. Mais pas seulement d'Identité de Référence. Dans les nuances des identités décentralisées, existe l'avantage de l'architecture blockchain par construction résiliente et particulièrement adaptée à des attributs complémentaires à l'identité civile de référence. Ces attributs (adresse, téléphone, diplôme etc.,) sont émis et certifiés par des émetteurs qualifiés pour les garantir.

Contrairement à un document porteur de multiples informations qui sont divulguées à chaque présentation de celui-ci, l'usage des attributs sera limité à la stricte donnée demandée, voire simplement l'information. Par exemple, à la simple question "Etes-vous majeur ?" il n'est pas nécessaire de communiquer sa date et son lieu de naissance, voire son identité en présentant une pièce d'identité, mais uniquement l'information Certifiée : OUI. Ce cas d'usage, qui n'en est qu'un parmi d'autres, présente l'avantage des identités d'attributs décentralisées qui seraient très utiles aux jeunes de moins de 18 ans en France. Et ce n'est pas une exagération puisque l'actualité récente relata le cas d'un jeune de 17 ans souhaitant déguster une bière en terrasse et qui fut piégé par son pass sanitaire ! Pourquoi le statut Covid impose-t-il de connaitre sa date de naissance ? Ces identités décentralisées interrogent ainsi sur les moyens d'enrôlement ou de délivrance d'un M.I.E. à une personne après les vérifications nécessaires.

Dans un premier temps, il faut une identité "pivot", permettant de rattacher les futurs attributs à l'individu. Cette Identité, probablement régalienne



pour un usage civil, pourrait éventuellement être créée sur mesure dans un environnement virtuel comme le "metavers" déjà évoqué, dans un club d'amis ou encore sur un réseau privé pour d'autres usages. Certains imaginent des vérifications d'identités par consensus. Cela étant, dans nos sociétés, l'avenir est à une dérivation de l'identité élevée à partir d'un document régalien d'identité numérique. Le point commun et essentiel étant que l'ensemble des échanges soient réalisés par des messages normés et sécurisés pour garantir l'interopérabilité de ces approches entre la multitude des acteurs impliqués qui sont encore aujourd'hui au stade recherche et développement.

Alors quelle autre solution pour l'interopérabilité et l'usage universel de son identité numérique dans l'attente de ce futur ? Le "Bon vieux SSO" et ses approches modernes au moyen de normes de partage d'authentification permettant d'utiliser les identités déclaratives utilisées auprès des GAFAM qui, à chaque nouvel usage, récupèrent vos données personnelles !

Afin de sécuriser le partage d'identité sans les risques de Souveraineté, l'approche de fédération d'Identités comme France Connect permet

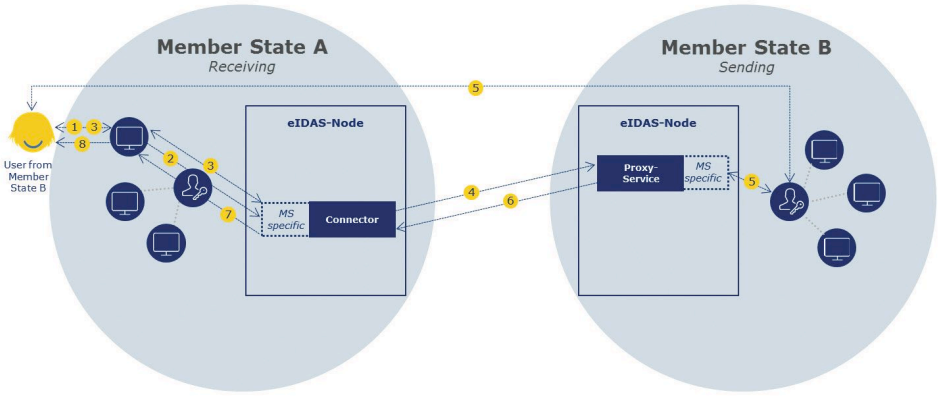
d'utiliser des identités de niveaux divers, opérée par des spécialistes de l'identité, selon les besoins de l'application utilisatrice. Ainsi se construit un écosystème permettant de partager des identités qualifiées respectueuses de la réglementation européenne en particulier.

Se dessine ainsi, dans ce nuancier de l'identité numérique, un cadre juridique rigoureux, instrument de clarté et de structuration qui a commencé son action avec le règlement eIDAS adopté le 23 juillet 2014, définissant avec une certaine précision conceptuelle les trois niveaux d'identités : simple, substantiel et élevé. Ces définitions reprennent les deux piliers de l'identité numérique qui permettent de fonctionner avec harmonie : Le premier pilier, identification, permet de s'assurer de la réalité ou de la stricte exactitude de l'identité revendiquée ou des attributs complémentaires. Le règlement définit le premier niveau de l'identité comme une "Présomption" simple pour l'identité du même nom : simple. Puis, deux autres niveaux de contrôles avancés et strictes de l'identité et du "titulaire" permettent d'accéder au niveau substantiel puis élevé.

Le second pilier, authentification, permet de doter le titulaire du moyen pratique, M.I.E technique, afin de prouver cette identité facilement en ligne ou lors de la réalisation d'un acte numérique. Ce volet authentification s'étage lui aussi en trois niveaux, du simple couple login/mot de passe facilement devinable ou "interceptable" y compris à l'insu du titulaire, au niveau élevé avec la carte à puce remise en face à face physique ou à distance et ses déclinaisons "chocs" de Wallet numérique évoqué dans divers contextes.







Le Wallet, en effet repris dans la dernière initiative structurante de l'Europe, propose un portefeuille d'identités hautement sécurisé en utilisant, probablement, des moyens physiques, peut-être même des cryptoprocesseurs de haut niveau. Cette initiative, incluse dans le "paquet" des propositions d'évolution du règlement vers eIDAS 2, est l'Identité Numérique Européenne qui propose une approche mixant la souveraineté nationale. Elle laisse la maitrise aux Etats de l'organisation nationale du Wallet en lien avec l'identité souveraine et la gestion d'attributs permettant, selon les concepts de l'identité décentralisée, d'échanger des valeurs certifiées avec les applications utilisatrices. La promesse est riche de disposer du meilleur des mondes Publics et Privés dans le respect de la vie privée et de la maitrise des données personnelles par un strict confinement des stockages et une traçabilité des échanges. Promesse à tenir lors du passage du texte de référence aux actes d'exécution, seuls capables de garantir interopérabilité et sécurité à l'échelle européenne.

Enthousiasmant ce nouveau monde n'est-ce pas ? Il n'y a pas de phantasme inaccessible mais simplement de multiples facettes complémentaires pour façonner un Concept, ou plutôt des "Outils bien réels" que nous utiliserons demain sans comprendre comment nous avons pu nous en passer jusqu'à aujourd'hui. Comme dans toutes les technologies et encore plus dans les solutions globales proposées autour d'Internet, c'est à l'utilisateur dans ses dimensions de citoyen et de consommateur de rester vigilant en s'impliquant, apprenant et réagissant si certains tentaient de dévoyer le dispositif. Pour s'initier, essayons la nouvelle carte d'identité électronique française et ses promesses à venir, ainsi que les quelques identités électroniques disponibles dans les prochains mois. ■

1 Un Jeu de Rôle se déroule dans le monde physique réel et permet aux participants d'incarner des personnages sous le direction d'un maitre du jeu. Les participants peuvent ne pas se connaitre.
2 Dans les années 80 la France a déployé un système télématique appelé Minitel et permettant de se connecter dans un pseudo anonymat à des sites de rencontre ou à divers services marchands ou culturels.
3 Wikipedia : Le métavers (de l'anglais metaverse, contraction de metauniverse, c'est-à-dire méta-univers) est un monde virtuel fictif. Le terme est régulièrement utilisé pour décrire une future version d'Internet où des espaces virtuels, persistants et partagés sont accessibles via un univers en 3D
4 Je vous invite à voir le « Le chant du Loup »
5 Le M.I.E. est un moyen technique qui fait le lien entre une identité physique ou numérique à l'utilisation numérique de cette identité.

Savoir communiquer par temps de crise.



Auteur : Jean-Marc Bonnet

Une crise peut vite arriver et toucher toutes les organisations. Nul n'est à l'abri avec les nouvelles technologies et son flot continu d'informations. Tout va très vite, trop vite…C'est pourquoi il est utile d'anticiper par un plan de communication prêt à être adapté et déployé.

Jouer la transparence

Une crise éclate autour de votre produit, vos services ou votre organisation. Le public commence à réagir négativement sur les réseaux sociaux et les médias commencent peut-être à relayer le buzz. Il faut garder la tête froide et opter pour une stabilité relationnelle. Prenez de la hauteur et gardez le contrôle de l'évènement pour rassurez vos clients, vos équipes et vos partenaires. C'est indispensable pour prendre les bonnes décisions.

Il est vital pour cela de jouer la carte de la transparence. Ce n'est pas le moment de faire la sourde oreille.

N'hésitez pas à rendre vous-même public ce qui se passe avant que des personnes extérieures le fassent pour vous, en promettant de tout mettre en œuvre pour y remédier. Faites-le dans un premier temps par écrit. Chaque mot doit être pesé pour éviter tout dérapage.



Comprendre ce qui se passe

Vous avez identifié le problème. Avant de communiquer, il est important de posséder le plus d'informations et de comprendre ce qui se passe. Utilisez des outils de veille et posez-vous les questions suivantes : combien de personnes en parlent sur les réseaux sociaux ? Combien de mails ou d'appels avez-vous reçus ? La presse en parle-t-elle ? Les réponses vous permettront de mesurer l'impact de cette crise.

Maitriser sa communication



Site internet, blog, réseaux sociaux, communiqué de presse ou newsletters, les canaux de communication sont nombreux. Lequel choisirez-vous pour communiquer ? Il faudra prendre en compte les avantages et les inconvénients de chacun, mais aussi suivre vos habitudes de

BIO

Bio Dirigeant du cabinet FINOVA Conseil à Saintes, Jean-Marc Bonnet accompagne les entreprises dans leur développement et leur communication. Il apporte un regard différent et partage avec ses clients les deux éléments qui ont jalonné sa carrière, des compétences économiques (connaissance des problématiques de l'entrepreneur) et sa volonté de transmettre lors d'une conférence ou une formation. Il a fondé dernièrement l'Ecole de l'Expression Orale, un organisme de formation certifié sur la prise de parole, la relation client et la posture commerciale. Sa devise : Prendre de la hauteur, voir plus loin, se révéler !

communication afin que votre audience habituelle reçoive votre message. Et n'oubliez pas que communiquer sur les réseaux sociaux invitera les clients au dialogue et nécessitera de répondre individuellement. Un communiqué de presse, au contraire, limitera l'échange.



Préparer votre message

Avec toutes ces données récoltées et le canal choisi, vous avez pu préparer votre message et votre stratégie de communication. Encore une fois, soyez le plus transparent possible. Le message doit contenir trois éléments capitaux :

1/Voilà ce qui s'est passé : assumez cette erreur et acceptez d'en assurer la responsabilité. Rejeter la faute sur un autre donnera l'impression que vous vous déchargez complètement de la situation et contribuera à donner de vous une mauvaise image.

2/Voilà ce que nous avons mis en place : énoncez les éléments que vous avez immédiatement mis en place pour circonscrire l'incident et réparer les préjudices subis par les clients.

3/Voilà ce que nous avons mis en place pour que cela ne se reproduise plus : afin de rassurer définitivement le client, expliquez-lui les diverses opérations que vous avez entreprises pour qu'il n'ait plus jamais à vivre une telle situation.



Si vous devez vous exprimer à l'oral (radio, TV, web…), répétez votre message au préalable en situation avec votre entourage. Optez pour des phrases courtes et une posture responsable (clarté d'expression, voix grave, ton ferme mais rassurant…)

Le succès de votre communication ne sera pleinement mesuré qu'à long terme. Tirez les leçons de cette période difficile. Cela vous permettra de mieux anticiper si ce type de situation se reproduit et d'adapter votre communication de crise pour le futur. ■



La cybercriminalité: un problème de management bien plus que de technologie.



Auteur : Nathalie MALICET

Le 11 avril 2020, les usines de Fleury Michon ont suspendu leur production pendant 5 jours en raison d'un virus informatique. Le 13 mai suivant, la société Picoty a été la cible d'un rançongiciel : 80% des données sont cryptées, une rançon de 500 000 euros est réclamée.

Et il ne s'agit là que de quelques exemples pour 2020. L'année 2021 se révèle tout aussi riche en attaques contre des intérêts économiques ou sociétaux. Des mairies, des hôpitaux, des entreprises ont ainsi été visés en France. La crise sanitaire mondiale n'a pas offert de "pause". Bien au contraire ! Les pirates ont profité de la désorganisation et du télétravail pour exploiter des vulnérabilités. Parfois directement attaquées, les entreprises peuvent aussi être victimes par "rebond". Quand le prestataire Solware est victime d'une attaque majeure courant août 2021, ce sont des centaines d'entreprises de toute taille qui sont bloquées ! Depuis plus d'un mois, la filière automobile est impactée : accès compliqué (voir impossible) à la base clients, aux réservations, à la facturation etc. … Les conséquences financières s'annoncent coûteuses.



La cybercriminalité n'est pas un concept à la mode mais une réalité coûteuse

Autrefois l'apanage de "geeks", aujourd'hui arme silencieuse de certains Etats, la cybercriminalité fragilise l'économie mondiale. Les attaques se sont multipliées et revêtent des formes diverses. La France n'y échappe pas. Elle vient même de se hisser au deuxième rang mondial de vols de données sur Internet, derrière les Etats-Unis.

Les attaques n'épargnent pas les entreprises, quelle que soit leur taille. L'actualité récente prouve qu'aucune structure n'est à l'abri. Les petites entreprises sont aussi des cibles de cyberattaques. Elles sont parfois visées spécifiquement car elles sont des points d'entrée pour atteindre les plus grosses entités avec qui elles entretiennent des relations d'affaires.

Dans son rapport d'activité 2018, l'Agence nationale pour la sécurité des systèmes d'information (Anssi) souligne: "en ciblant un ou plusieurs intermédiaires (fournisseur, prestataire, etc.), les attaquants parviennent à contourner les mesures de sécurité de très grandes organisation, pourtant de plus en plus conscientes du risque numérique". Et justement, "la

BIO

Nathalie est Expert-Comptable, Commissaire aux Comptes et Expert Judiciaire. Elle est Membre du bureau national de la compagnie nationale des commissaires aux comptes et Présidente de la commission Prospective et Innovation.

compromission d'un seul intermédiaire suffit parfois à accéder à plusieurs organisations".

Ces attaques par rebond, et plus généralement sur la chaîne logistique dans son ensemble, donnent alors tout son sens au message de l'Anssi pour 2019 : "tous connectés, tous impliqués, tous responsables".

Les 3,1 millions de TPE PME représentent une immense majorité des entreprises françaises ; elles pèsent 44% de la valeur ajoutée française et 49% de l'emploi salarié. Néanmoins elles sont très en retard dans la transformation digitale et souffrent d'une acculturation insuffisante en matière de cybersécurité. Moins bien organisées, elles sont plus vulnérables. Déni ou incompréhension de la gouvernance face à ce nouveau risque, formation inexistante du personnel, insuffisante protection des données et actifs critiques, absence de plan de continuité et de reprise d'activité, ces faiblesses peuvent conduire les entreprises dans des situations financières critiques.

Il est aujourd'hui plus rentable et moins risqué d'utiliser les outils informatiques pour détourner des fonds que d'attaquer une banque. Le cyberespace est vulnérable et en proie à des actes délictueux croissants. Les spécialistes de la cybersécurité tirent régulièrement la sonnette d'alarme : les attaques informatiques se complexifient et se professionnalisent.

Noyées dans le flot des données échangées, elles peuvent rester invisibles pendant plusieurs années. Elles peuvent piller le patrimoine informationnel des entreprises et toucher des infrastructures stratégiques. Pour élever le niveau de sécurité, tout en conservant la fluidité d'un Internet ouvert et décentralisé, les organisations doivent adopter une démarche rationnelle d'analyse de risques.

Les avancées technologiques au sein des entreprises, la mobilité des équipements, l'augmentation des données à protéger, la recrudescence des réseaux sociaux rendent les entreprises plus vulnérables.

Les usages nouveaux ("cloud computing", mobilité) sont les talons d'Achille des systèmes d'information. Qui n'a jamais utilisé son smartphone pour télécharger des applications, réaliser des achats en ligne ou surfer sur Internet avant de le connecter sur le réseau de l'entreprise ?

Le confinement imposé pendant plusieurs mois en 2020, le maintien du télétravail pour une majeure partie des salariés ont provoqué une modification soudaine (et souvent mal préparée) des modes de travail. Des accès aux réseaux d'entreprises ont été ouverts dans la précipitation. Des salariés ont utilisé des ordinateurs familiaux (dont le niveau de sécurité et de protection n'a pas été vérifié au préalable). Des données ont été stockées sur des drives personnels : le respect du RGPD, le rapatriement des données sur les serveurs de l'entreprise l'effacement définitif de ces stockages temporaires n'ont pas toujours été appliqués.

Les locaux désertés, les serveurs et les systèmes d'information ont été parfois (dans les plus petites entreprises) moins bien sauvegardés.

Autant de failles, autant de vulnérabilités …



La cybercriminalité fait désormais partie des risques majeurs auxquels sont exposés toutes les entreprises, quelle que soit leur taille.

La cybersécurité c'est 20% de technologie et 80% de management



Anticiper pour ne pas subir ...

Alors que les cybermenaces se multiplient et se diversifient, la prévention et la protection sont les meilleurs alliés. Une stratégie de cybersécurité s'avère essentielle pour toute organisation, afin de prévenir les attaques ou, dans le cas contraire, être prêt à réagir face à celles-ci.

En octobre 2018, Guillaume Poupard, Directeur de l'ANSII, déclarait : "Il n'y a pas de sécurité à 100 %. Donc ce qu'il faut c'est une sécurité à bon niveau, qui s'appuie sur une bonne analyse de risque, et d'être capable de détecter très vite si les choses ne sont pas normales."

Du MOOC de l'ANSSI à la platerforme Cybermalveillance, les pouvoirs publics ont mis à la disposition du grand public de nombreux outils. Mais ces outils restent insuffisants pour développer une véritable stratégie de cyber-résilience dans les entreprises. Il est nécessaire de convaincre les chefs d'entreprise qu'ils doivent investir dans la sécurité de leur système d'information.

Souvent coûteux, ces investissements sont repoussés dans le temps car le dirigeant évalue mal les conséquences financières d'une cyberattaque.

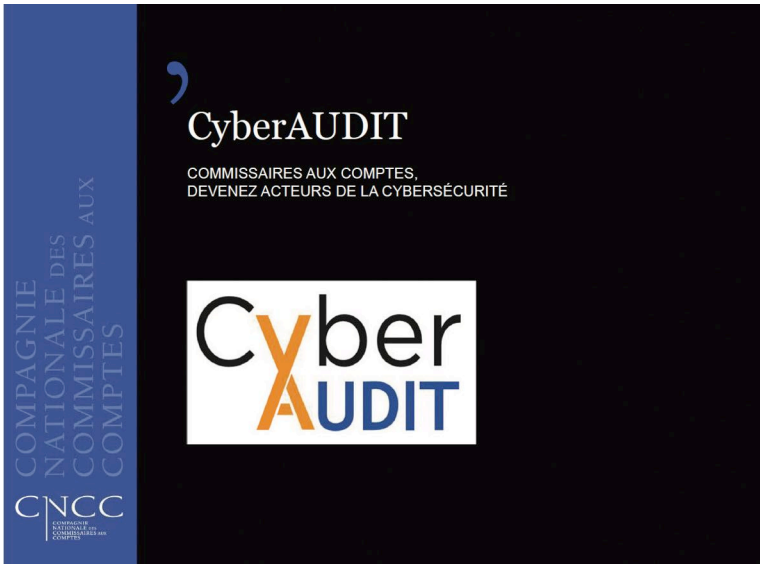
Un outil pour les Commissaires aux Comptes dédié à la cybersécurité des TPE - PME

La Compagnie des Commissaires aux Comptes a développé une plateforme (CyberAudit) qui permet aux Commissaires aux Comptes de réaliser une mission de diagnostic, pour évaluer les impacts financiers des menaces probables de cyberattaques.

L'objectif de la mission est de :

- déterminer l'exposition de l'entreprise face à ces risques,
- mesurer sa maturité pour répondre à ces menaces,
- envisager les scénarios probables de cyberattaques,
- en évaluer les impacts financiers.

A l'occasion de cette mission, le Commissaire aux Comptes s'entretient avec le dirigeant et toute autre



personne pertinente pour recenser les pratiques de l'entreprise en matière de cybersécurité. Ces entretiens permettent de prendre connaissance des usages en vigueur dans l'entreprise. Les questions posées traitent des données critiques, de la mobilité, de la résilience, du degré de digitalisation de l'entreprise. Les thèmes sont abordés à l'aide d'un jeu de soixante dix questions-réponses.

Après cette prise de connaissance détaillée, le Commissaire aux Comptes détermine des seuils de résilience financière. Trois zones seront ainsi délimitées : supportable, significative et critique.



Il est indispensable de confronter les conséquences financières des cyber-risques à la capacité de l'entreprise d'y faire face. Un préjudice de 100 Keuros peut être supportable pour une entité et condamner une autre. Ainsi, et par exemple, une entreprise avec une faible rentabilité (donc une capacité moindre à créer de la richesse), risque d'être définitivement condamnée si la cyberattaque la prive d'une part significative de sa trésorerie.

Des scénarios de menaces probables sont ensuite co-construits pour déterminer quels types d'attaques peuvent survenir. Ces scénarios sont personnalisés en fonction de l'organisation interne de l'entreprise, ses relations avec ses clients et fournisseurs, la criticité des données détenues, le degré de digitalisation des moyens de production.

Pour une entreprise réalisant la totalité de son chiffre d'affaires sur Internet, la menace de déni de services (DDoS) sera évaluée alors que pour une entreprise ne proposant pas de services en ligne, cette menace pourrait être écartée.



Pour chacun des scénarios de menace considérés comme probables, les différentes composantes financières du préjudice sont évaluées : perte d'exploitation, pénalités, frais de réponses à incidence, frais de justice, amendes, frais d'amélioration, etc …

Des scénarios de menaces probables pour cerner les enjeux financiers

Le diagnostic établi par le Commissaire aux Comptes ne traduit pas de certitudes mais des éventualités destinées à aider la gouvernance dans la prise de décisions stratégiques. La dimension financière de cette analyse permet de mieux évaluer les budgets nécessaires à l'amélioration de la sécurité des systèmes d'information. Elle permet aussi d'identifier les zones de faiblesses, les axes d'amélioration pour faire progresser la maturité de l'entreprise.

commissaire aux comptes

ORDRE DES EXPERTS-COMPTABLES

Le commissaire aux comptes participe ainsi, au travers de cette mission de diagnostic, à une sensibilisation forte des chefs d'entreprises sur les impacts financiers des cyberattaques. Il favorise la prise de conscience qu'aucune entreprise n'est trop petite pour être une cible. Il contribue ainsi au renforcement de la sécurité de la supply chain.

En conclusion, l'organisation des systèmes d'information et l'environnement technologique évoluant régulièrement, il est recommandé de solliciter un Commissaire aux Comptes pour réaliser périodiquement ce diagnostic et mesurer l'évolution de l'exposition de l'entreprise aux risques de cyberattaques. Les résultats tirés de ce diagnostic peuvent même être utilisés dans un tableau de bord, pour un meilleur pilotage de l'entreprise, et aller ainsi vers plus de résilience. ■

CHARENTE-MARITIME CYBER SÉCURITÉ CMCS 2021

bibliothèque EUREKA - Vanbergen

MIRAT DI NERIDE Cyber Sécurité

CMCS et Mirat Di Neride s'associent à la Bibliothèque EUREKA-Vanbergen

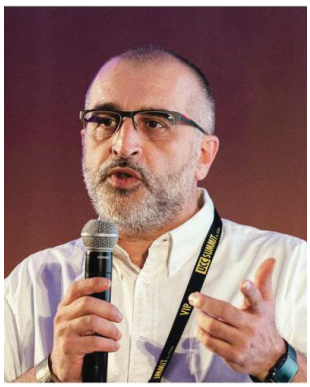
"Un intervenant - Un livre"

EUREKA-Vanbergen est une bibliothèque scientifique universitaire créée et soutenue par des mécènes.
Située à LIKASI, dans l'Est de la République Démocratique du Congo, elle a pour vocation la diffusion des connaissances scientifiques auprès des étudiants, des chercheurs et des professionnels de cette région.



"Un intervenant - Un livre" vise à permettre à la bibliothèque EUREKA-Vanbergen de mettre à disposition des jeunes congolais un rayon "cybersécurité". Chaque intervenant au CMCS 2021 est invité à offrir un livre de son choix, à le présenter en une minute avant son intervention et ainsi contribuer à diffuser une culture de la cybersécurité sur le continent africain.

Cyberdéfense : mettre l'humain au cœur du dispositif.



Auteur : Dominique Maïano

Une fois de plus, l'année passée aura vu une croissance exponentielle de la cybercriminalité. Malgré la mise en place d'organisations étatiques de lutte contre la cybercriminalité, la facilité d'accès aux armes de nuisance et la quasi-immunité des groupes de prédateurs laissent présager que cette situation va perturber encore quelques temps.

Le terme a déjà été plusieurs fois évoqué : c'est bien d'une guerre dont il s'agit. Silencieuse, invisible, sans motivations clairement revendiquées, semblable au terrorisme. Il est alors vital que chaque Etat constitue et renforce ses moyens de défense. Mais les conflits conventionnels nous ont montré par le passé que leur efficacité est conditionnée à la vigilance, au soutien et, éventuellement à la participation des citoyens. Au quotidien et dans la durée. Il ne s'agit évidemment pas faire prendre des armes à la population, mais de lui apprendre à détecter des situations à risque, à les neutraliser, et à alerter les services compétents pour les détruire. Faire prendre conscience à chacun qu'il est un acteur de la cyberdéfense, que ce soit dans son environnement personnel ou professionnel, tous les jours et en toutes circonstances !

Quittons maintenant ce climat guerrier et anxiogène pour recoller à notre quotidien. Et étudions comment le pragmatisme et le bon sens peuvent une fois de plus permettre d'éviter de se retrouver en situation cyber-délicate.

Chéri, on sonne à la porte !

Près de 90% des attaques sont réalisées par phishing, technique qui consiste à inciter la cible à cliquer sur un lien frauduleux. Vous est-il arrivé, étant jeune (ou moins jeune), d'appuyer sur tous les boutons d'un interphone en bas d'un immeuble dans l'espoir que quelqu'un vous ouvrira



BIO

Diplômé de l'université de La Rochelle dans les métiers du Génie Civil, et passionné très tôt par l'univers informatique, Dominique Maïano, établit très rapidement un lien entre ce domaine en pleine expansion et les processus d'analyse fonctionnelle qu'il met en œuvre dans le monde des travaux publics. Homme de convictions, Il obtient en 1994 un poste d'enseignant informatique dans l'éducation nationale. En 2002, il crée l'entreprise Maïano Informatique, qui ne cessera de se développer pour apporter un panel de solutions le plus large possible à ses clients. Visionnaire, Dominique fait très tôt évoluer son entreprise pour proposer ses services en mode MSP. Conscient de la complexification des technologies et des questionnements de ses clients, Dominique et ses équipes construisent des réponses concrètes et pragmatiques aux besoins des entreprises afin de garantir leur productivité, leur sécurité et l'adaptation de leurs outils à leur développement.
Ses expériences d'ingénieur et d'enseignant permettent à Dominique de transmettre sa passion de l'informatique avec une grande pédagogie, pour le plus grand bénéfice de ses clients.

la porte sans demander qui vous êtes ? Oui qui se contentera d'un "c'est moi !" ? C'est ça le phishing. Ce n'est pas de la technologie, c'est de la manipulation mentale. Et la technologie est loin d'être suffisante pour s'en prémunir.

Bon sens, observation et réflexion…

De nombreux éditeurs proposent aujourd'hui des outils visant à mesurer l'exposition aux risques des utilisateurs et à la réduire par la mise en place de bonnes pratiques. Leur fonction est essentiellement de faire prendre conscience aux utilisateurs des techniques élaborées et souvent invisibles


Mardi 19 Décembre 1837. 60 FRANCS PAR AN. Annonces 75 cent. la ligne.

LE BON SENS

Journal de la Démocratie.

Paris et les départemens, un an, 60 fr.; six mois, 30 fr.; trois mois, 15 fr.—Étranger, 76 fr. par an.— Feuille du dimanche, Paris, 40 fr. par an; départemens 42 fr.
Les bureaux sont rue du Croissant, 16, hôtel Colbert.

des cybercriminels pour acquérir les réflexes d'évitement. Comme souvent, les pratiques les plus simples sont les plus efficaces.

Reprenons l'exemple de l'interphone. Vous êtes chez vous et votre interphone sonne. "C'est qui ?", "C'est moi". La situation à risque est créée. Il va falloir vous assurer de l'identité de ce "c'est moi" et valider l'objet de sa visite. Ces vérifications faites, vous pourrez décider en conscience de lui ouvrir la porte…

Autrefois grossières, les attaques par phishing exploitent les techniques du marketing les plus abouties. Les emails sont bien construits, sans faute d'orthographe, et très proches graphiquement des emails des entreprises qu'ils copient. L'email n'est plus le seul support ; Les réseaux sociaux et les messageries instantanées sont également exploitées pour usurper les identités des individus. Il est donc indispensable de suivre quotidiennement l'évolution des pratiques cybercriminelles, de sensibiliser les utilisateurs et de vérifier quotidiennement leur exposition au risque.

Il y a quelqu'un dans mon salon !

Aucun système de cyberprotection ne garantit à 100% contre les malveillances. Si La prévention est bien entendu fondamentale, elle n'est pas suffisante. Il est donc nécessaire d'élaborer une stratégie de réaction si un piratage est détecté sur votre système.

Malgré votre clôture et vos verrous sophistiqués, votre système d'alarme vous avertit qu'un individu s'est introduit dans votre domicile. Vous en concluez facilement qu'il est mal intentionné, et peut-être dangereux. Le bon réflexe dans cette situation est de ne surtout pas intervenir, mais de vous mettre en sécurité et d'alerter les forces de l'ordre, plus aptes et mieux équipées que vous pour agir.

Il en est de même pour la sécurité de votre système informatique : l'anti-virus n'est qu'une pièce de l'arsenal à déployer pour assurer la résilience de vos données, qui doit être complétée par une sauvegarde et une protection périmétrique efficaces. On l'a vu, les techniques de cybercriminalité sont sophistiquées, et il serait illusoire de penser pouvoir gérer seul une attaque. L'assistance de spécialistes formés, organisés et équipés contre les cybercriminels est déterminante, pour une réponse immédiate avec des moyens proportionnés.



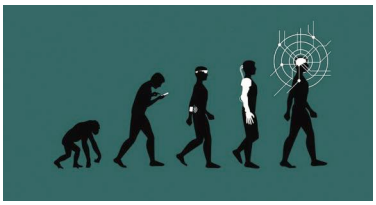


La serrure était grippée …

L'entretien permanent de votre parc informatique est le premier garant de votre sécurité. Des failles de sécurité sont régulièrement détectées sur vos logiciels, et font rapidement l'objet de correctifs. Leur efficacité n'est réelle que si ces mises à jour sont réalisées immédiatement afin de réduire au maximum l'ouverture de la "fenêtre de tir" disponible pour les cybercriminels.

Plus généralement, l'inspection continue de l'intégrité et du bon fonctionnement de vos systèmes est un gage non seulement de sa sécurité, mais surtout de la productivité de votre entreprise. Les cyberattaques sont foudroyantes et peuvent paralyser votre activité en quelques minutes. Le mode réactif n'est plus d'actualité : La maintenance proactive de vos équipements n'est pas une option.

Ne restez pas isolé !



S'appuyant sur des technologies en constante évolution, les cybercriminels mènent une guerre de harcèlement en s'attaquant aux failles les plus étroites des outils de notre quotidien. Pour y faire face, les éditeurs et équipementiers nous proposent des solutions élaborées, capables de s'adapter rapidement aux nouveaux types d'attaques. Le risque serait de considérer qu'il suffit d'installer ces solutions pour être définitivement en sécurité.

La cybersécurisation d'un système informatique est un ensemble complexe composé de stratégies définies par les enjeux particuliers, de compétences techniques et d'expérience, et de haute technologie. C'est une lutte de tous les jours, qui nécessite une organisation et des ressources dédiées, dont la majorité des entreprises ne disposent pas.

MSP : Meilleur Service de Protection ? Pas seulement…

Depuis quelques années, un nombre grandissant de prestataires informatiques ont transformé leur modèle économique pour répondre plus efficacement aux enjeux de la cybersécurité. Appelés MSP (Managed Services Providers), ces professionnels surveillent en permanence vos systèmes et les maintiennent en condition opérationnelle, anticipent et préviennent les incidents, et vous permettent de faire évoluer votre infrastructure en fonction de votre activité et de vos enjeux.

Sorte d'infogéreur 2.0, le MSP gère à distance votre infrastructure informatique, quelle que soit sa taille et sa complexité, de manière proactive



et sous un modèle forfaitaire. L'objectif d'un MSP est de prendre en charge l'intégralité de votre système afin que vous puissiez vous concentrer exclusivement sur votre activité. Il assure le bon fonctionnement de votre informatique, et donc la productivité de votre entreprise.

Le MSP fournit un large panel de services comprenant la supervision, la gestion des alertes, la maintenance et la résolution des incidents de tout ou partie de votre infrastructure, en fonction du périmètre défini avec lui. Alors que nos environnements technologiques se diversifient et deviennent de plus en plus complexes, le MSP vous apporte un support utilisateur pointu et pluridisciplinaire, quasiment impossible à réaliser avec des ressources internes.

Bien qu'équipé des outils les plus aboutis pour assurer ses obligations contractuelles, le MSP s'appuie avant tout sur une méthodologie éprouvée pour vous apporter un service continu et efficace :

- Inventorier
- Documenter
- Superviser
- Maintenir
- Intervenir
- Supporter
- Conseiller
- Partager l'expérience

Cette organisation vertueuse, basée sur la documentation de toute action réalisée sur votre infrastructure, assure une connaissance précise et partagée, exploitable par l'ensemble des intervenants. Point notable, cette documentation vous appartient et garantit de ce fait votre souveraineté informatique. Elle s'applique à l'ensemble de votre périmètre, qu'il s'agisse des postes de travail, des serveurs, du réseau, de vos outils de communication, de votre stockage et de vos sauvegardes, en local et dans le Cloud.

Enfin, le MSP est le garant de votre résilience informatique : Il vous accompagne dans la mise en place de l'ensemble des processus nécessaire au maintien de votre activité, quels que soient les risques auxquels elle est exposée (piratage, incendie, vol, catastrophe naturelle, etc…). Au-delà des solutions de cybersécurité qui, nous l'avons vu, n'offrent pas une protection étanche à 100%, le MSP vous proposera les dispositifs de sauvegarde et de continuité ou reprise d'activité (PRA/PCA) adaptés à vos enjeux de productivité.

Qu'il s'agisse d'un grand groupe disposant d'une DSI, ou d'une TPE aux moyens plus limités, les entreprises réclament un système d'information toujours plus performant, et à minima disponible et opérationnel. La complexité des environnements techniques rend une gestion en interne difficile, voire impossible. Plus qu'une simple maintenance assurée par une équipe d'experts, le MSP procure aux entreprises une vision élargie, stratégique et visionnaire de leurs systèmes d'information.

De quoi se sentir moins seul dans cette jungle technologique ! ■



L'agriculture, un secteur stratégique exposé à la cybercriminalité



MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Gendarmerie Nationale

Auteur : Stéphane MORTIER

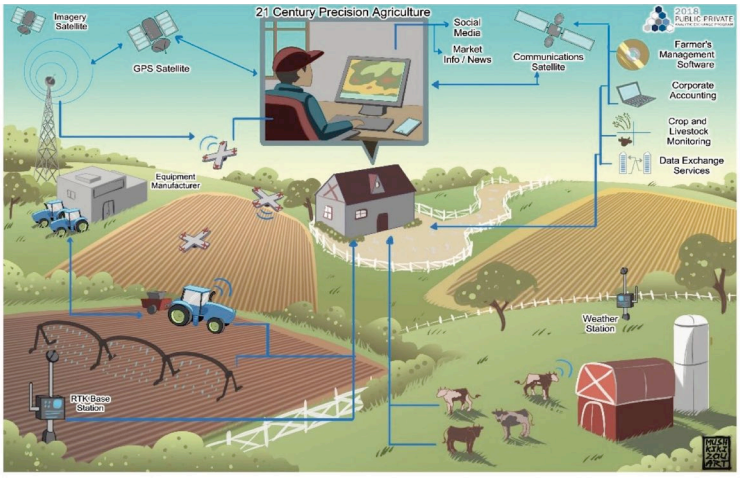
Le règlement européen n°2019/452 du Parlement européen et du Conseil du 19 mars 2019 établissant un cadre pour le filtrage des investissements directs étranger dans l'Union met en place des mécanismes de coopération entre États membres et avec la Commission européenne pour contrôler les investissements directs étrangers liés à des secteurs européens sensibles. Parmi ces secteurs sensibles, stratégiques, figurent l'approvisionnement en intrants essentiels, y compris l'énergie ou les matières premières, ainsi que la sécurité alimentaire et la cybersécurité. Agriculture, agroalimentaire et cybersécurité sont donc au nombres des activités stratégiques au sein des pays membres de l'Union.

Dans l'imaginaire collectif, l'agriculture reste une activité liée à la terre, tout au plus on imagine du matériel agricole imposant mais uniquement mécanique. Or il en est tout autre, l'agriculture du 21ème siècle est particulièrement précise, innovante et connectée. Les risques pesant sur une exploitation agricole ne sont plus uniquement des risques naturels mais aussi, et de plus en plus, des risques "cyber".

Quels sont ces risques ? L'agriculture étant stratégique elle est d'autant plus exposée. Les conséquences d'une cyberattaque visant ce secteur d'activité peuvent être multiples et particulièrement importantes.

2018 Public-Private Analytic Exchange Program

Threats to Precision Agriculture



BIO

Docteur en sciences de gestion (Paris 1 Panthéon-Sorbonne), Stéphane est spécialiste de l'intelligence économique et de l'Afrique et à ce titre, il enseigne à l'École de Guerre Économique de Université de Likasi (RDC), où il est Conseiller du Recteur, en sus d'être membre de l'Association pour l'Unification du Droit en Afrique (UNIDA). Il est également membre de la communauté des chercheurs du Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale (CREOGN)

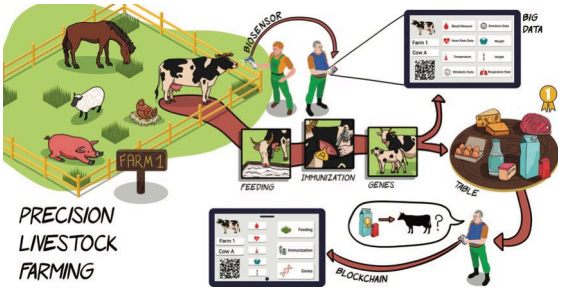
En 2018, aux États-Unis, le département de la Sécurité intérieure (Department of Homeland Security, ou DHS) publie un rapport sur les cybermenaces en collaboration avec le FBI et le département de l'Agriculture1 dont l'image particulièrement évocatrice de l'agriculture moderne, dite "de précision", ci-dessous est issue. Cette image montre quelles sont les réalités de l'agriculteur actuel, réalités dépassant l'imaginaire collectif !

On y parle de la "précision" en agriculture. Les agriculteurs ont toujours recherché des méthodes pour réduire les coûts et augmenter la production. Au travers des semoirs et des systèmes de gestion automatisés du bétail, des trayeuses connectées ou encore des dispositifs autonomes de distribution d'aliments, les agriculteurs recueillent des données leur permettant de prendre des décisions. "L'agriculture de précision moderne" n'est pas nouvelle et depuis les années 1960, elle n'a cessé de s'adapter aux nouvelles technologies, intégrant notamment l'utilisation des satellites et des réseaux informatiques. Cela se traduit par exemple par l'application de la quantité optimale de nutriments, de semences et de pesticides au bon endroit, au bon moment, en utilisant le bon produit et la bonne quantité pour maximiser le rendement des cultures, économiser du temps et de la main-d'œuvre.



L'élevage de précision2 est un ensemble de techniques regroupant différents outils numériques innovants : capteurs (mouvements, température), détecteurs (caméras, microphones), technologies de gestion et automates visant un pilotage précis et continu des animaux et des systèmes de production. Leurs applications sont multiples : optimiser les performances techniques et économiques du système de production, améliorer les conditions de travail de l'agriculteur (automatisation de la traite, détection des chaleurs, …), diminuer leur isolement (applications de communication,…), favoriser le bien-être des animaux (détection de stress, de problèmes sanitaires…), réduire l'impact environnemental des élevages (meilleure gestion des intrants : alimentation, produits vétérinaires,…).

Que ce soit dans les cultures ou dans l'élevage, l'agriculture de précision procure ainsi des avantages environnementaux : réduction des intrants requis, de la consommation d'énergie et des déchets. Elle contribue également à la compétitivité de l'agriculture.



Une telle agriculture, connectée, est confrontée à une série de menaces d'ordre "cyber". En effet, en sus des aléas du climat, des dégâts occasionnés par le gibier ou encore du cours des matières premières concernées, l'utilisation des nouvelles technologies ouvre la porte à tout un panel de menaces nouvelles et évolutives. Il est possible de les classer en trois catégories, à l'instar de ce qui a été fait dans le rapport américain de 2018 susmentionné : les menaces principales, d'ordre général, les menaces relatives à l'intégrité des données et enfin à la disponibilité des équipements utilisés.

Les menaces principales, d'ordre général

Elles concernent la confidentialité des données, qui est une préoccupation majeure pour l'agriculture de précision. Les agriculteurs disposent de données sensibles, stratégiques voire confidentielles (données sur le rendement, prix des terres, santé du bétail,...). La perte ou l'utilisation abusive de ces données pourrait engendrer des conséquences financières mais également sociales et émotionnelles. Le risque réputationnel est intimement lié à de telles conséquences tant pour l'agriculteur que pour les fabricants d'équipement et de logiciels.

Quatre menaces principales peuvent être relevées :

- **Vol ou fuite de données.** Des systèmes de gestion de l'information agricole, des applications mobiles,… sont conçus pour accompagner les agriculteurs. Comme tout système, ils peuvent contenir des failles plus ou moins importantes. Il convient alors de les mettre régulièrement à jour et de privilégier des opérateurs pérennes et reconnus. L'histoire récente nous a démontré que des systèmes d'exploitations non-mis à jour pouvaient amener des catastrophes (WannaCry, NotPetya,…).
- Publication intentionnelle d'informations confidentielles pour nuire à l'entreprise, la fragiliser ou la déstabiliser. La diffusion publique d'informations telles que des prix, négociés confidentiellement avec chaque client pourrait avoir des répercussions catastrophiques pour le fournisseur, en détruisant les relations de confiance par exemple. Il s'agit d'une menace particulièrement importante au regard de la viralité de l'information sur les réseaux sociaux par exemple..

▸ Accès d'une puissance étrangère a des données stratégiques, y compris captées par les drones agricoles. Les principaux fabricants d'équipements sur le marché agricole de précision sont situés à l'étranger. Un gouvernement étranger pourrait être intéressé par les données agricoles d'un autre État ; rappelons que l'agriculture est un secteur stratégique en Europe. La captation d'images par les drones agricoles qui seraient détournées vers un "État concurrent" constitue une réelle menace potentielle.

▸ Vente illégales de données sensibles. Les données stratégiques ont toujours une valeur pour quelqu'un, et plus encore pour un acteur malveillant. Un courtier en matière première pourrait être friand de données agricoles confidentielles… Un cybercriminel n'hésitera pas à les lui vendre...



Les menaces à l'intégrité des données

L'agriculture de précision n'est autre que la "smart-agriculture" avec l'utilisation de capteurs de données dans les secteurs des cultures et de l'élevage. La collecte et l'exploitation des données constituent un outil d'aide à la décision en temps réel. Alors que l'agriculture de précision adopte de plus en plus l'automatisation des équipements, la robotique, l'apprentissage automatique et l'informatique de pointe, les menaces à l'intégrité des données se manifestent de façon croissante voire exponentielle.

▸ **Falsification intentionnelle de données.** Une épizootie dans le cheptel d'un État, par exemple, peut causer des perturbations économiques massives, des problématiques de commerce extérieur et surtout des répercussions réelles sur la sécurité alimentaire. Confirmer ou infirmer l'épizootie implique des travaux de terrain et de laboratoire qui prennent un temps plus en moins long. Un acteur malveillant, qui publie de fausses données imitant les données agricoles réelles avant ou pendant la survenance de la maladie comme la fièvre aphteuse, la brucellose ou encore la peste porcine, pourrait brouiller les pistes pendant des mois pour lever le doute. Ce temps ne peut être mis entre parenthèse sur les marchés agricoles et commerciaux étrangers. Il en irait de même pour les cultures (maladie, pesticides, modification génétique,…). Il s'agit d'une atteinte facile à mettre en oeuvre, car elle ne repose pas sur l'accès original à des données réelles.

▸ **Introduction de données douteuses dans un réseau.** L'introduction de données fausses ou biaisées pourrait avoir une incidence sur une culture ou un cheptel. Dans les secteurs des cultures (légumes, fruits, céréales, vignes, oléagineux,...), la mise en œuvre de capteurs intelligents de données est très importante. Ceux-ci sont connectés via des réseaux cellulaires, Bluetooth ou Wi-Fi, et beaucoup comptent sur l'informatique de bord pour prendre des décisions à la source. L'introduction de données douteuses dans ces réseaux pourrait, intentionnellement ou par l'intermédiaire de capteurs défectueux, entraîner des problèmes comme par exemple une modification de l'arrosage d'une culture et ainsi la détruire. Le même scénario pourrait s'appliquer aux bâtiments agricoles "intelligents" construits pour gérer du bétail. Des capteurs défectueux pourraient avoir des effets néfastes sur la santé ou entraîner la perte d'animaux (modification de température, dosage des aliments, perturbation de la traite, système d'aération,...).

▸ **Modélisation du machine learning insuffisamment vérifiée.** Les techniques d'apprentissage automatique sont de plus en plus régulièrement déployées dans des applications agricoles de précision. Des algorithmes insuffisamment modélisés, des données aberrantes et des biais inhérents aux données elles-mêmes se glissant dans les modèles prédictifs peuvent produire des effets indésirables et non intentionnels. Il s'agit d'une menace naissante et évolutive qui prendra en importance avec le temps.

Les menaces relatives à la disponibilité

Les exploitations agricoles sont fortement tributaires de l'équipement. Le matériel agricole principal est un système qui s'appuie sur des outils intégrés complexes et un ensemble sophistiqué de systèmes de communication et d'orientation. Les menaces liées à la disponibilité de l'équipement se manifestent à la fois dans les domaines "cyber" et des catastrophes naturelles.

▸ **Disponibilité de l'équipement selon le calendrier agricole.** Pour chaque secteur de culture, il existe des fenêtres très étroites et précises pour la plantation et la récolte où l'équipement doit fonctionner. La perte d'équipement pendant ces fenêtres clés pourrait empêcher la plantation pendant la période optimale ou retarder la récolte, ce qui entraînerait une perte de la qualité des cultures. Si un acteur malveillant identifie une vulnérabilité dans une pièce d'équipement, il peut perturber des milliers de machines à la fois. Il en irait de même pour un correctif mal conçu qui verrouillerait des quantités importantes d'équipement. Les conséquences sur la sécurité alimentaire seraient alors inéluctables. Il en irait de même pour la réputation du fabricant de l'équipement concerné. Il s'agit d'une menace avec conséquences possibles sur la souveraineté alimentaire d'un État par exemple.

▸ **Perturbation des systèmes de synchronisation et de positionnement.** Le spectre des fréquences est à lui seul un secteur stratégique. Or il est de plus en plus encombré. Les agriculteurs font régulièrement face à une forme de perte de signal de guidage. GPS,



GLONASS ou Galiléo, lorsque le système de guidage utilisé est étranger, l'accès pourrait être refusé en cas de crise ou de conflit, ce qui limiterait la capacité de production agricole. Il s'agit d'une menace qui touche tous les secteurs d'activité mais l'impact en matière d'agriculture serait incontestablement important.

▸ **Le positionnement cinématique en temps réel** est une technique utilisée pour améliorer la précision des données de position dérivées des systèmes satellitaires. Il permet à l'agriculture de précision de passer de la précision du mètre à celle du centimètre pour la plantation des semences, l'application d'intrants agricoles et l'alignement des cultures en rangs. Elle exige que les stations de base traitent et raffinent les signaux spatiaux. La perte de plusieurs stations de base pourrait avoir une incidence sur les applications agricoles de précision au niveau d'une région entière. Notons que les catastrophes naturelles peuvent détruire des stations de base. Risque "cyber" et naturel s'enchevêtrent à nouveau.

▸ **Perturbation des réseaux de communication.** Les exploitations agricoles sont essentiellement rurales. L'agriculture de précision est construite sur des réseaux de capteurs distribués nécessitant des niveaux toujours croissants de transfert de données. Le manque de fiabilité de la bande passante en milieu rural est parfois un facteur limitatif à l'adoption de l'agriculture de précision. Elle peut impliquer notamment une perte de signal qui engendre à son tour une indisponibilité de l'équipement. Les agriculteurs utilisent un "mille-feuille" de réseaux cellulaires, Bluetooth et Wi-Fi, et comptent encore beaucoup sur les clés USB pour transférer manuellement des données. Cela constitue autant de faille et de portes ouvertes aux acteurs malveillants.

▸ **Chaîne d'approvisionnement étrangère pour les équipements.** En sus des risques liés à l'intégrité des données, les équipements fabriqués à l'étranger pourraient être désactivés à distance (accès par porte dérobée, code malveillant,...). Il s'agit là également d'une problématique de souveraineté nationale (ou régionale).

▸ **Défaillance de l'installation intelligente de production animale.** De plus en plus complexes, les bâtiments connectés abritant et gérant du bétail ouvrent de vastes possibilités aux cybercriminels. Les systèmes CVCA (Chauffage, ventilation, conditionnement d'air) ou les systèmes d'alimentation pour les cyberacteurs malveillants, une défaillance logicielle ou une erreur humaine, qui pourraient entraîner une perte potentielle de bétail.

Voici en quelques lignes les menaces identifiées qui pèsent sur l'agriculture de précision. Il n'est pas inintéressant de mettre cela en perspective avec les grands enjeux de notre monde actuel. Nous en retiendrons trois : la transition numérique, la protection de l'environnement et la croissance démographique.

Au regard de la croissance de la population mondiale (à titre d'exemple, la population de l'Afrique va doubler d'ici à 2050), il est impératif de développer une agriculture innovante pour nourrir l'Humanité. Cette agriculture doit allier productivité, compétitivité, qualité et respect de l'environnement. Le moyen d'y parvenir est l'utilisation des outils et moyens numériques. C'est, semble-t-il, inéluctable. Or l'usage des nouvelles technologies, des réseaux et du cyberespace expose l'agriculture à de nouvelles menaces, parfois très concrètes pour l'exploitant, parfois relevant de la souveraineté nationale comme nous l'avons vu. L'agriculture est depuis peu en Europe un secteur d'intérêt stratégique, au même titre que la cybersécurité, l'énergie, les réseaux de transport,… L'impératif de sécurité (et de cybersécurité) quant à ces différents secteurs ne peut qu'être un vecteur d'accompagnement de nos agriculteurs vers l'agriculture de demain, vers une agriculture de précision, empreinte de progrès.



Voici un portrait du monde agricole tel qu'on ne le montre que rarement : un monde connecté, stratégique, humaniste aussi mais tout autant vulnérable, fragile et exposé. ■

Cyber-attaque chez Cérèsia (année 2020).



Auteur : Olivier Bacon

En 2020 le groupe Cérèsia a connu une cyberattaque importante paralysant l'ensemble des applications et donc leur utilisation par l'ensemble de l'entreprise. Comme la plupart des entreprises nous n'étions pas préparés à ce type d'accident même si notre système d'information, testé 2 ans auparavant, était réputé comme quasi à niveau en terme de sécurité au regard de notre activité.

L'effectivité de l'attaque a eu lieu la veille d'un week-end afin de compliquer notre capacité à intervenir. A cette période nous réfléchissions à la souscription d'une assurance cyber-sécurité … L'entreprise a été très réactive avec une première réunion de crise dès le lendemain, un dimanche. Notre réaction a été la bonne : prendre le dossier calmement et sans précipitation.

Le fait d'avoir eu à gérer une situation de crise au travers la situation COVID connue en 2020 nous a aidé par l'effet d'expérience. D'autre part nous avons eu la chance que la production de notre activité puisse se faire en mode dégradé dès le lundi matin sans les outils informatiques. Les services supports ont été les plus impactés.



L'union

Les conséquences de la cyberattaque chez Cérèsia à Reims

MIS EN LIGNE LE 11/12/2020 À 14:00 JULIEN BOUILLÉ

REIMS (MARNE) COOPÉRATIVE POLITIQUE RANDSTAD HOLDING N.V.

L'entreprise fonctionne, assure la direction. Mais , papiers et crayons ont remplacé les ordinateurs dans l'attente de la relance des systèmes d'information. - DR



La gestion de cette crise a été largement facilitée par l'approche de l'entreprise. Même si la pression était présente le service informatique n'a pas subi de pression interne que ce soit des métiers, de la direction comme de la gouvernance. C'est le point le plus important pour le rétablissement de nos outils afin de ne pas faire d'erreur sur la remise en service des systèmes.

La partie coût n'est pas l'élément primordial du préjudice subi, estimé à 400 K€. On peut considérer que moitié des dépenses réalisées auraient dû l'être à moyen terme pour un niveau de protection amélioré.

Partant du principe qu'aucun schéma technique n'est inattaquable, je retiens 2 facteurs majeurs dans une situation de cyber-attaque : les sauvegardes et la capacité à recharger les données comme les applis. Les techniques d'attaque évoluant chaque jour, nous devons "accompagner" cette évolution.

BIO

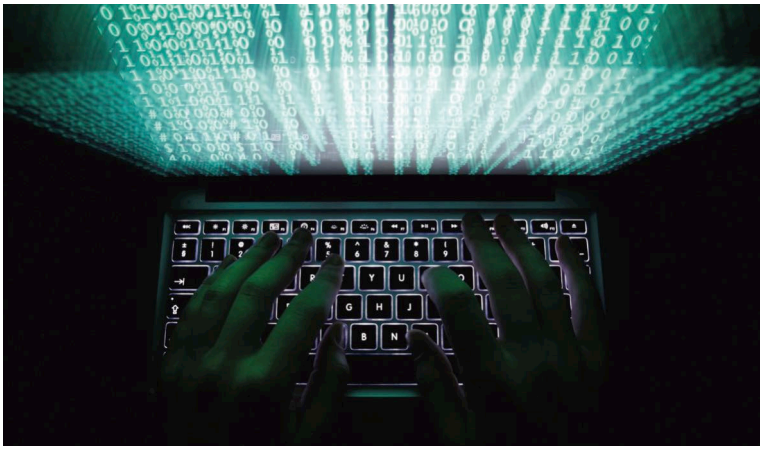
Olivier Bacon est directeur des opérations au sein du Comité de Direction du groupe Cérèsia.



Au final nous avons décidé l'embauche d'un RSSI afin d'opérer en permanence sur ce sujet. Pour le futur, le plus compliqué n'est pas la partie technique mais le changement des habitudes de chacun.

D'un point de vue chronologique les événements se sont déroulés comme suit :

Le vendredi 6 novembre 2020 à 23h42 une connexion en provenance du darknet a été identifiée sur le portail d'accès au télétravail. Le lendemain des fichiers malveillants seront déposés sur ces mêmes serveurs. Dans la



continuité, une élévation de privilège s'opère et les attaquants ont par conséquent acquis les droits administrateurs sur le domaine.

Durant les jours qui ont suivi, plusieurs connexions ont été observées sur différents serveurs et un dossier contenant les informations récoltées sera créé.

Le samedi 21 novembre, marque la fin de la période d'observation, la charge est introduite dans le système et une tache automatique, destinée à chiffrer les serveurs, est créée. Comme souvent, les attaquants cherchent à maximiser le temps avant la détection et la réaction. L'attaque est lancée à l'entrée du week-end.

Le dimanche 22 novembre est organisé la première cellule de crise rassemblant le service informatique, les métiers, la direction et la gouvernance.

Le lundi 23 novembre, la propagation est contenue et la demande de rançon est présente sur les postes. Notre prestataire d'infogérance est appelé pour aider à la résolution. Un dossier de collecte des preuves est constitué. On trouvera quelques jours plus tard le fichier de rançon qui est lui-même porteur d'un malware.

Début décembre, l'évaluation du système se termine et les premiers signes de reprise se font sentir. L'annuaire d'entreprise et le système RH sont les premiers objectifs de restauration et sont déjà partiellement disponibles. Conjointement, un plan de restauration est établi et les objectifs sont priorisés.

L'application de comptabilité est identifiée comme l'application prioritaire qui suivra les actions déjà entamées.

Mi-décembre le rapport d'analyse post-attaque est livré, la cible de reconstruction est définie et commence. L'annuaire d'entreprise et la paye sont les premiers objectifs. A ce stade, 10 applications sont restaurées, le logiciel de comptabilité est de nouveau exploitable. Le chantier de reconstruction continue et les 2/3 des applications sont restaurées.

Fin décembre, d'importantes complications impactent la reprise de certaines applications du fait de la désynchronisation des données qui remonte à la date où la sauvegarde a été faite. L'un des plus gros chantiers commence alors, le réalignement des applications restaurées avec le présent des domaines fonctionnel. La reconstruction de l'environnement de travail des utilisateurs du système d'information commence.

De janvier à mars les applications vont se rouvrir progressivement.



Il faudra encore 2 mois afin que le système d'information soit stabilisé. ■

Acteurs du tourisme : protégez vos données personnelles et celles de vos clients !



Auteur : Lisa CROIZET

Problématique :



Si la donnée constitue un enjeu majeur pour les acteurs du tourisme, la donnée personnelle est une mine d'or pour les services marketing : elle permet de qualifier son fichier client, de proposer une communication ciblée de plus en plus fine, de personnaliser l'offre, de fidéliser... Mais attention, l'utilisation de données à caractère personnel est encadrée et il convient d'être en conformité pour limiter de nombreux risques.

BIO

Lisa est conseillère-formatrice en protection des données au sein du service Confiance numérique de Soluris (Solutions Numériques Territoriales Innovantes), certifiée Déléguée à la protection des données par l'AFNOR - 2021-2024, Lisa CROIZET accompagne depuis 2018 plus de 500 collectivités en Charente-Maritime.

Qu'entend-on par donnée personnelle ?

C'est toute information qui permet d'identifier une personne physique directement ou indirectement : nom, prénom, adresse, âge, photo, numéro de carte bancaire… la liste peut être longue !

Quel cadre juridique ?

Depuis le 25 mai 2018, le RGPD, règlement général sur la protection des données - complété en France par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés "modifiée" -encadre l'utilisation des données à caractère personnel. Il impose un ensemble de mesures juridiques, techniques et organisationnelles aux structures relevant des secteurs publics comme privés.

Comment mettre en place sa conformité au RGPD en 8 points ?

Pour accompagner les professionnels à leur mise en conformité, la CNIL - Commission Nationale Informatique et Libertés - propose des outils adaptés (modèle de registre, formulaires, référentiels, conseils…). La liste ci-dessous donne les grandes étapes de la démarche :

1. Identifier les rôles et responsabilités au sein de l'organisation : responsable du traitement, délégué à la protection des données…
2. Recenser les traitements de données à caractère personnel dans un registre et identifier les risques pour la vie privée des personnes concernées
3. Evaluer la conformité des traitements, de l'organisation et des sous-traitants
4. Définir et mettre en œuvre les procédures de gestion des données personnelles en priorisant les actions en fonction des risques
5. Respecter les droits des personnes concernées en informant et gérant les demandes
6. Communiquer, former et sensibiliser pour développer une culture de protection de la donnée
7. Sécuriser les données
8. Documenter la conformité.

Enfin, pour savoir où vous en êtes en gestion de la protection des données, une autoévaluation de maturité est désormais disponible sur le site de la CNIL (https://www.cnil.fr/sites/default/files/atoms/files/autoevaluation_de_maturite_en_gestion_de_la_protection_des_donnees.pdf).

Autoévaluation de maturité en gestion de la protection des données

Un modèle pour se positionner et choisir les actions à mener

Quels sont les risques en cas de non-conformité au RGPD ?

D'un point de vue juridique, avoir mis en place une organisation pour répondre aux demandes d'exercices de droits des personnes concernées évite les plaintes éventuelles et les contrôles de la CNIL (les sanctions peuvent aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire mondial).

Au niveau technique, le RGPD impose la mise en place de mesures de sécurité qui permettent de limiter les risques de cyberattaques et de violations de données. Précisons, que depuis 2017, les contrôles de la CNIL relevant des manquements à la sécurité représentent 40% des sanctions sur ce seul fondement *(Source : CNIL- Cybersécurité - Chiffres 2020 et informations)*. Les pertes financières ne sont pas seulement dues aux risques de sanctions mais aussi aux conséquences des cyberattaques : arrêt temporaire de l'activité, demandes de rançons, faux ordres de virements etc… Rappelons qu'en 2018, Mariott a été la cible d'un piratage d'envergure se faisant voler plus de 500 millions de données de clients. EasyJet, Misterfly et bien d'autres encore en ont fait également les frais !

Enfin, la réputation de la structure (suite à une sanction rendue publique, à une violation de données, …) peut être atteinte et avoir de sérieuses conséquences (perte de confiance, de clientèle, de chiffre d'affaires…)



Quelles opportunités d'entreprendre une démarche de conformité au RGPD ?

La démarche implique l'appropriation d'une méthode : la gestion des risques. Elle permet un diagnostic précis des processus de la structure puis de définir un plan de progrès : c'est l'occasion de qualifier son fichier client mais aussi de s'améliorer en interne !

La protection des données personnelles c'est aussi celle des salariés : l'approche transversale permet de mobiliser tous les acteurs de l'organisation de près ou de loin : elle fédère les équipes qui travaillent sur un projet commun et instaure un climat de confiance.



Enfin, protéger les données de ses clients, être transparent sur l'utilisation des données permet aussi de mieux communiquer et de fidéliser la clientèle ce qui peut présenter un réel avantage concurrentiel.

N'attendez plus pour démarrer !



"En période de crise, les budgets sont revus à la baisse", "ce n'est pas le sujet prioritaire", …les arguments pour reporter la démarche existent mais n'oublions pas que ce qui est fait aujourd'hui portera ses fruits demain. On peut agir avec des mesures simples et proportionnées. Bien s'organiser, communiquer et sensibiliser est un élément essentiel et les mesures techniques doivent elles aussi être appropriées. Le plus difficile c'est de se lancer : commençons ensemble au CMCS (Charente-Maritime Cybersécurité) du 11 au 14 octobre à La Rochelle ! ■

Quels business models pour le tourisme de demain ?



MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Gendarmerie Nationale

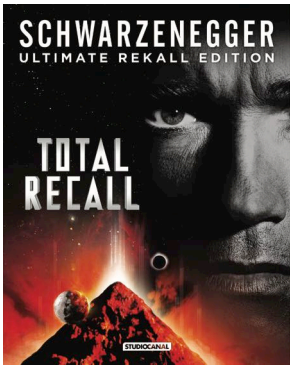
Auteur : Stéphane MORTIER

Liminaire

Le tourisme, à l'instar de nombreux autres secteurs d'activité, évolue, de façon essentiellement incrémentale. Cette marche traditionnelle n'exclut toutefois pas la rupture dans l'offre touristique et dans le *business model*. Les plateformes de réservation en sont un exemple, les bornes interactives un autre. La crise de la COVID-19 a particulièrement touché le secteur du tourisme qui subit de plein fouet les règles sanitaires. Non seulement les déplacements des individus étaient, et sont toujours, limités mais également des protocoles sanitaires ont bouleversé l'accueil du public. Par conséquent, tout l'environnement du tourisme a été et continue d'être impacté. Toute l'activité touristique doit se repenser, toute sa chaîne de valeur doit être repensée, le touriste lui-même est en pleine mutation.

BIO

Docteur en sciences de gestion (Paris 1 Panthéon-Sorbonne), Stéphane est spécialiste de l'intelligence économique et de l'Afrique et à ce titre, il enseigne à l'École de Guerre Économique de Université de Likasi (RDC), où il est Conseiller du Recteur, en sus d'être membre de l'Association pour l'Unification du Droit en Afrique (UNIDA). Il est également membre de la communauté des chercheurs du Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale (CREOGN)



La dématérialisation de l'offre touristique (visites virtuelles de musées et autres biens culturels, commandes et réservations en lignes, uberisation, utilisation de la réalité augmentée,…) était déjà une réalité avant la crise sanitaire mais semble pouvoir constituer un point de départ nouveau pour le tourisme d'après crise, le tourisme de demain. L'intelligence artificielle en sera probablement la colonne vertébrale, les neurosciences la moelle épinière.



Comme souvent la science-fiction se veut précurseur…

En 1966, Philip K. Dick publie une nouvelle intitulée "We Can Remember It for You Wholesale" (Souvenir à vendre). Elle sera adaptée au cinéma par

Paul Verhoeven avec "Total Recall" en 1990. Cette nouvelle concerne un individu qui rêve de voyager sur la planète Mars mais il ne peut s'offrir ce voyage… Il a donc recours à une société qui implante de faux souvenirs (Rekal Inc). Moyennant paiement, la société peut lui implanter des souvenirs correspondant à un voyage de deux semaines sur Mars. Il recevra ensuite par la poste des accessoires (dague martienne, photographies, exemplaires de la faune et de la flore martiennes, etc.) lui laissant penser qu'il aura effectivement vécu ce dont il croit se souvenir… Dans la nouvelle et le film, le processus d'implantation ne se passe pas comme prévu et l'individu en question vit des "aventures extraordinaires" non initialement prévues !

On va donc dans ce cas proposer des voyages qui seront marqués dans les souvenirs via un processus à définir mais qui touche aux neurosciences. Et ces souvenirs seront accompagnés par des biens matériels comme des souvenirs de vacances, des photos,…



Plus proche de nous, en 2018, le roman "Player One" d'Ernest Cline (2011) est adapté au cinéma par Steven Spielberg (Ready player one). En 2045, le monde est en proie à de nombreux soucis : crise énergétique, désastres causés par le changement climatique, la famine, la pauvreté, la guerre, etc. Dans ce monde chaotique, l'Oasis est un système mondial de réalité virtuelle, accessible par l'intermédiaire de visiocasques et de dispositifs haptiques tels que des gants et des combinaisons. Conçu à l'origine comme un Jeu de rôle en ligne massivement multijoueur (MMORPG – Massively multiplayer online role-playing game), il est devenu au fil du temps une société virtuelle dont toute l'humanité se sert comme exutoire.



Crise énergétique, changement climatique, famine, pauvreté, guerre… cela caractérise, malheureusement, assez bien le monde actuel… Dans une telle situation, les individus ont besoin d'évasion ; on leur crée donc un monde virtuel, accessible via le matériel que nous connaissons déjà (casques de réalité augmentée, gants et combinaisons haptiques1). Ce monde est étrangement similaire à l'environnement d'un jeu de rôle multijoueur… Bref, rien qui ne soit étranger à nos pratiques et usages dans le contexte actuel !

Dans un registre un peu différent mais qui est aussi une réalité, le tourisme sexuel ! "Intelligence artificielle" en 2001, adaptation par Steven Spielberg des *"Les Supertoys durent tout l'été"* de Brian Aldiss, où des androïdes sont créés pour répondre aux besoins des humains, y compris pour la satisfaction des besoins sexuels. Cela se passe évidemment dans un monde ravagé par le réchauffement climatique, dans lequel la procréation est totalement encadrée (lutte contre la surpopulation). Les androïdes assistent les humains et sont un substitut en matière de sexualité. Déjà en 1993, le film *"Demolition man"* comportait une scène de rapport sexuel entre deux acteurs connus, par l'intermédiaire d'un casque de réalité virtuelle (dans le film en 2032). Cela pose la question notamment du fantasme. *"A l'adolescence, de nouveaux fantasmes apparaissent : fantasmes érotiques liés à une sexualité qui s'éveille, fantasmes d'évasion et de liberté, fantasmes de gloire où les stars et héros tiennent le rôle de modèles identificatoires. A l'âge adulte, les fantasmes seront plus intériorisés. Ils s'ancrent dans la vie quotidienne :*



projets de reconversion, vacances, aménagement de la maison, éducation des enfants, sexualité, conflits familiaux ou professionnels, rencontres, etc. A l'échelle collective, les fantasmes - comme le fantasme de complot par exemple - alimentent les passions politiques. D'autres, comme l'idéal de l'amour romantique, accompagnent certaines mutations sociales et culturelles. Il n'est guère d'activité qui ne suscite une riche production fantasmatique" (Ethel S. Person, Voyage au pays du rêve). Imaginez que la réalisation, virtuelle mais dans le champs de la perception, de tous ces fantasmes soient à la portée d'une agence de voyage ?

Quelles implications dans le secteur du tourisme ?

Ce qui vient d'être exposé au travers de ces trois exemples de monuments de la science-fiction n'est autre qu'une étude prospective sur l'avenir du secteur du tourisme. Un véritable changement de paradigme est en train de s'opérer et la réalité rejoint, semble-t-il, la science-fiction.

L'offre touristique pourrait bientôt s'affranchir du déplacement physique des individus du fait de l'utilisation de matériels, de nouvelles technologies, permettant à chacun de voyager, de visiter, de s'épanouir et de prendre du plaisir chez lui. L'impact sur le secteur du transport serait alors particulièrement important : moins d'avion, moins de train, moins de voiture, par conséquent un besoin moindre en carburant,… Tout cela répond à nos impératifs de réduction des émissions de CO2, de respect de l'environnement,… Mais quid des constructeurs automobiles, des équipementiers, des sociétés pétrolières, de l'industrie du pneu,… de leurs sous-traitants,… et surtout de leurs travailleurs ? Une réflexion sur une réorientation ou une diversification doit absolument être menée par ces différents acteurs. Il en va de même pour l'hôtellerie, la restauration, l'offre culturelle,… Il est également urgent d'adapter la formation des futurs "voyageurs" aux réalités de demain.

L'offre touristique en tant que telle, existera toujours. C'est la forme du tourisme qui tend à se transformer et la crise de la COVID-19 joue le rôle d'accélérateur. Les univers du jeu vidéo, qui en soit sont des formes de voyage, à l'instar d'ailleurs de se plonger dans un bon roman pour les plus *"has been"* (sic) d'entre nous. Les jeux de rôle multijoueur dans lequel l'individu se crée une vie totalement parallèle et virtuelle, sont les prémices de la révolution touristique. On voyage en restant chez soi, dans son confort quotidien (ce qui correspond au développement du concept de cocooning).

Les professionnels du tourisme de demain seront donc les opérateurs de nouvelles technologies, les entités qui maîtriseront l'intelligence artificielle et la robotique mais également celles qui concernent l'aménagement des lieux privés de vie (mobilier, domotique,…), les services aux personnes (livraisons à domicile,…). Pour cette dernière catégorie, l'uberisation a déjà fait son œuvre. Le processus est donc engagé.

La place de la donnée dans le "renouveau touristique"

Il semble que le tourisme se dirige vers une option "tout à la maison" guidée par une utilisation massive des données relatives aux individus. Ce sont bien ces données qui permettront d'établir, à la carte et surtout sur mesure le voyage de rêve tant espéré. Non seulement le déplacement sera virtuel mais le voyage pourra être vécu dans la peau d'un personnage, c'est une dimension nouvelle par rapport à l'existant. Rien n'empêche le touriste de faire une traversée de l'Atlantique dans la peau de Christophe Colomb, ou encore de marcher sur la Lune aux côtés de Patrick Baudry, tout en étant confortablement assis dans un canapé signé Paulin dans un appartement du centre de La Rochelle, ou encore installé sur un banc face au Lac Léman ! Les données et leurs utilisations sont l'avenir du tourisme ; l'intelligence artificielle et ses corollaires seront alors au cœur du tourisme



de demain. Qui dit données dit recueil et protection des données et aussi éthique dans leur utilisation (RGPD,...). Les enjeux seront donc concentrés autour de celui, ou ceux, qui détiendront la donnée. Cela n'est pas sans poser de problèmes. Les plus grands opérateurs traitant de la données aujourd'hui sont généralement les GAFA, NATU et autres BATX3 qui, demain, vous feront voyager depuis votre salon. L'offre touristique sera alors concentrée dans les mains de ces grandes entreprises, souvent décriées.

De plus, le risque d'être manipulé durant ses voyages virtuels ne peut être écarté. Une société mi-virtuelle mi-réelle, façonnée par les GAFA ou autres Baidu et Alibaba, serait-elle le monde de demain, tel que sorti d'un roman de science-fiction ?

Vers quels *business models* ?

Telle est la question ? Ou plutôt quelle sera la place des *business models* actuels face au tourisme de demain ?

Les vacances bien établies (réservation ou location d'un hébergement, déplacement sur les lieux, restaurant, souvenirs de vacances et traditionnelle glace en terrasse) concernent des opérateurs qui, malgré une éventuelle volonté d'adaptation, risquent fort de disparaître. La crise de la COVID-19 nous en a montré, et ce n'est pas terminé, les prémices : hôtels vides, restaurants fermés, avions au sol,…



L'inflexion est engagée, les opérateurs traditionnels risquent de disparaître pour faire place à un tourisme totalement dénaturé et exempt de relations sociales (jusqu'aux relations sexuelles dans l'exemple susmentionné). A l'instar du *"Meilleur des mondes"* d'Huxley, les touristes seront conditionnés et voyageront, virtuellement, en fonction de leur position dans une société dématérialisée… Des cyber-citoyens bien seuls, au fond de leur canapé, dont le présent et l'avenir seront suspendus aux fils tirés par un marionnettiste appelé géant du numérique… Les *business models* du tourisme de demain sont et seront portés par ceux qui auront traversé la crise sanitaire sans encombres tels les GAFA, NATU et BATX : tout contrôler par la donnée (la publicité, la santé, la banque,... et bientôt le tourisme). ■



De l'impérieuse nécessité de s'appuyer sur un datacenter vérifié, de confiance et soumis à la législation souveraine de l'État de domicile de ses clients.

Dialogue entre Delphine CHEVALLIER, Eric ARBARETAZ et Okan TUREDI





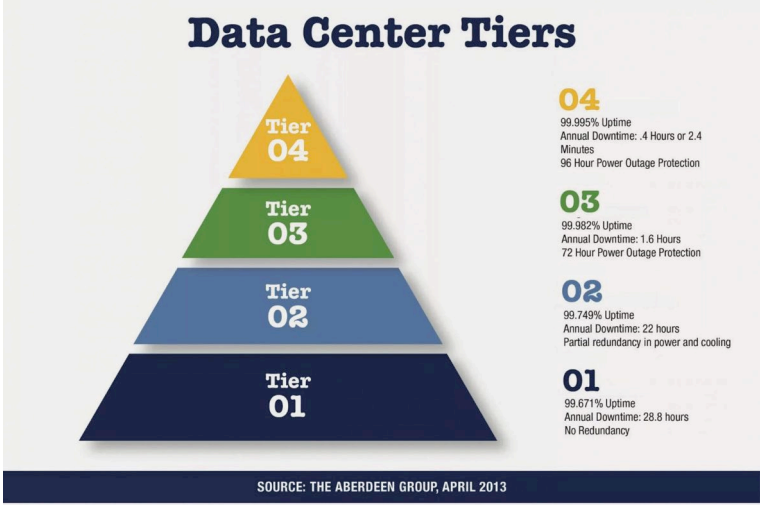
Auteur : Delphine CHEVALLIER

[Eric Arbaretaz] : Nouvellement arrivé dans l'univers des opérateurs de datacenters en France, Thésée Datacenter a ouvert les portes de son campus de Datacenters en juin 2021 et accueille actuellement ses premiers clients dans les Yvelines. La souveraineté de nos données est un enjeu majeur de nos sociétés. Thésée est un des rares acteurs français qui peut réellement garantir la sécurité des données hébergées au sein de ses datacenters. Du fait d'être une société de droit français à capitaux 100% français, Thésée est régie par les seules lois française et européenne et échappe donc à des règles de type "Cloud Act". Pour les clients cela veut donc dire que l'intégralité de leurs données informatiques sont sécurisées et ne seront jamais transmises à des tiers sans leur accord. Le Datacenter se démarque par son



approche de la sûreté en profondeur et l'utilisation des technologies les plus avancées pour assurer la protection des données contenues au sein du datacenter.

Ce bâtiment est également le premier datacenter en colocation à être certifié Tier IV en Ile de France, soit le plus haut degré de certification garantissant un site dit "à tolérance de panne". Une certification particulièrement indiquée pour les datacenters puisqu'elle impose que chaque composant et chaque connexion puissent supporter une panne, une erreur ou un événement imprévu sans affecter l'environnement critique ou les processus informatiques. Et s'il fait autant parler de lui, c'est parce qu'il sera également le premier datacenter à intégrer, dès sa conception des solutions innovantes permettant à la fois de réduire son empreinte environnementale mais aussi de faire baisser sa facture énergétique, et par ricochet, celle de ses clients. Le PUE, indicateur d'efficacité énergétique, sera inférieur à 1.2, soit l'une des toutes meilleures performances environnementales en France.



Le nom de Thésée fait référence au héros qui aidé par le fil d'Ariane sut se défaire de l'épreuve du labyrinthe et tua le minotaure. Le mythe du taureau de Minos est une mise en garde : certaines opportunités sont trop généreuses pour ne pas impliquer de contrepartie. Dédale, l'architecte du labyrinthe, incarne l'avancée technologique, mais une avancée sans éthique, sans anticipation des risques. L'ensemble du mythe crétois peut être vu comme un rappel de la fragilité des systèmes d'information à l'heure du Cloud Computing. La puissance des géants du Web américains ou chinois concurrence aujourd'hui celui des Etats et affecte la liberté d'autodétermination des individus. Parallèlement la capacité de recueil et d'accumulation de données fait exploser le poids écologique et énergétique du secteur numérique. L'ambition de Thésée DataCenter est de contribuer à la souveraineté numérique et de minimiser l'impact environnemental du secteur numérique. Et effectivement, la crise sanitaire a indéniablement mis le sujet de la souveraineté au premier rang.

Le campus d'Aubergenville sera composé à terme de 6 bâtiments de 2.300 m^2 chacun sur 3 hectares de terrain. Chaque bâtiment offre deux salles de 534 m2, la surface totale d'hébergement atteindra ainsi 6.400 m2 pour une puissance IT de 18 MW. Le datacenter peut accueillir tout type d'informatique et d'équipements de calcul, qu'il s'agisse d'Intelligence Artificielle, de Deep Analysis, de Deep Learning, de simulation, de rendering. Le site TDC02 est un datacenter "enterré", disposant d'un niveau de sécurité

BIO

Eric Arbaretaz et l'un des deux fondateurs de la société Thésée Datacenter et il en assure la direction technique. Après 10 ans passés au sein d'IBM, il a fondé en 2007 le bureau d'études Apis Engineering spécialisé dans la Maîtrise d'Œuvre pour la construction de centres informatiques. Au cours de cette période, APIS a participé à plus de 150 projets de Datacenters en France et Afrique : Orange, France Télévision, Céleste, Banque de France, Télécity, BNP, Française des Jeux, différents conseils généraux et hôpitaux. Entreprise très innovante, Apis Engineering a introduit en France de nombreux nouveaux concepts et technologies permettant de diminuer l'empreinte environnementale des datacenters : récupération chaleur fatale, Free-cooling direct et indirect, Tri-génération, etc.

BIO

Delphine Chevallier a une expérience de plus de quinze ans dans le développement et l'animation de programme de (trans)formations dans les grands groupes internationaux, notamment de conseil. S'appuyant sur son expérience en matière de pédagogie et d'édition, elle a fondé Thalia NeoMédia, pour accélérer le développement des talents en mettant à leur disposition des outils d'apprentissage favorisant le partage d'expérience et l'engagement, plus particulièrement dans le domaine de la cybersécurité. Elle est lauréate Femmes en Vue du concours Vox Femina 2020.

BIO

Okan Turedi est le le directeur général de Nation Data Center, filiale de conception et d'exploitation de datacenter du Groupe Bakjy.

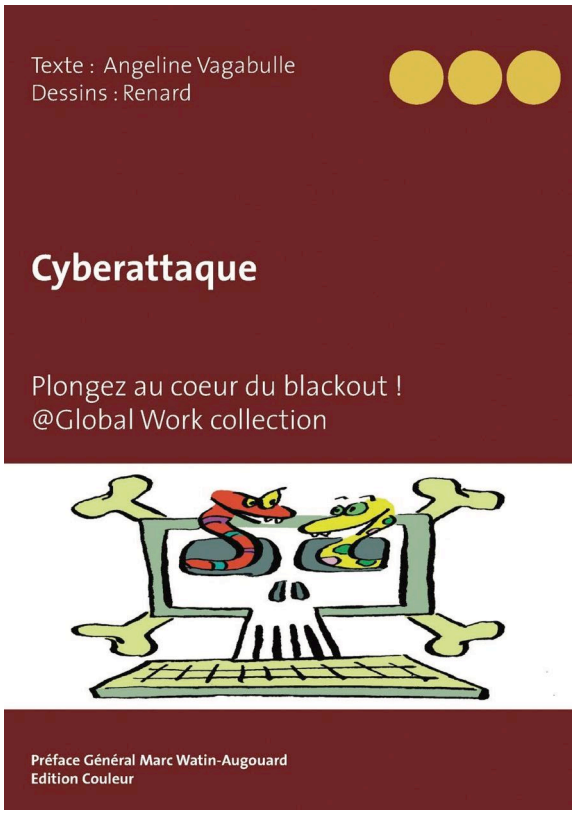


très rare en région parisienne et particulièrement discret, ce qui en fait un site de secours eidéal de notre site principal. Nous hébergeons déjà actuellement une centaine de baies informatiques pour une puissance totale atteignant environ 1 MW reparti entre les deux sites.

Notre participation la semaine dernière au FIC au côté de Thalia NeoMedia renforce notre volonté d'être un acteur de l'écosystème qui se construit en France pour assurer notre souveraineté numérique.

[Delphine Chevallier] : Auchan, NorskHydro, SDIS Dordogne, Bouygues Construction, CHU de Rouen, Eurofins, Altran, TV5 Monde, Lise Charmel, Ville de Sarrebourg, Picanol, Ville d'Huez, Marriott, Saint Gobain, Asco….

Que peuvent bien avoir en commun toutes ces organisations ? Des secteurs très différents, des tailles très variées, public ou privé….. Et bien elles ont toutes été touchées par une grave cyber attaque qui a mis à mal leurs activités pendant de longues semaines. Et dans la liste j'aurai pu rajouter Clermont Pièces : cependant, elle, elle n'existe plus. Elle a fait faillite. 60% des PME touchées par une cyber attaque font faillite dans les 6 mois qui suivent.



J'ai moi-même travaillé dans une organisation qui a été victime d'une attaque cyber, une histoire dont j'ai tiré un livre[1] et qui raconte comment j'ai traversé cette douloureuse expérience avec les équipes. Cette expérience m'a fait toucher du doigt : bien sûr notre hyper dépendance aux outils numériques, mais aussi notre vulnérabilité et l'immensité de notre ignorance du monde cyber. Finalement, c'est un peu comme d'être passé du statut de simple passager dans un avion à celui de co pilote : nous nous retrouvons tous dans le cockpit, avec de faibles connaissances en matière de pilotage aérien voire aucune, mais avec une part de responsabilité pour mener l'appareil à bon port et en plus avec la possibilité de mettre en danger la sécurité même du vol par une mauvaise manipulation, pas forcément malveillante, des outils de navigation.

Les managers et les dirigeants ne sont pas suffisamment outillés pour faire naviguer sereinement leur organisation dans le cyber espace. Forte de mon expérience de plus de 20 ans en tant que DRH opérationnelle et en charge de grands programmes de transformations dans les organisations, j'ai fondé Thalia NeoMedia, qui met en oeuvre une offre de conseil et de formation, de sensibilisation, d'engagement des managers pour acquérir les nouveaux comportements de travail et les compétences indispensables pour développer la cyber immunité de leur organisation.

La rencontre avec Thésée Datacenter nous permet de créer un fil de réflexion et de navigation pour nos participants entre le monde tangible des infrastructures et le monde virtuel des opérations de leur organisation dans le cyberespace.

[Okan Turedi] : Notre vocation est de créer un réseau de datacenters de proximité souverain, local et écoresponsable. Notre offre se concentre à fournir un service de colocation neutre en telecoms et services IT. Nous nous appuyons sur notre expertise immobilière acquise au sein du groupe Unibail Rodamco Westfield afin de permettre le déploiement d'infrastructures numériques de qualité sur le territoire français en nouant des partenariats avec des « champions locaux » issus du tissu économique local dans le but d'assurer la meilleure harmonie avec les besoins de chaque territoire. C'est ainsi que notre chemin s'est croisé avec Thésée DataCenter, notre représentant pour la zone Paris – île de France.



[Eric Arbaretaz] : La stratégie d'accès marché de Thésée DataCenter consiste à cibler en particulier les sociétés de services informatiques qui doivent externaliser leur hébergement afin de mieux protéger leurs serveurs des risques physiques et cybers et assurer la continuité de leur activité. Thésée DataCenter souhaite être un des acteurs majeurs de cette transformation. La crise sanitaire a été un accélérateur de la

transformation. J'espère que des exemples concrets démontreront que la prise de conscience se transforme en plan d'actions déterminé de la part des décideurs des entreprises publiques et de nos grandes entreprises. Les solutions européennes doivent être privilégiées car il s'agit d'un sujet d'intérêt public et la crise actuelle permet un sursaut pour ne pas sombrer définitivement dans une dépendance économique et sociétale.

Depuis la crise sanitaire, la souveraineté des données devient l'une des préoccupations majeures des entreprises françaises et de l'administration française. Depuis les années 2000, le pouvoir des GAFAM, NATU (Netflix, Airbnb, Tesla, Uber) et BATX chinois concurrence celui des États et affecte la liberté d'autodétermination des individus, faisant émerger la notion de souveraineté numérique.



En 2014, à la suite de l'affaire Snowden, les premières Assises de la souveraineté numérique accompagnent la création d'un Institut de la souveraineté numérique, association chargée de sensibiliser le public et les élus aux enjeux, notamment par la publication des Cahiers de la souveraineté numérique. L'article 29 de la loi du 7 octobre 2016 «pour une République numérique» consacre ensuite la notion en proposant de créer un Commissariat à la souveraineté numérique (finalement abandonné), chargé de concourir «à l'exercice, dans le cyberespace, de la souveraineté nationale et des droits et libertés individuels et collectifs que la République protège». La réflexion se poursuit depuis, au Parlement, notamment au Sénat, avec la production de nombreux rapports d'information et d'enquête.



Aux capacités de recueil et d'accumulation de données désormais sans précédent correspond ainsi le développement de nouvelles technologies de traitement par les grands acteurs du numérique : agrégation à très grande échelle et traitements massifs (big data), algorithmes comprenant des mécanismes d'apprentissage automatique (machine learning), recours à l'intelligence artificielle... Or l'exploitation massive de données est permise par la diminution du coût de traitement déjà décrite dans le rapport de la mission commune d'information sur l'Europe au secours de l'Internet. Les modèles économiques des grands acteurs dominants (gratuité d'accès, collecte massive, utilisation et valorisation des données personnelles, vente de publicités ciblées) passent aujourd'hui par la mise en œuvre de stratégies d'évitement leur permettant d'échapper aux contraintes traditionnelles de notre ordre juridique. Certains acteurs du numérique sont même susceptibles d'être en France les vecteurs - consentant ou non - d'ordres juridiques étrangers : les géants américains sont tenus à l'application des régimes de sanctions extraterritoriales ou des règles d'accès aux preuves électroniques (comme le Cloud Act) et de grands acteurs industriels du numérique chinois restent marqués par une certaine porosité avec les intérêts militaires de leur pays.



Le PATRIOT Act de 2001 autorisait déjà les agences gouvernementales américaines à accéder aux données hébergées par des compagnies américaines dans le cadre de la lutte antiterroriste, mais c'est avec les révélations d'Edward Snowden en 2013 sur les systèmes de surveillance à grande échelle déployés par les États-Unis, collectant massivement, avec l'aide des grandes entreprises du numérique, des données provenant de l'étranger et bien au-delà du périmètre prescrit par le PATRIOT Act, que le projet de cloud souverain en France a vu son importance stratégique considérablement amplifiée (Bômont & Cattaruzza, 2020). Le risque de voir des informations critiques, au niveau de l'État ou d'entreprises françaises, être collectées dans le cadre de mesures de surveillance (ou d'opérations d'intelligence économique) a été renforcé par la signature du Clarifying Lawful Overseas Use of Data Act, en Mars 2018. Le CLOUD Act réaffirme la capacité du droit américain à s'appliquer, en matière numérique, peu importe le territoire. Il permet, en particulier à la justice américaine, munie d'un simple mandat, d'exiger auprès des entreprises technologiques établies aux États-Unis la transmission des données de communications d'un utilisateur stockées sur des serveurs appartenant ou étant opérés par l'entreprise, où qu'ils se trouvent, sans en informer l'individu en question.

D'ici 2022, à l'échelle mondiale, 72 % des grandes entreprises pourraient transférer l'intégralité de leurs données sur un cloud les rendant particulièrement à

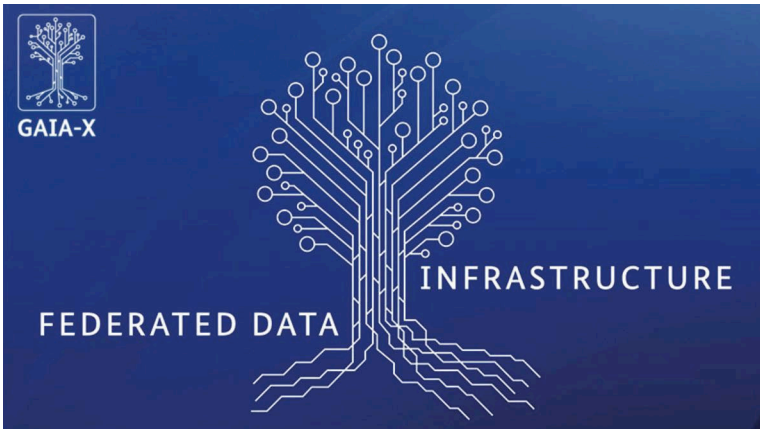


risque vis-à-vis des intérêts non européens. Pour les entreprises comme pour les États, il apparaît en effet essentiel d'assurer la protection des données qu'ils y stockent. Aujourd'hui, les GAFAM (Google, Apple, Facebook, Amazon, Microsoft) dominent largement le marché. Cette situation monopolistique suscite plusieurs interrogations en matière de vie privée, de maintien du secret des affaires et de sécurité nationale. Autre source d'inquiétude : ces dernières années, les entreprises américaines, mettant à profit la dépendance des entreprises européennes à leur services numériques, conduisent des stratégies d'augmentation des prix de ces services, obligeant leurs clients à s'y adapter, au risque de voir leurs activités reposant sur l'usage de ces outils numériques interrompues. D'autre part, elles utilisent les règles et les lois de leur propre pays concernant l'accès et l'usage des données des utilisateurs. Ces exceptions réglementaires extraterritoriales atteignent la souveraineté des entreprises européennes.

Le 4 juin 2020, les ministres de l'économie français et allemand ont détaillé, lors d'une conférence de presse conjointe, Gaia-X, leur nouveau projet d'infrastructure européenne de services cloud. Alors que le confinement d'une large partie de la population européenne et le recours au télétravail ont mis en lumière le manque d'alternatives aux solutions américaines, cette présentation de Gaia-X ramène les ambitions françaises de création d'un "cloud souverain" sur le devant de l'actualité. A l'échelle européenne, ce projet s'inscrit dans la continuité de la politique de Digital Single Market, en 2015, du Règlement Général sur la Protection des Données, adopté en avril 2016, et de la « European Strategy for Data », présentée par la Commission européenne, qui évoquait déjà, en février 2020, au travers de sa vision "d'espace européen de la donnée", le projet de "super cloud » européen. Pour permettre le développement et la compétitivité des entreprises européennes, Gaia-X doit désormais assurer la coordination entre des acteurs économiques, et indirectement entre des États, d'ordinaire en situation de concurrence, pour standardiser leurs offres et maximiser l'acquisition des clients européens.

Promouvoir, voire dans certains cas imposer, une obligation de localisation des données sur un territoire précis (en France ou en Europe) permet de protéger certaines données particulièrement sensibles (traitements publics souverains, données privées financières ou commerciales stratégiques). De telles solutions pourraient ainsi être imposées dans le cadre plus général des régimes des opérateurs d'importance vitale (OIV) ou des opérateurs de services essentiels (OSE). C'est également garantir une accessibilité renforcée, soit du point de vue des entreprises dans une logique de gestion des risques (lorsque les données ne sont plus localisées en France ou en Europe, il est plus difficile en pratique de les contrôler et d'avoir une assurance de l'usage qui a été fait par des prestataires ou des partenaires localisés à l'étranger), soit du point de vue de la puissance publique. Cependant, et en tout état de cause, les clauses de localisation des données n'offrent pas de garanties face aux nouvelles législations ou pratiques étrangères à portée extraterritoriale (sanctions internationales, « Cloud Act » adopté aux Etats-Unis en mars 2018, etc.) ni contre la porosité entre certains acteurs industriels et leur Gouvernement (certains équipementiers chinois, par exemple). Ainsi, quand bien même des données seraient physiquement localisées sur le territoire français ou européen, les entités qui contrôlent les datacenters continueront, en raison de leur nationalité, à être également soumises à des régimes juridiques les obligeant à coopérer avec des puissances étrangères.









C'est pourquoi, la priorité pour développer une réelle souveraineté nationale et européenne est de faire émerger des solutions pour l'hébergement et le stockage des données sensibles de ces entreprises, autour de prestataires français et européens non soumis aux législations étrangères à portée extraterritoriale. Du fait d'être une société de droit français à capitaux 100% français, TDC est régie par les seules lois française et européenne et échappe donc à des règles de type "Cloud Act". Pour les clients cela veut donc dire que l'intégralité de leurs données informatiques sont sécurisées et ne seront jamais transmises à des tiers sans leur accord. Thésée DataCenter applique l'ensemble des règles et recommandations de l'ANSSI, qui est l'autorité nationale en matière de sécurité et de défense des systèmes d'information, et Thésée DataCenter sera donc parfaitement aligné avec les futures obligations de souveraineté nationale.

[Delphine Chevallier] : Affronter une crise cyber présente de multiples enjeux pour une organisation. Elle peut provoquer un traumatisme très profond pour les équipes comme pour les activités. Comme je le mentionnais plus haut, certaines organisations ne s'en remettent pas. Les défis sont multiples : affronter un ennemi invisible, faire face à l'inconnu et au stress de la menace et la pression, trouver le bon rythme de décision (ne pas sur réagir mais aussi savoir décider même quand on est 'dans le noir'), assurer la continuité de ses activités, 'tenir' ses équipes, communiquer à bon escient en interne comme en externe, appréhender l'abysse de ses pertes financières à chaque minute d'arrêt de production qui s'écoule, réaliser de façon brutale que lorsque la technologie est à l'arrêt, on ne peut plus faire grand-chose voire plus rien du tout, que l'on est impuissant. Et pourtant, des solutions existent. La première et la plus efficace consiste à s'entrainer, à se préparer. A vivre de l'intérieur ce que cela pourrait dire d'être mis à l'arrêt par un acte grave de cyber malveillance, simuler tous les scénarii possibles pour 'stress tester' la résilience de son organisation et de ses équipes. Comme tout (co) pilote d'avion qui se teste, s'entraine encore et encore en simulateur à toutes les situations extrêmes qu'il pourrait avoir à affronter.

C'est tout l'objet de #crisis 42, notre salle de simulation de crise cyber pour les dirigeants, leur manager et toutes leurs équipes opérationnelles. Cet espace nous permet de créer tous les scénarii possibles pour une organisation qui souhaite se préparer. Grâce à cette expérience, les équipes identifient les points d'amélioration organisationnels (quels sont nos back-ups ? savons-nous les activer ?) et humains (que devons-nous travailler pour résister au stress et être capable de prendre les bonnes décisions, même sous pression ? quelle culture d'engagement devons nous mettre en place pour assurer la solidarité de tous pour faire face à l'adversité ?) ainsi que les actions à mettre en place (que faire pour assurer la continuité de tel ou tel processus critique de nos activités de production par exemple ?).

Cet espace permet de développer une culture d'humilité : en venant se challenger régulièrement, les équipes se mettent à jour sur les techniques utilisées par les cybercriminels, celles-ci évoluant très rapidement.

[Eric Arbaretaz] : Comme la majorité des Data Centers français, Thésée DataCenter a ses deux sites en région parisienne. Cependant, Thésée DataCenter fait partie de l'alliance Nation Datacenter dont la stratégie est de s'implanter sur l'ensemble du territoire et très rapidement dans toutes les grandes métropoles.

[Okan Turedi] : Dans le cadre de notre stratégie d'expansion nationale, le prochain projet porté par Nation DataCenter, est baptisé Roahdata et sera basé aux environs de Rennes afin d'être le premier DataCenter Rennais en colocation neutre. Cette nouvelle localisation ne doit rien au hasard et a fait l'objet de nombreuses rencontres avec les futurs utilisateurs. En effet, Rennes constitue aujourd'hui le premier pôle de recherche numérique en France après Paris et peut compter sur la présence de très nombreuses startups en cyber sécurité extrêmement talentueuses et pleines d'ambitions ! Nous souhaitons être leur partenaire pour réaliser leurs objectifs.

[Delphine Chevalier] : Les besoins de sécurité pour la résilience des datacenters face aux menaces sont grandissants. De nombreux datacenters sont aujourd'hui considérés comme des Organismes d'Intérêt Vitaux en fonction des clients qui y sont hébergés. Par exemple, les deux malwares, Wannacry et NotPetya, apparus en 2017 ont montré une rupture dans les cyberattaques puisqu'ils comportaient un chiffrement de bas niveau, permettant par exemple l'amorçage d'un disque. Face aux augmentations de cyberattaques de ces dernières années (Equinix en septembre 2020, data centers privés

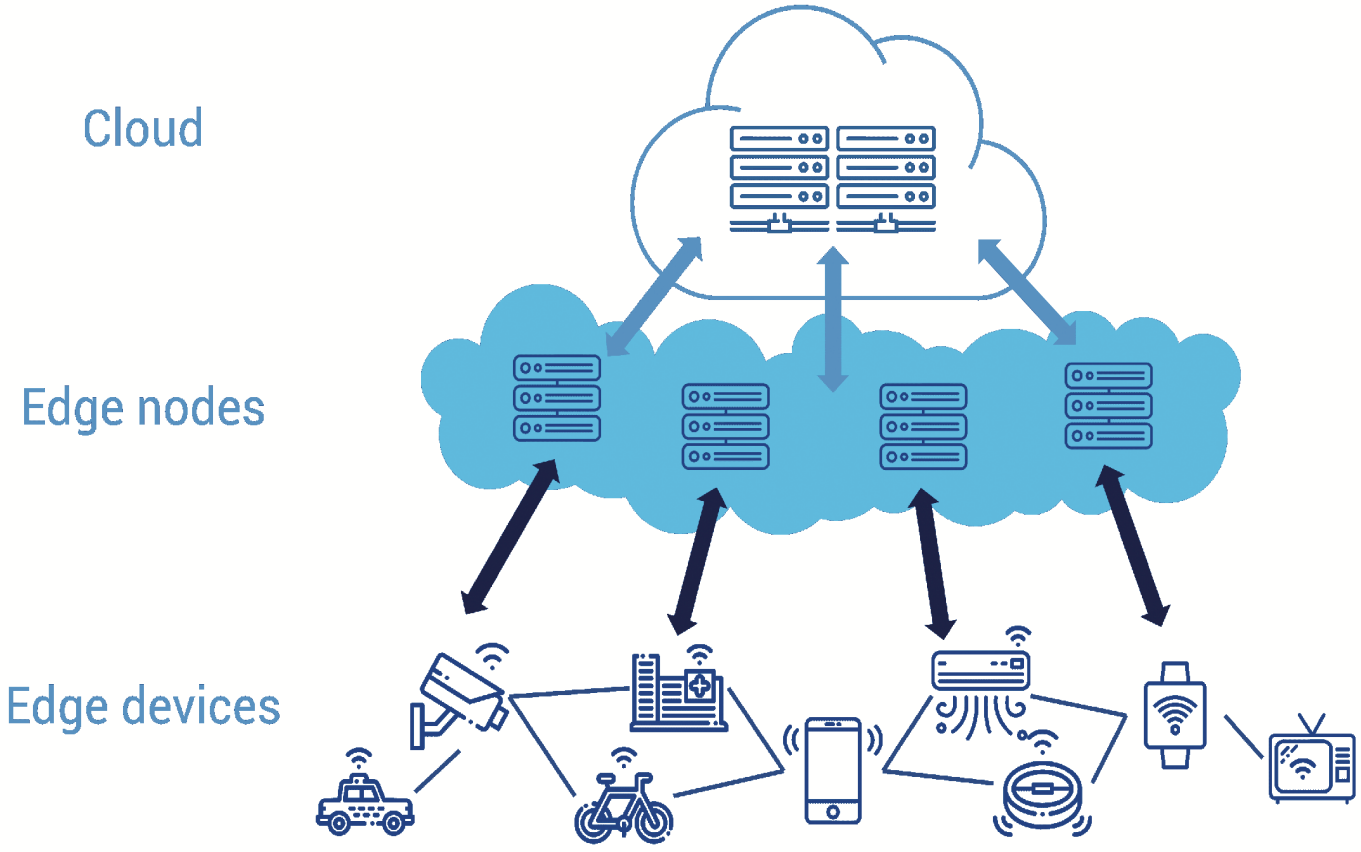
d'Orange, Garmin Spie…), les entreprises sont soumises à une augmentation de contraintes règlementaires pour la protection de leurs données et des données de leurs usagers pour assurer une continuité d'activité (audits internes, audits par commissaires aux comptes, directive Solvency II, directive Bâle 2, …). Il existe aussi d'autres risques : grève, blocage volontaire d'un site comme ça l'a été lors de la crise des gilets jaunes, ainsi que des risques plus graves comme nuisances volontaires à l'intérieur du site, attaque béliers, attaques terroristes, et évènements climatiques majeurs qui compte-tenu de l'aspect critique des données pour plusieurs secteurs (e-commerce, finances, activités militaires ou administratives…), peuvent avoir un impact majeur et représente de ce fait des risques importants. En conséquence un client va vouloir limiter ces risques en disposant d'un second site pour héberger des infrastructures IT de secours ou redondée. Le récent incendie du Data Center d'OVH à Strasbourg ne fera qu'amplifier ce mouvement : il n'est plus possible d'héberger ses installations et données critiques dans le même Data Center, au risque de voir disparaitre les sauvegardes principales ET leur back-up. De ce fait, les entreprises et services publics modifient et augmentent leurs demandes de résilience et de service de sécurité, tout en demandant une capacité de s'adapter à leurs besoins évolutifs.



Les Plans de Reprise d'Activité (PRA) et Plans de Continuité d'Activité (PCA) qui résultent de ces contraintes de résilience , ne supportant de plus en plus aucune durée d'interruption de services, nécessitent de disposer au minimum de deux datacenters redondants se situant à distance suffisante pour éviter que les deux sites soient touchés par la même catastrophe (plus de 10 km) mais suffisamment proches pour que les deux sites soient directement reliés par une fibre optique permettant de synchroniser les systèmes d'informations (moins de 50 km). Cette architecture composant un Dual Site a longtemps composé la stratégie de résilience de la production informatique mais semblait devenir obsolète avec le Cloud Computing.

[Eric Arbaretaz] : Les plans de continuité d'activité qui résultent des contraintes de résilience de l'informatique Edge nécessitent de disposer de datacenters de proximité de plus en plus nombreux. Le principe de l'Edge Computing en est la référence pour le numérique.

L'apparition de ces nouveaux data centers régionaux qui collecteront, stockeront et traiteront un très grand nombre de données créées par les





villes de demain, est inéluctable. Il est essentiel que la conception et la réalisation de ces datacenters supportant l'Edge Computing suivent une approche nouvelle, différente de ceux des Data Center de très grandes tailles. Les Data Center de ces géants américains assurent une fonction numérique très centralisée et très consommatrice d'énergie.



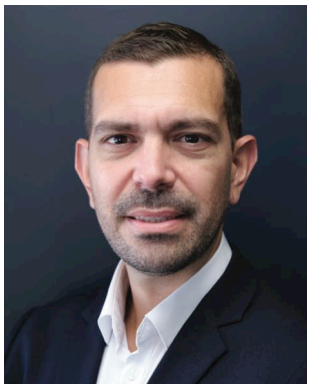
Le poids écologiques de ces géants posent d'ailleurs question dans le cadre de la transition énergétique. Ils sont coûteux en capitaux et en empreinte carbone car ils sont technologiquement conçus uniquement pour leurs seuls besoins. Ils ne permettent aucun partage des investissements avec d'autres services et en particuliers ceux liés aux différentes formes d'énergie. Il est nécessaire d'inventer des concepts où le numérique et les énergies sont un ensemble de services qui se valorisent entre eux. Ils apporteront ainsi une réponse aux besoins nouveaux des énergies renouvelables devant être mises à disposition de la collectivité et des entreprises. Sur le plan sécuritaire (physique et cyber), je pense que le modèle des datacenters géants et hyper concentrés est obsolète, atteint ce que j'appellerai du syndrome de Pearl Harbour. A votre avis, en cas de conflit majeur pour lequel nous savons que le cyberespace serait un des premiers terrains de combat, qui seraient prioritairement ciblés ?

[Eric Arbaretaz] : Nous arrivons à la fin de notre entretien, quelle serait notre conclusion ?

[Delphine Chevalier] : Les organisations doivent monter en exigence en termes de capacité à bien protéger leurs actifs et leurs opérations dans l'univers numérique. Elles doivent également reprendre le contrôle pour s'assurer de bénéficier de solutions véritablement souveraines mais également eco-responsables et de proximité. C'est ce que la complémentarité de nos expertises et solutions offre au travers de notre partenariat. ■

1 Ecrit sous le nom de plume d'Angeline Vagabulle, 'Cyberattaque – Plongez au cœur du blackout !' est illustré par Renard er préfacé par le Général Marc Watin-Augouard, foncateur du FIC.

Risques, Cybersécurité et Conformité.



Auteur : Benoit LACOUR



Face à de nouveaux écosystèmes de menaces où les acteurs changent d'échelle, la cybersécurité organise de nouveaux collectifs de défense. Ces nouveaux écosystèmes réalisent leurs opérations via des plateformes innovantes, technologiques ou humaines.

La cybersécurité à l'ère des écosystèmes

La disruption engendrée par la digitalisation de l'économie accélère l'émergence de risques stratégiques. Les nouvelles technologies et usages exposent les entreprises et les Etats à un nouveau monde de menaces, plus complexes et nombreuses.

La cybersécurité, un risque stratégique majeur

Le risque cyber est considéré comme le deuxième risque le plus important pour les entreprises et les Etats, devant le risque lié aux catastrophes naturelles. Dans le monde de la finance, par exemple, le risque de cybersécurité est devenu plus important que les risques liés à la non-conformité réglementaire ou aux fluctuations des marchés.

Ces risques accrus mettent en péril les actifs stratégiques des organisations, à savoir ses produits, ses services, ses données, son image auprès des clients, des fournisseurs, des partenaires et du grand public. C'est la confiance des employés, des clients et du grand public envers l'entreprise et les Etats qui est aujourd'hui menacée.

La cybersécurité est devenue un risque stratégique majeur.

Les acteurs et les risques changent d'échelle

A l'heure de la pénurie mondiale d'expertises en cybersécurité, les ensembles d'acteurs malveillants qui menacent la sécurité des biens et services changent d'échelle. Des hackers agissent en réseaux, en ensembles auto-organisés, transfrontaliers, opaques. Ensemble, ils déploient une capacité d'exploration, d'analyse et d'intrusion démultipliée, liée au

BIO

Benoit Lacour est un expert en cybersécurité et réglementation pour la protection des données personnelles au sein de la société onepoint.
Spécialisé en sécurisation des systèmes d'informations et protection de la donnée personnelle, il intervient dans de nombreux domaines comme les analyses de risques, les audits techniques et organisationnels.
Fort d'une expérience de 17 ans acquise au sein du ministère des Armées, il a occupé plusieurs fonctions à responsabilité dans les domaines stratégiques et techniques.
Il intervient dans de nombreux groupes d'expertises au sein du Club EBIOS, de la Fédération Française de la Cybersécurité et au CLUSIR Aquitaine



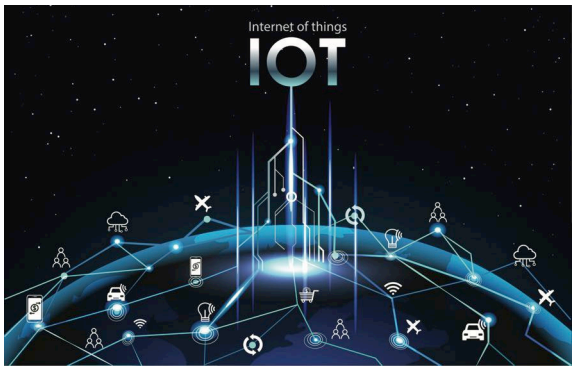
grand nombre d'acteurs interagissant. Ces forces prosélytes recrutent des armées de volontaires qui, par contrat ou par défi, adoptent chaque nouvelle technologie à un rythme toujours plus rapide, exploitent chaque nouvelle faille presque immédiatement. Ces organisations collaboratives, augmentées par l'effet des interactions et du nombre, réparties en équipes distribuées, représentent une nouvelle nature de menace. Elles sont en avance.

De manière symétrique, les risques changent d'échelle. De nouvelles technologies créent des risques systémiques pour la bonne organisation de nos sociétés : l'Internet des objets, les Smart Buildings et Smart Cities, la digitalisation des centres financiers, de transports ou de soins digitalisés sont autant de surfaces d'attaque paralysantes pour tout collectif de vie. Les réseaux sociaux publics et les réseaux privés distribuent de manière incontrôlée des informations qui font courir des risques d'image et de confidentialité à grande échelle.

Mobiliser les nouveaux collectifs de défense : la sécurité à l'ère des écosystèmes et des plateformes

Face à ces risques globaux où les acteurs changent d'échelle, face à des écosystèmes de menaces qui fonctionnent en allocation de ressources distribuées par effet de réseau, le temps est venu de changer de paradigme et de structurer la sécurité à l'ère des écosystèmes.

La sécurité à l'ère des écosystèmes nécessite la formation de nouveaux collectifs de défense, profitant à leur tour de la démultiplication liée à l'effet



du grand nombre et de l'organisation en réseau. Ces collectifs, des écosystèmes, opèrent via des plateformes technologiques ou humaines, forgées pour décupler des capacités de défense et opposer une même nature de défense à ces nouveaux risques globaux.

A l'ère des écosystèmes, trois plateformes de défense émergent.

1. Les plateformes technologiques

Face à l'inflation démesurée du nombre d'attaques, de nouvelles plateformes technologiques voient le jour. Des nouvelles générations de plateformes de sécurité orientées métier se créent. Elles permettent d'automatiser

en temps réel toute la chaîne de valeur de la gestion du risque. Ces plateformes technologiques, conçues pour des cas d'usages métiers focalisés, automatisent depuis la capture de connaissance en amont (Cyber Threat Intel), l'identification des vulnérabilités, jusqu'à la détection et alerte (SOC), ainsi que la réponse et remédiation des incidents (CERT, CSIRT), portés par des algorithmes d'intelligence artificielle de type Machine Learning, ou encore exploitant des mécanismes de type Distributed Ledgers (blockchains).

Déployées en mode SaaS, ces plateformes sont dotées de capacités d'analyse (Advanced Analytics) et de visualisation graphiques (DataViz) pour fournir aux métiers des outils de suivis en temps réel. Dans ce cas, la force démultiplicatrice du nombre est portée par la scalabilité d'une plateforme exploitant les larges volumes de données (Big Data) et les nouvelles puissances de calcul.



2. Les plateformes d'intelligence collective pour une organisation résiliente

La cybersécurité est désormais la responsabilité de tous et doit être portée personnellement par les dirigeants des entreprises et des Etats, ainsi que par l'ensemble des salariés et citoyens. Depuis des années, la grande majorité des cyberattaques provient de ce qui est appelé le "facteur humain" : les comportements à risque quotidiens du grand nombre des salariés ou citoyens, qui sans le savoir, ignorent les bonnes pratiques et mettent en péril leur environnement (clients, fournisseurs et partenaires).

Elargissant les actions traditionnelles de sensibilisation, de nouvelles plateformes d'intelligence collectives émergent, constituées d'un collectif formé et spécialisé et de méthodes ayant comme objectif la cyber-résilience de l'organisation. Ce collectif anime l'ensemble de l'écosystème de partenaires, de prestataires, de clients et de prospects selon une nouvelle approche de gestion. Celle-ci permet à l'organisation, en cas de crise, de ne pas interrompre son fonctionnement et de réduire l'impact de l'incident.

Cette approche de la résilience par l'intelligence collective tire profit de l'apport des nouvelles méthodes de type Serious Gaming, Secure Design Thinking, démarche innovante agile itérative de type "Secured



Product Management", focalisation sur la valeur métier avec les "Epics", les "User Stories" et "abuser Stories" métier, les démarches formelles d'homologation interne qui engagent et acculturent des employés et partenaires responsabilisés.

Cette plateforme d'intelligence collective se développe à tous les niveaux autour de l'organisation et augmente le degré de résilience de l'ensemble de l'écosystème.

3. Les plateformes de savoirs

Dans le monde des risques et de la sécurité, une économie spécifique se développe autour des informations relatives aux nouvelles vulnérabilités. La vitesse d'accès à ces informations, le partage des informations stratégiques comme opérationnelles, les protocoles de réponse, de remédiation, de contournement, la mise en commun des retours d'expérience suite aux attaques, virus ou incidents identifiés, représentent un enjeu vital. Dans ce contexte, la coopération et la mise en partage des référentiels d'expérience revêt une importance stratégique pour de nouvelles fédérations de collectifs au sein de l'écosystème de défense : des clubs de dirigeants, de RSSI, des associations d'utilisateurs, des éditeurs et fournisseurs spécialistes, des experts indépendants ou des chercheurs qui se regroupent au sein de ces futures nouvelles "plateformes de savoirs".



Dans les années qui viennent, les apports de ces trois plateformes de services, piliers de la cybersécurité, vont développer de nouveaux écosystèmes de défense. L'innovation technologique, les transformations de modèles opérationnels favorisant l'intelligence collective au service de la résilience et le renforcement de l'économie des savoirs, seront des réponses nouvelles, à l'échelle de ces nouveaux risques globaux. ■

Cybersécurité et ISO 27001 : à chacun son parcours.



Auteur : Brice GILBERT

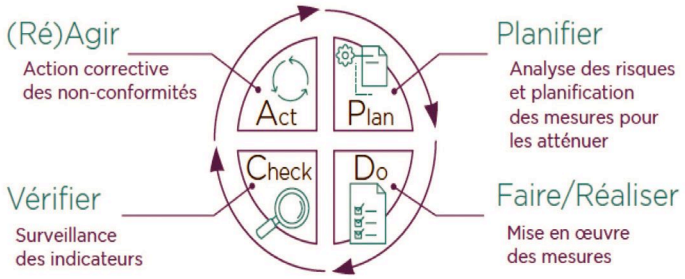
Qu'est-ce que l'ISO 27001 ?

La norme internationale ISO/IEC 27001 définit les exigences relatives aux systèmes de management de la sécurité de l'information (SMSI). Elle définit comment les organismes privés et publics doivent s'organiser et les moyens qu'ils doivent mettre en œuvre pour assurer la sécurité des informations numériques et non-numériques. Elle est actuellement la référence internationale en terme d'organisation liée à la cybersécurité. L'ISO Survey estimait le nombre de certificats ISO 27001 en 2020 à 44499 dans le monde dont 392 en France.

BIO

Responsable de Projets Confiance Numérique chez AFNOR Certification, Brice a en charge la gestion des certifications et labellisations en lien avec la cybersécurité : certification ISO 27001, certification HDS, qualification SecNumCloud, Label ExpertCyber,… Fort de son expertise en méthode d'évaluation, il participe également à la rédaction de textes de référence pour le compte d'acteurs publics ou privés. Partisan des textes normatifs et de leur méthode collective d'élaboration qui assure leur représentativité, il a également à cœur de développer des guides et référentiels adaptés aux PME, TPE et start-up.

Schéma simplifié d'un système de management
Boucle d'amélioration continue



La norme ISO/IEC 27001 compte 114 mesures de sécurité à appliquer par l'organisme afin de traiter les risques qui pèsent sur ses actifs (serveurs, logiciels, brevets, informations sensibles,…). Elles constituent généralement un socle minimal de mesures à appliquer qui peut être enrichi si l'organisme le juge nécessaire. L'organisme doit justifier l'application ou la non-application de ces mesures au regard de son activité et de ses risques.

Les 114 mesures de sécurité impliquent les processus métiers et supports de l'organisme. Elles sont classées en 18 thématiques, parmi lesquelles :

- Les ressources humaines : sensibilisation des salariés à la sécurité de l'information,…
- La sécurité physique : sécurisation des bureaux, contrôle des accès physiques,…
- Les accès numériques : gestion des droits d'accès, gestion des mots de passe,…
- L'exploitation : journaux d'évènement enregistrant les activités des utilisateurs, sauvegarde des données,…
- La maitrise de la sous-traitance : audits des fournisseurs ayant un impact sur la sécurité de l'information,…
- La gestion des incidents de sécurité : détection et réponse aux incidents de sécurité,…
- La continuité d'activité : plan de continuité d'activité, redondances,…

Pourquoi passer par une démarche progressive de montée en maturité ?

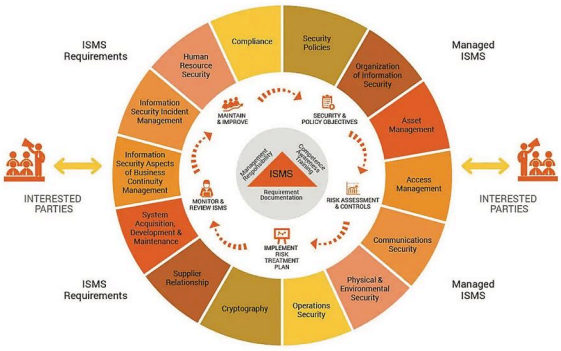
La mise en œuvre d'un système de management tel que décrit dans la norme ISO/IEC 27001 avec les 114 mesures de sécurité associées nécessite des moyens humains et financiers conséquents qui ne sont pas à la portée



de tous les organismes et qui peuvent décourager les moins matures d'entre eux.

Pourtant, le numérique démontre jour après jour la nécessité de s'emparer pleinement des enjeux de cybersécurité et de protection des données afin notamment de tisser un lien de confiance avec ses clients et partenaires. Déployer des mesures adaptées à son contexte et ses enjeux est indispensable. Dans cette perspective, l'adoption d'une démarche progressive facilite cette mise en œuvre.

L'appréciation des risques, la connaissance de ses vulnérabilités, la détection et la gestion des incidents sont des processus qui nécessitent des boucles d'amélioration continue pour arriver à maturité. Ils peuvent également être mis en œuvre par augmentation progressive du niveau de sécurité.



Les parcours de montée en maturité : une démarche dans l'ère du temps

Une prise de conscience générale des enjeux liés à la cybersécurité est en cours dans nos sociétés. La montée en maturité des organismes est déjà bien engagée dans certains secteurs, en particulier les secteurs sensibles, et peut être impulsée par les attentes du Marché ou par les politiques publiques, notamment au travers des lois et réglementations.

Les lois et réglementations suivantes ont obligé les organismes concernés à monter en maturité :

- Les Organismes d'Importance Vitale en application de la Loi de Programmation Militaire.
- Les hébergeurs de données de santé à caractère personnel qui doivent mettre en œuvre la norme ISO/IEC 27001 et être certifiés en application du décret HDS du 26 février 2018.
- Les organismes qui traitent des données personnelles qui doivent mettre en place des mesures de sécurité en application du RGPD.
- Les constructeurs automobiles qui devront mettre en place un système de management de la cybersécurité à partir de juin 2022 en application de la réglementation de l'UNECE WP29.



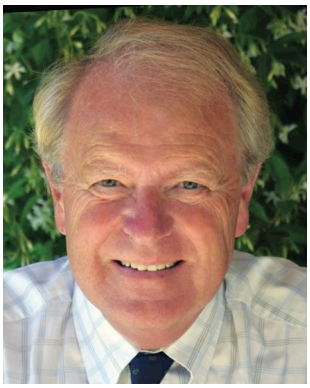
Pour les secteurs moins sensibles où les acteurs sont moins matures, l'Etat peut inciter à mettre en place une démarche progressive. Ainsi, afin d'élever le niveau de cybersécurité de l'Etat, des collectivités territoriales et des organismes au service des citoyens, l'ANSSI a conçu 4 parcours de cybersécurité dans le cadre de France Relance avec des niveaux progressifs (fondation, intermédiaire, avancé, renforcé) afin que chaque organisme concerné ait une réponse adapté à son contexte et ses moyens.

Dans la même perspective, AFNOR Certification encourage les organismes privés et publics de toutes tailles à monter progressivement en maturité sur la norme ISO/IEC 27001 en s'auto-évaluant sur les points clés de la norme. Une plateforme d'auto-évaluation en ligne est d'ailleurs mise à disposition gratuitement pour tous les organismes souhaitant analyser leurs forces et faiblesses en matière de cybersécurité et disposer d'une feuille de route sur les actions prioritaires à mettre en œuvre afin d'entrer dans une démarche vertueuse et progressive de cybersécurité.



https://certification.afnor.org/numerique/focus-cybersecurite ■

Du DSI au CDO : une gestion stratégique des données.



Auteur : Jacques-Louis KESZLER



C'est une banalité de dire que beaucoup d'entreprises sont aujourd'hui plus riches de leurs données que de leurs investissements "Brick and Mortar". Mais en mesure-t-on les conséquences de façon complète ?

La pandémie, en contraignant les entreprises BtoC à distribuer leurs produits en omnicanal a permis d'engranger une quantité très importante et inattendue de renseignements sur les clients finaux. Dans certains groupes multi-enseignes les données collectées permettent de tracer un profil assez précis du client, de son potentiel en termes de chiffre d'affaires, de ses goûts, de la composition de sa famille, de son mode de vie, etc.

D'une connaissance somme toute grossière de la clientèle, à base d'études de marché et de relevés de caisse qui alimentaient le service marketing d'une entreprise, on est passé à une connaissance fine de la clientèle. De campagnes de publicité et de promotions destinées à attirer et convaincre le chaland de l'excellence des propositions de l'entreprise on a la possibilité de passer à une politique commerciale "data-driven" Où l'on propose presqu'à coup sûr ce qui correspond aux besoins exprimés, voire latents du consommateur.

La masse de données collectées induit des problèmes de sécurité, ainsi que de respect des règles RGPD. Mais la question principale sera, est déjà, celle de la capacité et du coût du stockage. Discerner les "bonnes données" à collecter et à traiter dans une optique d'investissement et de long terme demande une vision différente et extensive qui dépasse celles des services d'études marketing et de direction des services informatiques. Ainsi se crée une nouvelle fonction d'État-Major : Celle de DCO.



Que peut-on dire de ce "Digital Chief Officer", en Français de ce Directeur Général en charge des données ?

Responsable d'un actif clef c'est d'abord un stratège, membre du Comité de Direction, (du Directoire) : il a une claire vision des options stratégiques qui s'offrent à son entreprise.

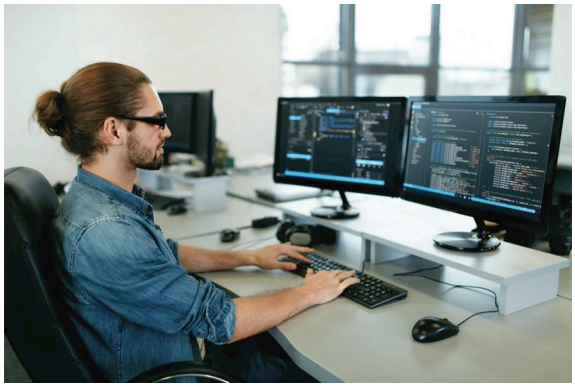
BIO

Jacques-Louis Keszler a commencé sa carrière chez Renault-Marine comme contrôleur de gestion, avant de rejoindre le groupe pharmaceutique Boehringer-Ingelheim France où il a été responsable de la grande exportation. Après avoir dirigé l'EDHEC, puis fondé l'ESC La Rochelle, il est conseil en stratégie, particulièrement en redressement d'entreprise, depuis plus de vingt ans. Il est diplômé de l'ESSEC, d'une maîtrise d'économie, et d'un titre en pharmacie industrielle. Il est également membre associé de l'Institut des Hautes Etudes de Défense Nationale.

Polyvalent au sens qu'il intègre les préoccupations stratégiques, marketing, financières, de supply-chain, de production et de gestion des ressources humaines, il est capable de discerner les nouvelles opportunités de business qu'offrent les données dont dispose l'entreprise.

Réciproquement il a une vision prospective des chiffres et renseignements dont l'entreprise va avoir besoin pour conforter son développement dans le futur. A ce titre, il a notamment en charge les questions d'intelligence économique, et coopère avec les services marketing, de production et d'une façon générale avec l'ensemble de l'entreprise.

C'est un analyste et un créatif qui sait faire parler les chiffres au travers d'outils d'intelligence artificielle, et maximiser ainsi la productivité de l'investissement immatériel dont il a la responsabilité.



C'est un organisateur bien sûr qui doit décider de ce qui reste sur les serveurs de l'entreprise, et de ce qui peut être mis sur le cloud. Ainsi va-t-il déterminer les données critiques de l'entreprise dans deux horizons de temps : l'immédiat opérationnel, et le long terme. Certaines données comme le fichier des clients s'inscrivant dans les deux perspectives.

Aura-t-il aussi la casquette de DSI ? Ce sera question de circonstances comme de taille et de typologie d'entreprise.

Si le DSI est l'homme du quotidien et de la prospective hard et soft, on voit bien que le CDO s'inscrit dans une autre logique qui est celle de l'utilisation des données et de leur valorisation. Il est cependant probable que dans



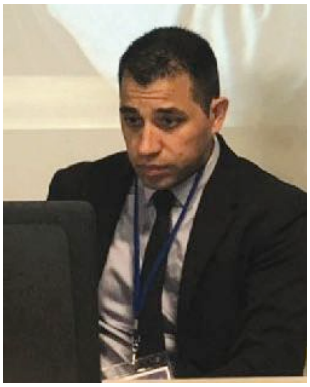
nombre d'entreprises les deux casquettes soient sur la même tête. C'est une évolution normale à la fois pour des raisons de compétences informatiques mais aussi tout simplement de gestion de carrière.

Pour autant la mutation ne sera ni simple ni naturelle. Elle va impliquer, elle implique, une remise en cause personnelle du DSI. Un changement de dimension et de préoccupations : passer de la gestion, de la protection, et du stockage des données à la valorisation des données. C'est une montée en compétences qu'il faut planifier et organiser, par des formations en stratégie d'entreprise, en marketing, et les autres "métiers" majeurs de l'entreprise.

C'est enfin un changement de regard porté sur l'entreprise : de l'opérationnel de haut niveau, au stratège. ■



L'évolution du poste de RSSI, de responsable informatique à directeur de la cybersécurité…



Auteur : Pierre VENOT



Depuis de nombreuses années, les cyber menaces sont de plus en plus prégnantes et omniprésentes, il n'est évidemment pas question d'en débattre, tout le monde en convient aisément. Guillaume POUPARD, le directeur général de l'ANSSI, l'évoquait sans filtre lors de la dernière édition du FIC (Forum International sur la cybersécurité) : "le pire est devant nous".

Cependant, si l'on regarde de plus près la prise en compte de cette problématique par les entreprises, il y a encore malheureusement du travail à accomplir pour garantir une protection efficiente par la plupart des parties prenantes. Au-delà des investissements financiers, parfois lourds, que la mise en place de moyens de protections et de surveillances entraine, un facteur humain reste le dénominateur commun et garant de la bonne harmonisation de ces moyens : le RSSI.

Les débuts du rôle de RSSI

Il y a plus d'une vingtaine d'année, date à laquelle on peut estimer l'apparition de ce titre, le rôle de RSSI était souvent dévolu à des responsables



BIO

DSSI du groupe PICOTY, responsable du Bureau CLUSIR – Nouvelle Aquitaine Est, ancien expert en lutte contre la cybercriminalité au sein de la gendarmerie nationale, il dispose d'une très forte expérience du monde de la cybercriminalité et de son impact au niveau des TPE, PME et du citoyen en général. Le champ infractionnel auquel il a été conforté (ransomware, escroqueries, intrusion frauduleuse dans des serveurs d'entreprises…) lui ont apporté une vision périphérique du panorama de la cybercriminalité et une approche pragmatique des impacts.

informatiques disposant de solides compétences techniques au niveau infrastructure et réseaux mais peu dans le domaine de la sécurité. Ils étaient à ce poste parfois par défaut et, endossaient cette casquette que personne d'autre ne voulait porter souvent malgré eux. Les menaces de l'époque pouvaient être contenues avec des moyens techniques limités, la connectivité à internet y était encore balbutiante et les attaques rarement frontales.

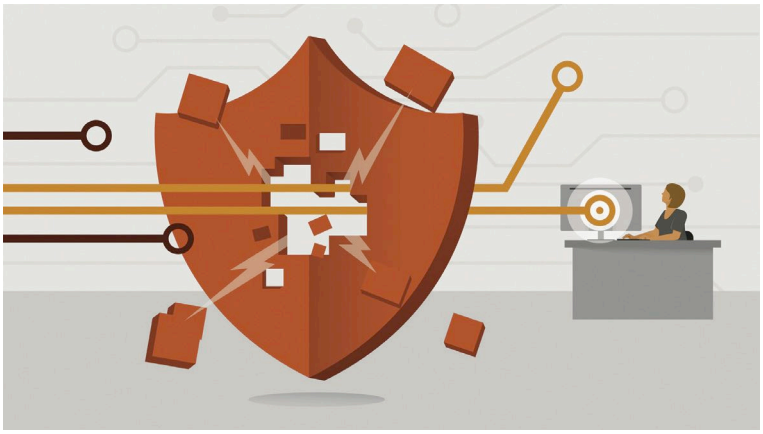
Ainsi, la mise en place d'un antivirus reposant sur des bases de signatures, un anti spam efficace, le tout couplé avec des protections périphériques telles qu'un ou plusieurs firewall, pouvaient garantir une protection suffisante dans la majeure partie des cas. Le principe du moindre privilège comme nous l'appliquons et le connaissons aujourd'hui n'était qu'un obscur concept pour certains tout comme la surveillance active des traces mais les impacts étaient pour l'heure assez négligeables.



La mise en place de formations dédiées

Petit à petit les formations dédiées à l'informatique ont commencé à évoluer et à intégrer la sécurité informatique dans un rythme cependant moins soutenu que les évolutions des menaces avançant quant à elles de manière exponentielle. Les RSSI ont donc intégré cette composante en se formant et en bénéficiant d'un milieu associatif naissant dans le domaine.

Ce n'est cependant que récemment, que les formations ont commencé à inclure des modules spécifiques à la cyber sécurité. La prise en compte des menaces toujours plus pressantes et complexes d'un aspect plus scolaire a servi à faciliter l'accès aux postes de RSSI de manière beaucoup plus confortable et efficiente. Des formations dédiées, liées aux tests d'intrusions et aux protections périphériques avancées, se mettent également en place permettant une meilleure compréhension technique des approches des attaquants.



Un virage dans la gouvernance

De manière concomitante et naturelle, l'émergence des analyses de risques a rajouté un pivot essentiel à l'action du RSSI : la nécessité d'acquérir une vision globale et stratégique de l'activité de l'entreprise.

Ainsi, il ne s'agit plus d'empiler les outils de défense technologique mais bel et bien d'avoir une vision globale et stratégique de son organisation au sens large et non seulement du périmètre de son Système d'Information.

Le renseignement d'intérêt cyber

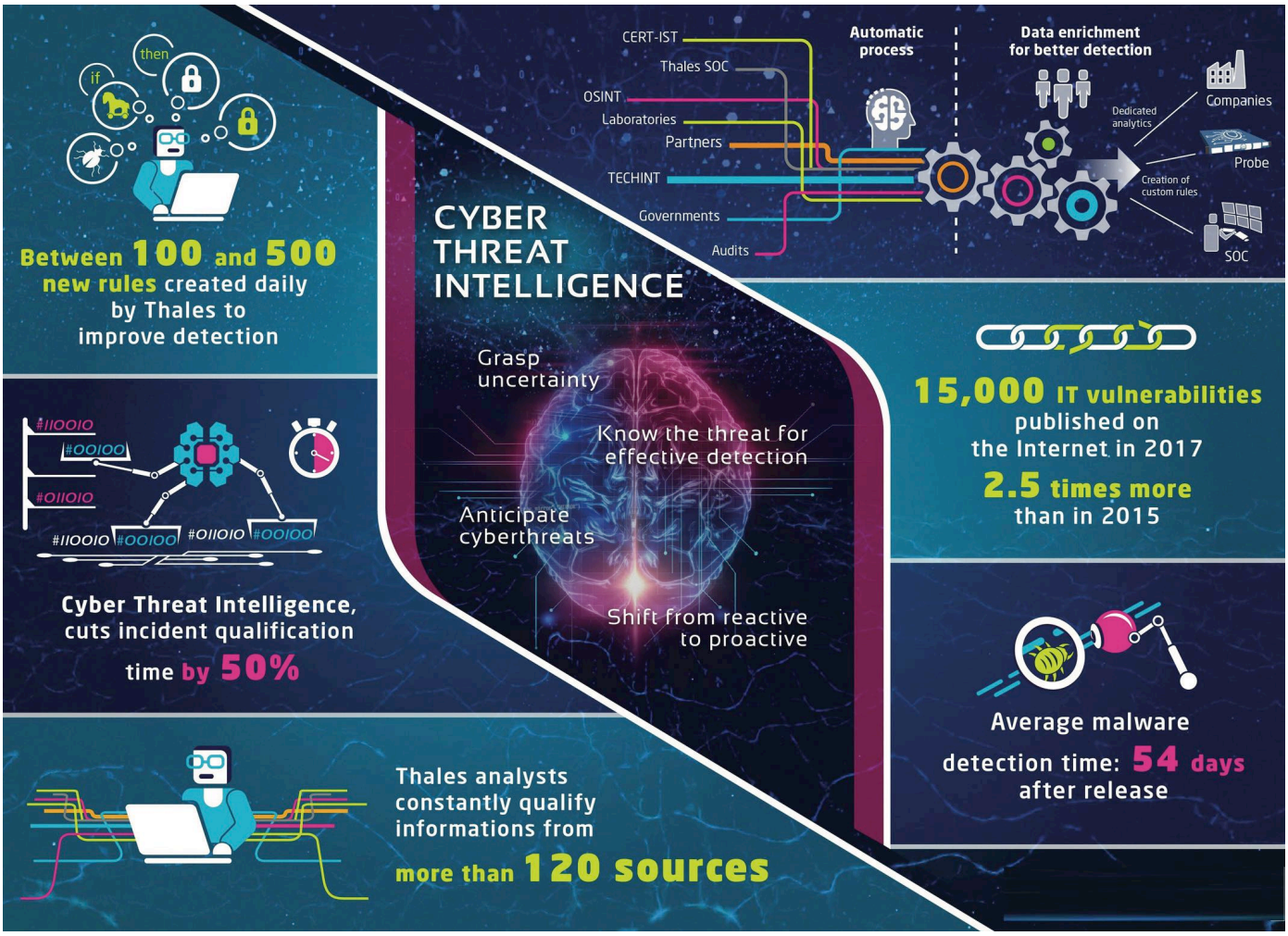
Outre cette implication dans la gouvernance, une connaissance plus approfondie des menaces actuelles est indispensable, définie par le CTI (Cyber Threat Intelligence, en Français le renseignement d'intérêt cyber), permet de mieux appréhender les modes opératoires et apporter une dose de compréhension essentielle que trop peu envisageaient auparavant.



Cela permet non seulement d'être au fait des techniques d'attaques mais également de pouvoir orienter sa défense et se focaliser de manière un peu plus précise sur les signaux faibles de son SI.

De plus, élément important et primordial, cela permet de communiquer afin de prévenir et sensibiliser les collaborateurs à une éventuelle vague de mails disposant de contenus malveillants.

Prenons par exemple la vague d'attaque du malware emotet[1] survenue à l'été 2020. Il a été véhiculé par des emails d'hameçonnage envoyé depuis des adresses emails issues de boites mails compromises rendant ainsi le



premier rempart du filtrage des emails illégitime compliqué. Ces emails étaient en effet issus de conversations légitimes avec par exemple des prestataires habituels. Ils contenaient généralement des pièces jointes Word ou PDF malveillantes, et plus rarement des URL pointant vers des sites compromis ou vers des documents Word contenant des macros.

Certains RSSI ont pu faire confiance en leur technologie (antivirus traditionnel ou comportemental, anti spam…) et se retrouver impacté et d'autres, en étudiant cette notion stratégique, récupérer des précieuses informations afin de déceler des traces en amont (adresses IP de serveurs ayant relayé ces emails par exemple) ou encore restreindre les utilisations des macros en interne (tout en prenant soin de cerner le périmètre d'utilisation des collaborateurs) et donc adopter une vrai posture défensive et proactive.

La communication interne en amont aura également permis de pouvoir augmenter la vigilance des collaborateurs et ainsi réduire un éventuel impact.

Fort de cette connaissance des menaces obligatoires, le RSSI se mue dorénavant en un vrai responsable de la cybersécurité.

Diriger la cybersécurité

Avec la digitalisation à l'extrême, chaque projet doit donc faire l'objet d'un suivi et de directives de sécurités particulières. Cela rend le rôle du RSSI central et incontournable en renforçant son rôle stratégique. L'ANSSI a



d'ailleurs, l'année passée, explicité le poste de directeur cybersécurité ou DSSI.

Il s'agit bel et bien d'un repositionnement en haut de la pyramide du RSSI qui désormais doit réellement s'attacher à prendre en compte l'ensemble des composantes de son organisation et faire partie intégrante des décisions stratégiques. ■

1 https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-019/

Le CLUSIF, Association de professionnels de la sécurité de l'information, propose son Espace CoTer pour fournir des réponses pérennes aux problèmes rencontrés par les collectivités territoriales et assimilées.



Auteur : Damien ALEXANDRE

Le CLUSIF œuvre depuis de nombreuses années pour développer les échanges entre professionnels, permettant de mettre en commun expertises et réflexions au service d'une SSI efficace. Face à la vague de cyberattaque impactant les collectivités, l'Espace CoTer a été créé pour fournir non seulement un espace entre pairs (RSSI, DPO) mais aussi un lieu de rencontre non corporatiste pour tous ceux qui agissent au sein des CoTer pour renforcer leur sécurité, reprenant ainsi de façon concrète le slogan : ***"la sécurité, c'est l'affaire de tous".***



L'Espace CoTer du CLUSIF est aussi un espace d'échanges entre les acteurs de la sécurité au sein des collectivités. Il a pour objectif d'aider les RSSI, DPO et autres acteurs de la sécurité à développer des démarches de gouvernance de la sécurité, sensibiliser les décideurs aux enjeux des cyber-risques, et mettre en œuvre des mesures de sécurité pragmatiques et proportionnées en prenant en compte les spécificités des collectivités.

Les Objectifs du CLUSIF

- Sensibiliser les dirigeants, les responsables d'entreprises et les organismes et pouvoirs publics à l'importance de la sécurité de l'information,
- Contribuer aux programmes d'éducation et de formation dans le domaine de la sécurité de l'information,
- Favoriser, entre ses membres et plus généralement parmi les professionnels de la sécurité, des échanges d'expériences et d'idées dans ce domaine,
- Participer aux grandes orientations nationales et internationales dans ce domaine,
- Réaliser des ouvrages, des synthèses sur l'état de l'art et des techniques en la matière, de créer et formaliser des recommandations, des méthodologies,
- Communiquer vers le grand public par des partenariats d'événements, des conférences, des salons...

Le CLUSIF en quelques chiffres

- Plus de 1 000 membres
- 2 collèges en parfaite équité (offreurs & utilisateurs de solutions SSI)
- 3 types d'adhésion quel que soit le collège
- 45% offreurs / 55% utilisateurs
- 17 groupes et espaces de travail
- 180 réunions par an
- 10 événements par an (conférences, ateliers, webinaires …)

Une réglementation récente pour les collectivités



Les principales obligations des collectivités en matière de sécurité de l'information sont assez récentes. Ainsi le méconnu Référentiel Général de Sécurité1 (RGS) est devenu une obligation pour les CoTer à partir de 2014 et le très médiatique Règlement Général sur la Protection des Données2 (RGPD) date de 2016.

Ainsi les collectivités, jusqu'à ses dernières années, étaient non seulement peu encadrées en matière de sécurité de l'information mais aussi relativement ignorées par les cybercriminels. C'est donc dans un contexte assez tendu que les administrations publiques locales se dotent aujourd'hui d'un Responsable de la Sécurité des Système d'Information (RSSI) soit par recrutement soit par des dispositifs de mutualisation territoriale via des Opérateurs Publics de Services Numériques (OPSN) ou des intercommunalités.

Développer la maturité en matière de Sécurité de l'Information des collectivités

Ce RSSI des collectivités ne doit surtout pas être un héros solitaire ! La maturité des structures en matière de sécurité peut être évaluée tout d'abord par la présence d'un RSSI dédié au sein de la structure puis par son rattachement à la Direction Générale. Trop souvent le RSSI est assimilé à un expert uniquement technique et rattaché à la DSI car la sécurité est vue comme une problématique purement "informatique". Le RSSI doit piloter une gouvernance de la sécurité (système de management de la sécurité



ou SMSI) qui intègre non seulement la direction générale mais également les autres directions ainsi que les élus afin que l'ensemble des acteurs prennent conscience des enjeux métiers associés aux problèmes de sécurité et que les décisions en matière de sécurité, qui sont aujourd'hui stratégiques, puissent être prises au bon niveau de responsabilité. ■

1 https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/

2 https://www.cnil.fr/fr/rgpd-de-quoi-parle-t-on

BIO

RSSI et DPO de SOLURIS, opérateur public de services numériques pour plus de 560 structures publiques, Damien est responsable du service Confiance Numérique avec des missions de conseil autour des Systèmes d'Information (sécurité du numérique, protection de la vie privée, architecture et urbanisation, Schéma Directeur). Il est aussi membre du CLUSIF et animateur de son espace CoTer.

Un club des RSSI pour renforcer la protection des Collectivités Territoriales (COTER) face aux cybermenaces.



Auteur : Philippe STEUER

Un contexte cyber extrêmement menaçant

Les collectivités territoriales (CoTer) sont engagées dans une transformation numérique profonde, autant pour répondre à des obligations réglementaires qu'à un souci de rendre un meilleur service aux citoyens. Cette dépendance de plus en plus forte aux systèmes d'information (SI), couplée à l'hétérogénéité de la taille des communes crée une fragilité, soulignée dans la **Revue stratégique de cyberdéfense** (RSC) de 2018. Cette fragilité, et la dimension très visible et essentielle des services rendus par les CoTer aux citoyens, en font des cibles de choix pour les cyberattaquants. Après Atlanta en 2018, c'est une vague de cyberattaques qui déferle sur la France et les collectivités avec une facteur de progression de x4 entre 2019 et 2020 (source ANSSI). Selon une étude 2020 du Clusif, trois collectivités sur dix auraient été victimes d'un rançongiciel ou ransomware (demande de rançon) en 2019, et la tendance s'est encore accentuée avec la crise sanitaire et la mise en place à marche forcée du travail à distance.

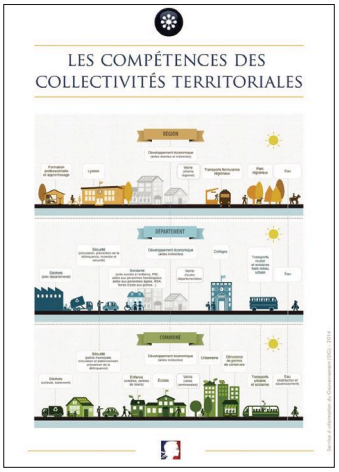


Une maturité cybersécurité des CoTer moindre que celle des acteurs privés de même taille

Les collectivités territoriales ont pris conscience tardivement des enjeux représentés par la cybersécurité, et les efforts déployés pour combler le retard pris dans la mise en œuvre de modèles de sécurisation adéquats **se heurtent à des problématiques inhérentes au contexte des collectivités territoriales.** En effet, certaines d'entre elles ne disposent que d'équipes informatiques réduites ce qui logiquement conduit à ce que la cybersécurité soit traitée par une personne dont ce n'est pas l'unique rôle. De plus, une CoTer seule peut ne pas disposer du poids suffisant pour convaincre un éditeur de renforcer le niveau de sécurité de sa solution, ou encore devoir attendre la fin d'un marché pour pouvoir faire évoluer certaines parties de son SI. Enfin, la sensibilisation des acteurs d'une collectivité territoriale est souvent bien plus complexe que celle d'une structure privée du fait de la multiplicité des métiers exercés par les agents de cette CoTer, mais également par le fait que les décideurs politiques à sensibiliser s'inscrivent dans le temps déterminé de la mandature.

Un réseau de partage dédié aux RSSI des CoTer

Partant de ces constats, plusieurs RSSI de collectivités territoriales ont décidé de créer en 2020 - lors du Forum International de la Cybercriminalité

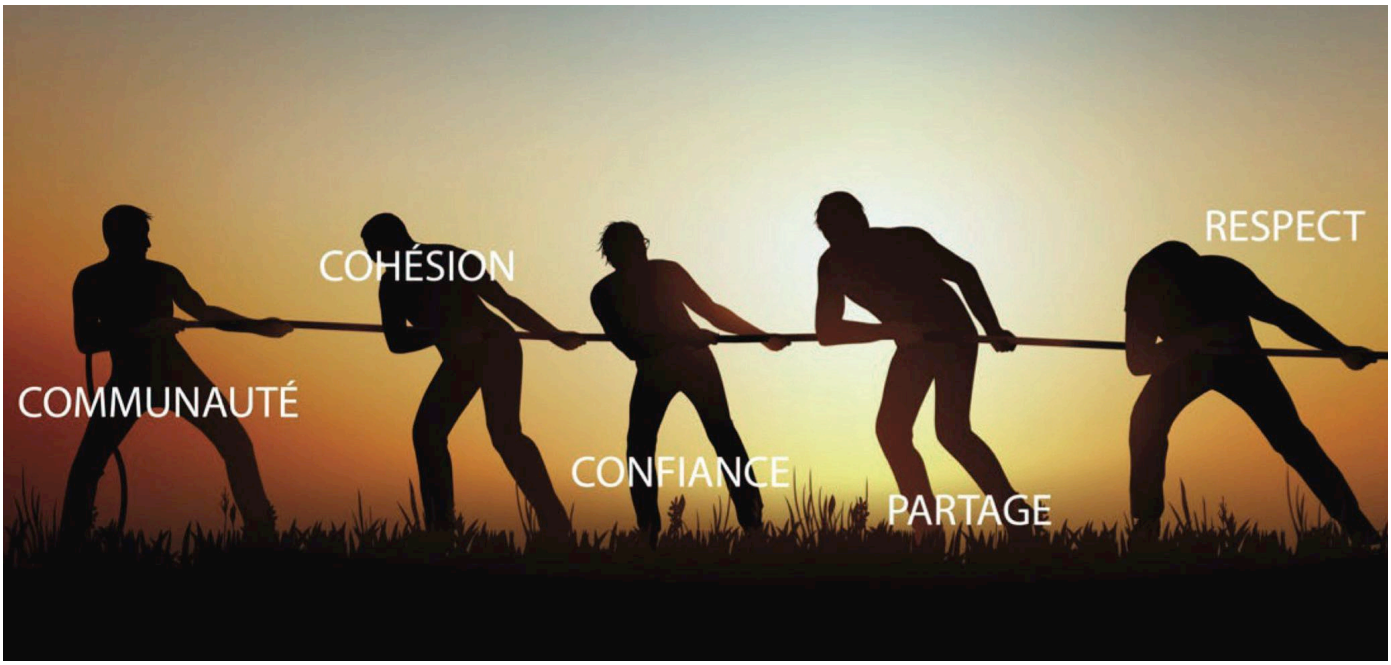


(FIC à Lille) - un réseau, avec le soutien de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), ayant pour vocation d'être **"un lieu de partage d'informations, de bonnes pratiques et d'expérience".** Ce réseau comprend aujourd'hui environ 150 membres venant de différents horizons, villes, métropoles opérateur public de services numériques (OPSN), service départemental d'incendie et de secours (SDIS), départements, régions réparties sur l'ensemble du territoire national et ultra-marin.

Quels objectifs se donne ce club des RSSI des CoTer ?

Les objectifs que se donnent les membres de ce club sont multiples et répondent aux attentes de l'ANSSI (RSC 2018). Tout d'abord il s'agit de se **partager de l'information** sur les cyberattaques subies ou constatées afin de faciliter la détection par les autres collectivités d'attaques semblables. Une plateforme d'échange d'indicateurs de compromission (IOC) a ainsi été déployée dans cette optique. C'est notamment via cette plateforme que certaines campagnes de phishing ont pu être anticipées. Le club permet aussi à ses membres d'échanger sur des **retours d'expérience et des conseils** sur différents sujets traitant de cybersécurité, qu'il s'agisse de sauvegarde, de solutions de sécurité ou encore de gestion des identités. Enfin, la collaboration des différents RSSI permet de montrer des **actions communes** vis-à-vis des éditeurs de solutions dédiées aux CoTer et ainsi d'être en mesure de peser sur les choix retenus par ces éditeurs en termes de cybersécurité.

Les mots forts de notre collaboration sont donc :



BIO

Avec plus de 30 années d'expérience dans le domaine des nouvelles technologies de l'information dont plus de la moitié dans la sécurité de l'information, Philippe STEUER est aujourd'hui Responsable de la sécurité des SI à Bordeaux Métropole. Par le passé, il a notamment été responsable d'une équipe d'intelligence économique au sein d'une banque française puis a été à l'initiative de la création d'un centre de lutte contre la cybercriminalité et en charge d'un centre de réponses aux attaques informatiques (CERT) au sein du grand groupe. Après une année d'étude passée chez Audencia, il crée sa société de conseil en cyber. Il accompagne alors des startups et sociétés françaises et luxembourgeoises pour développer leurs services cyber, les adapter à leur cible en prenant en compte le pays et le domaine d'activité. Fin 2018, nouveau défi professionnel sur Bordeaux. Il effectue un audit de maturité sécurité au sein de la DSI de Bordeaux Métropole après lequel il est intégré comme RSSI pour accompagner la transformation numérique de la Métropole. En veille permanente sur les enjeux de sécurité, Il a participé à différents groupes de travail, anime des conférences et des tables rondes sur les menaces, vulnérabilités et contre-mesures dans le cyberespace. Il est également actif dans le rayonnement de l'esprit de défense et dans le renforcement du lien armées-Nation en tant qu'auditeur IHEDN et réserviste auprès de la Direction Zonale de la Police Judiciaire de Bordeaux.

Le club se pérennise en se structurant.

2020 a été une année **d'expérimentation** avec un panel représentatif des collectivités territoriales avec une douzaine de RSSI qui a permis de confirmer l'intérêt de ce club avec le support de l'ANSSI.

2021 est une année dite de **déploiement** qui nous a permis d'étendre notre réseau à quelques 150 RSSI.

2022 sera l'année de la **pérennisation** avec la mise en place d'une structure légitime, toujours en relation forte avec l'ANSSI et nous permettant d'accueillir dans les meilleures conditions l'intégralité de nos amis RSSI des CoTer.

D'ores et déjà, le club assoit ses actions sur une note de cadrage, une charte et un engagement de confidentialité permettant des échanges se déroulant sous la règle de Chatham House.

Enfin, le club se réunit en comité de coordination chaque mois pour proposer les orientations thématiques, suivre les activités et assurer le secrétariat de la communauté.

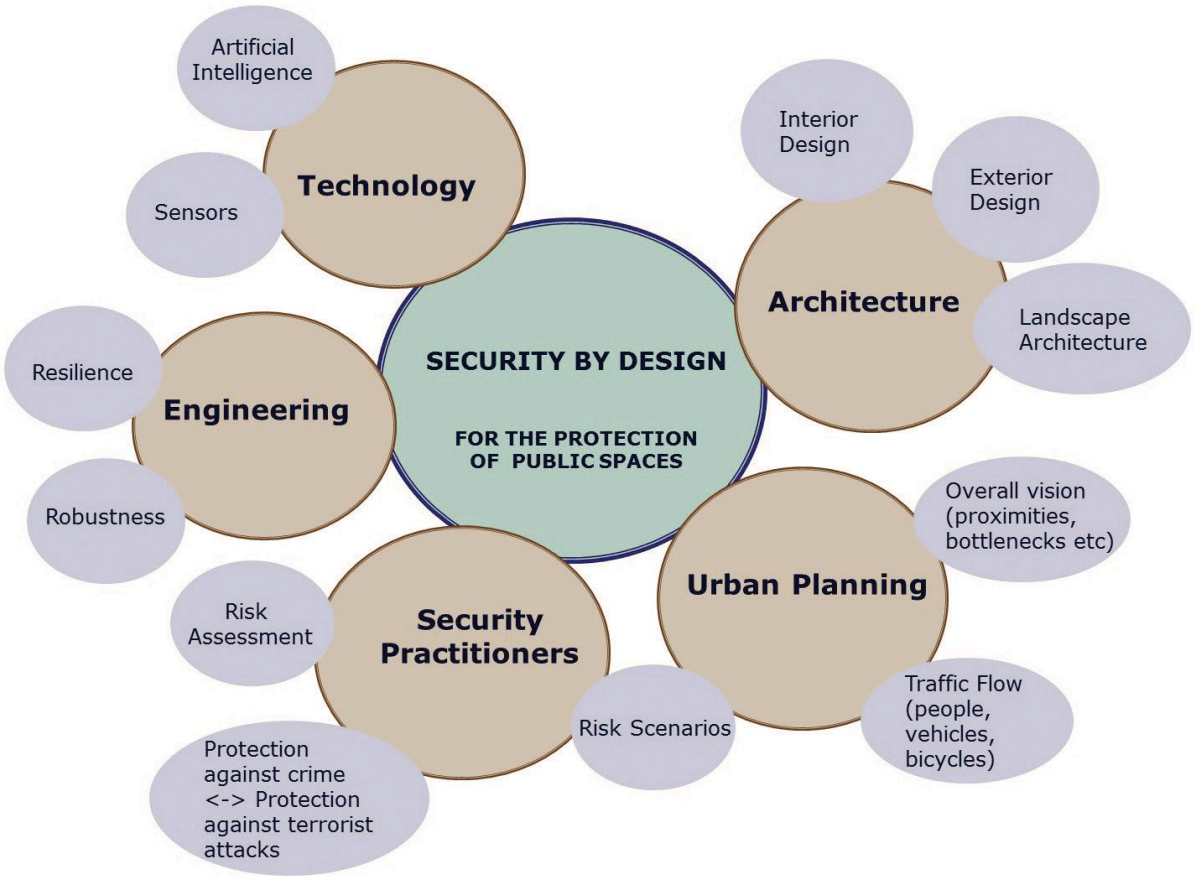
Les prochains défis

Les RSSI des collectivités territoriales vont faire face dans les mois et années à venir à des défis toujours



plus importants : identité citoyenne, smart city, dématérialisation de la vie publique,… dans un contexte de recherche de souveraineté, de déploiement de milliards d'objets connectés et de la 5G. Cette transformation, bien souvent, à marche forcée nécessite d'adopter une posture d'anticipation et de "security by design" afin de préserver la confiance de nos citoyens et partenaires.

Pour relever ces défis, ils pourront s'appuyer sur les travaux du club qui travaillera à renforcer la collaboration entre les collectivités territoriales mais aussi à garantir une meilleure prise en compte de la cybersécurité par les décideurs publics et les organisations en place au sein des collectivités. ■



Confiance numérique des territoires : mutualiser pour faire face aux cyber-risques.



Auteur : Benoît LIENARD

Le défi de la multitude

De quoi parlons-nous quand nous évoquons les collectivités locales ? Comme dans le secteur privé les petites structures sont bien plus nombreuses que les grandes. Conséquence directe : ces petites collectivités locales n'ont aucune compétence technique interne sur les questions de cybersécurité. Pourtant les petits villages disposent chacun d'un système d'information autonome, qui n'est pas plus épargné que celui d'une métropole face aux menaces cyber, ransomwares en tête.

Or la protection du système d'information des collectivités locales est un enjeu de souveraineté et de continuité de notre système économique et démocratique. Elles détiennent une multitude de données personnelles sur les citoyens des territoires, et la continuité des services publics locaux est souvent cruciale pour la vie locale (accueil des jeunes enfants, gestion des déchets, transports publics, etc.).



Agir collectivement dans l'intérêt de chacun

La force d'un opérateur public de services numériques comme Soluris est de réunir plusieurs centaines de collectivités adhérentes qui, bien qu'étant indépendantes les unes des autres, savent se réunir pour former une gouvernance unie capable de mutualiser les moyens pour porter des projets communs ambitieux.

C'est dans ce cadre que Soluris a imaginé une offre de confiance numérique locale, qui se nourrit d'une part des échanges nationaux et des

BIO

Passionné de projets collectifs et d'intérêt général, Benoît Liénard est directeur général de SOLURIS, opérateur public de services numériques de confiance pour les collectivités territoriales. Impliqué depuis 20 ans dans la transformation numérique publique, il participe à de nombreux projets nationaux de dématérialisation auprès de ministères, associations d'élus (Association des Maires de France, FNCCR) et de différents réseaux spécialisés (Déclic, SNDGCT, …). Pour maintenir la confiance entre les services publics et les citoyens ou les entreprises, la compréhension des enjeux de sécurité est centrale. SOLURIS en a fait une de ses priorités et s'attache à accompagner ses 560 adhérents vers un déploiement maîtrisé du numérique dans le respect des bonnes pratiques (RGS, RGPD, ….).



préconisations des autorités compétentes (ANSSI, CNIL) et d'autre part de remontées des besoins de terrain exprimés par les élus locaux et les agents territoriaux.

Une action en 4 volets complémentaires

Les actions de Soluris pour augmenter la confiance numérique de ses adhérents combinent 4 volets.

▸ **Volet 1 : la sensibilisation générale et la formation des élus et des agents.** Toute occasion est bonne pour parler cybersécurité ou RGPD aux élus et agents durant l'année : réunions dédiées (nos "matinales sécurité"), les assemblées du Comité Syndical, les formations dédiées, les communications écrites par newsletter ou dans des médias spécialisés comme celui-ci. Cet enjeu est majeur pour augmenter la maturité des décideurs, en indiquant les enjeux et responsabilités mais aussi les moyens d'action.

▸ **Volet 2 : l'équipement des collectivités.** Soluris déploie différentes solutions pour augmenter la sécurité des adhérents sur le terrain. La mutualisation permet des économies d'échelle qui rendent accessibles à chaque petit village le déploiement de solutions indispensables telles que la sauvegarde des données ou encore de logiciels anti-ransomware centralisés.

▸ **Volet 3 : l'accompagnement sur-mesure et l'analyse des risques.** Pour aider les élus locaux dans la définition de leur propre plan d'actions de sécurité, Soluris propose une méthode synthétique ("Pragmarisk") qui met en évidence les risques auxquels leur collectivité est exposée et les aide à identifier les actions prioritaires à mener, immédiatement et dans la durée. Cette démarche s'appuie sur la méthode EBIOS de l'ANSSI, en l'adaptant au contexte spécifiques des collectivités. La démarche permet d'aller jusqu'à l'homologation au Référentiel Général de Sécurité. Un gage de confiance pour les administrés et les partenaires des collectivités.

▸ **Volet 4 : l'accompagnement à la conformité au RGPD.** Soluris est Délégué mutualisé à la Protection des Données de plus de 450 collectivités locales qui sont accompagnées dans ce cadre par des sessions de sensibilisation et de formation, et outillées par le logiciel MADIS, spécifiquement conçu par Soluris dans ce but et dont le code est publié en logiciel libre sur la forge nationale de l'Adullact.



Soluris, **au cœur des réseaux de la confiance numérique.**

Soluris est un opérateur public de services numériques. Nous accompagnons les élus et agents de nos 580 collectivités territoriales adhérentes, en Charente-Maritime et Deux-Sèvres, sur les principaux défis de la transformation numérique. Notre panel de solutions est vaste, allant des besoins d'optimisation interne jusqu'au développement de services numériques aux citoyens, en passant par la confiance numérique.

SOLURIS
SOLUTIONS NUMÉRIQUES TERRITORIALES INNOVANTES

Soluris est très actif auprès des acteurs nationaux qui œuvrent pour la sécurité des collectivités : ANSSI, CNIL, GIP Cybermalveillance.gouv.fr, CLUSIF, CLUSIR, Fédération Déclic … L'objectif est double : vérifier le bon alignement de nos actions avec les préconisations nationales mais aussi et surtout partager les bonnes idées et les bonnes pratiques entre acteurs publics et privés mobilisés pour la confiance numérique des territoires.



Un guide dédié à la cybersécurité des collectivités

L'Association des Maires de France et l'ANSSI ont publié fin 2020 un guide intitulé : "Cybersécurité : toutes les communes et intercommunalités sont concernées". Il est librement téléchargeable sur le web. Soluris est fier d'y avoir contribué. ■

La prévention de la cyber-criminalité au niveau d'un territoire : l'exemple du réseau des référents cybermenaces de Nouvelle Aquitaine.



Auteur : Paul BOUSQUET

La cybercriminalité peut être décrite comme une délinquance organisée et transnationale, dont les motivations sont, à l'exception notable de l'ingérence interétatique, principalement d'ordre économique.



Les évolutions technologiques récentes, comme le développement des objets connectés, l'usage massif des réseaux sociaux, le Cloud, et bientôt la 5G ou les smarts cities, augmentent fortement les menaces qui pèsent sur les acteurs économiques. De la même manière, la modification des comportements individuels et des usages professionnels, induite notamment par l'actuelle pandémie due au coronavirus, a également eu un effet d'entraînement significatif en augmentant la surface d'exposition des acteurs aux attaques.



La facilité d'accès à des informations stratégiques sur les entreprises est donc une formidable opportunité pour les délinquants, qui disposent en outre de technologies d'agrégation des données (big data et intelligence artificielle), entraînant une sophistication grandissante des attaques et un meilleur ciblage des victimes, tout en garantissant un certain anonymat aux auteurs (VPN, darknet, chiffrement, etc).

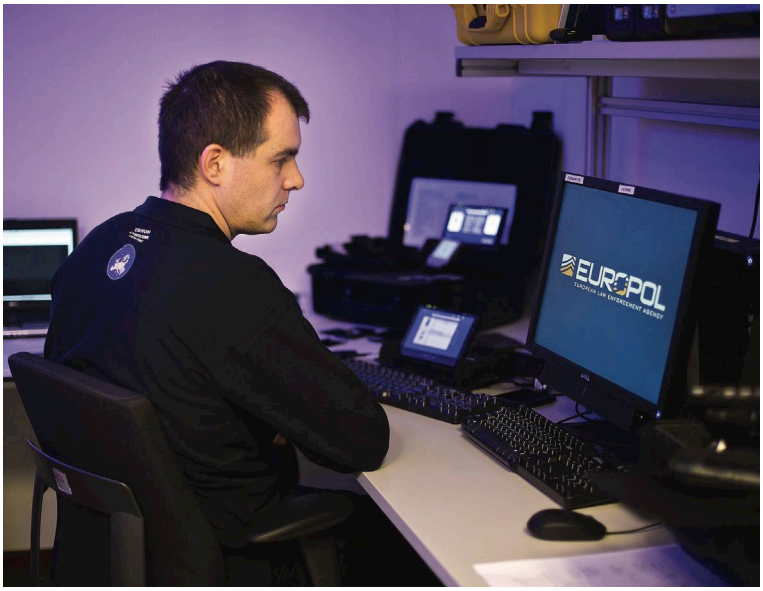
En définitive, le risque d'une attaque au niveau mondial, ayant des conséquences systémiques sur notre économie, n'est plus une hypothèse d'école et est évoquée de plus en plus souvent comme une des grandes vulnérabilité de nos sociétés modernes.



Or, en dépit de cette menace grandissante, les services d'enquête spécialisés de la Police et de la Gendarmerie nationale sont encore confrontés trop souvent au retard ou à l'absence de plainte de la part des victimes, ces dernières privilégiant la remédiation de leur système d'information dans la discrétion, pensant limiter de cette manière les conséquences négatives opérationnelles, réputationnelles et légales d'une cyberattaque.

Le signalement rapide des faits aux autorités de police présente pourtant de nombreux avantages tant pour les victimes que pour les autorités :

- aider les victimes à réagir de façon adéquate ;
- leur permettre d'obtenir le droit à réparation du préjudice subi ;
- déterminer les responsabilités, internes et externes, liées à l'attaque ;
- récupérer tout ou partie des fonds ou des données dérobées ;
- permettre aux services d'enquête de faire des recoupements et des analyses sur les méthodes et les modes opératoires utilisés par les cybercriminels, afin de faciliter leur identification ;
- contribuer à l'amélioration de la cybersécurité à l'échelon national et international, grâce à la collaboration policière ;
- déterminer la volumétrie et le type d'attaques afin d'évaluer l'état de la menace ;
- permettre à l'Etat d'affecter des ressources à la lutte contre ces menaces identifiées.



Le réseau des référents cybermenaces (RCM) mis en place à titre expérimental par la direction centrale de la Police Judiciaire depuis 2018 dans les régions Grand Est, Bretagne et Nouvelle Aquitaine, puis généralisé progressivement à l'ensemble du territoire national en 2020, ambitionne d'apporter une réponse à ce constat.

En Nouvelle Aquitaine, le réseau des référents cybermenaces est composé à ce jour de 16 réservistes citoyens, aux profils professionnels variés : chefs d'entreprise, cadres du secteur privé ou du secteur public, RSSI, experts dans le domaine technique ou juridique ... Ce réseau est en pleine expansion

territoriale, avec la création récente d'une section Nord Aquitaine, implantée à La Rochelle.

Les réservistes proposent des sensibilisations adaptées à chaque entités, publique ou privée, qui s'adressent tout particulièrement aux dirigeants, mais également à leurs collaborateurs et à leurs responsables informatiques. Ils donnent des conseils de bonne hygiène numérique et de premiers secours en cas de cyberattaque, de manière à en limiter les conséquences. Leur connaissance fine des modes opératoires des criminels, illustrée d'exemples concrets sur le territoire, permet une meilleure prise de conscience de la part des chefs d'entreprise, et a pour but de provoquer une amélioration effective de la sécurité des entreprises sensibilisées.

Deux objectifs opérationnels majeurs sont recherchés : la préservation des preuves numériques et la rapidité de l'alerte vers les services d'enquête.



BIO

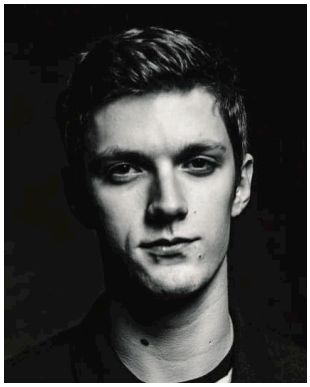
Paul Bousquet, commissaire divisionnaire, est le chef de la division de lutte contre la criminalité financière à la direction territoriale de Police Judiciaire de Bordeaux. La division de lutte contre la criminalité financière est composée d'une trentaine d'enquêteurs spécialisés, et notamment d'un groupe de lutte contre la cybercriminalité. La Police Judiciaire est en charge de la lutte contre la criminalité organisée et la grande délinquance financière. La lutte contre la cybercriminalité entre à ce titre dans ses domaines de compétence, et notamment les affaires de piratage, de pédopornographie, d'escroquerie ou d'extorsion commis par le moyen des nouvelles technologies. Afin de renforcer la prévention de cette criminalité et de sensibiliser les entreprises, grandes ou petites, à la cybersécurité, la direction territoriale de la Police Judiciaire de Bordeaux a également mis en place depuis 2018 un réseau de prévention des cybermenaces (RCM), actuellement composé de réservistes, issus du monde de l'entreprise et de la société civile, installés sur l'agglomération bordelaise et sur le nord de la Région Nouvelle Aquitaine (La Rochelle, Poitiers, Limoges).

La préservation des preuves numériques est évidemment le préalable obligatoire à une enquête. Trop souvent, les preuves d'une intrusion ne sont pas conservées, soit que le système de la victime ne le permette pas ou que la victime ait privilégié la remédiation, sans penser à conserver les traces intéressantes.

La rapidité de l'alerte vers les services de police ou de gendarmerie est également déterminante pour permettre des investigations efficaces. Par exemple, en cas de commission d'une escroquerie financière, une action rapide de la police, coordonnée avec l'établissement bancaire de la victime, permet souvent d'obtenir le gel et le retour des fonds, objet de l'escroquerie. De la même manière, la rapidité de l'alerte est cruciale pour permettre aux services enquêteurs de récupérer des données techniques, disponibles à l'étranger. Les outils de coopération policière et judiciaire internationale existent en matière de lutte contre la cybercriminalité, mais nécessitent une grande réactivité pour être véritablement opérationnels, les fournisseurs d'accès ou de service internet ne conservant les données qu'un temps limité. ■



Un nouvel impératif académique : faire comprendre aux étudiants les enjeux de la sécurité digitale.



Auteur : Nathan PRUDHOMME

Dans un monde toujours plus digitalisé où tout tend à être numérisé encore davantage, l'étudiant se doit de connaître l'importance de la technologie car il a bien souvent eu l'opportunité de grandir et de pouvoir travailler avec différents Systèmes d'Information. Ce dernier a pu, lors de son cursus mais aussi lors de ses activités extra-scolaires, utiliser et voir évoluer la technologie en prenant conscience des dérives occasionnées, des risques mais évidemment aussi des nombreux bénéfices que ces Systèmes ont pu apporter.



Toujours plus d'appareils disponibles signifient plus de fonctionnalités. Ces fonctionnalités ouvrent davantage le champ des possibles en ce qui concerne les failles et celles-ci représentent de nouveaux défis pour les pirates informatiques. La multiplication des appareils connectés a, bien entendu, créé de très nombreuses brèches auxquelles il faut obligatoirement faire particulièrement attention. Ce qui est valable ici pour la sphère privée l'est encore davantage pour la sphère professionnelle où les retombées pourraient être désastreuses. C'est à cela que les étudiants doivent être sensibilisés tout au long de leur scolarité.

On ne nous le répètera jamais suffisamment, les enjeux de la sécurité informatique sont primordiaux voire vitaux pour la prospérité économique et le bon fonctionnement de l'entreprise. Il est important pour les étudiants

BIO

Nathan Prudhomme est étudiant en Master 2 spécialité Audit et Conseil en Systèmes d'Information à Institut Mines-Télécom Business School après une Classe Préparatoire aux Grandes Ecoles option Economie. Ce dernier est Secrétaire Adjoint de Charente Maritime Cybersécurité, passionné par l'informatique depuis son plus jeune âge mais également de sport, plus particulièrement de football américain. Il s'intéresse à bons nombres de domaines différents et avec une expérience encore nouvelle de la cybersécurité, il a un regard neuf et jeune des Systèmes d'Information, avec lesquels il a grandi.

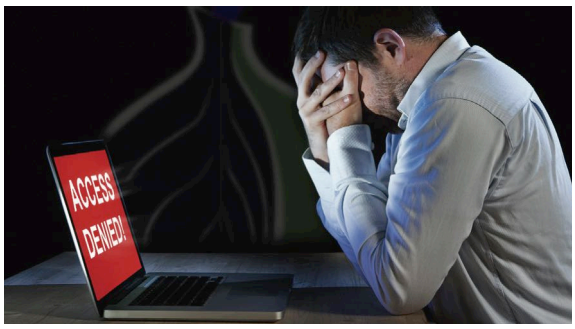


de le comprendre le plus tôt possible et de l'intégrer dans leurs priorités bien avant leur diplôme obtenu. Lors de la crise sanitaire, les attaques ont été multipliées par 4 d'après BPI France[1].

Cela doit nous toucher en tant qu'étudiant, ces attaques ont pu ou pourront probablement impacter les entreprises qui nous embaucheront à la fin de notre scolarité et nous pouvons agir pour prévenir davantage de catastrophes. Grâce à CMCS, il est possible d'avoir une vision plus étoffée et précise des enjeux de la cybersécurité, que l'on soit étudiant ou un professionnel en entreprise. L'un des facteurs les plus importants, je tends à le croire, pour un futur manager dans la sécurité des systèmes d'information est l'expérience.

A défaut de pouvoir avoir l'expérience de plusieurs années en entreprise, ce colloque permet aux étudiants de se renseigner sur la mise en place et le fonctionnement effectif d'une Politique de Sécurité des Systèmes d'Information, mais aussi de rencontrer des spécialistes et des professionnels férus de cybersécurité dans de nombreux domaines. CMCS permet donc d'acquérir de l'expérience grâce à de nombreux points de vue et grâce à l'expérience d'entreprises diverses ayant : soit été victime d'attaques, soit étant une entreprise active pour se prémunir contre d'éventuelles attaques.

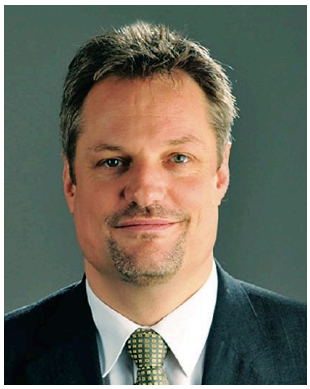
Notre génération et celles qui lui succèdent ont eu la chance (?) de pouvoir grandir avec un ordinateur entre les mains, chacun de nous en connaît les bénéfices mais aussi les risques qui vont de pair avec la numérisation de nos tâches. Cependant, il est possible de remarquer que, malgré cela, nous ne sommes pas suffisamment vigilants, les enjeux de la sécurité informatique semblent loin de nous. La plus grande faille dans les systèmes d'information reste quasi systématiquement le facteur humain lui-même. Une sensibilisation au plus tôt permettrait de changer le mantra "Cela n'arrive qu'aux autres, il n'y pas de raisons que cela m'arrive, je ne représente aucun intérêt pour les pirates". Cette mentalité en va de même pour les entreprises, trop nombreuses sont celles qui n'estiment pas être de taille suffisamment conséquente pour être la cible de pirates. Malheureusement, n'importe qui peut en être la cible. Une autre idée reçue serait celle de penser que seulement certains secteurs sont touchés par les cyberattaques. Comme nous l'avons décrit plutôt, c'est quand on s'y attend le moins que nous pouvons devenir la cible d'attaques. Malheureusement, bon nombre d'entreprises l'ont appris à leur dépens.



CMCS permet en cela d'avoir une vision plus claire du danger avec des explications brèves, néanmoins précises à la portée du plus grand nombre, y compris des étudiants. Le format se veut dynamique et varié avec de nombreuses interventions d'experts. Il y a également autant d'interactions que possible grâce aux tables rondes pour rendre le colloque plus intéressant en impliquant les participants. ■



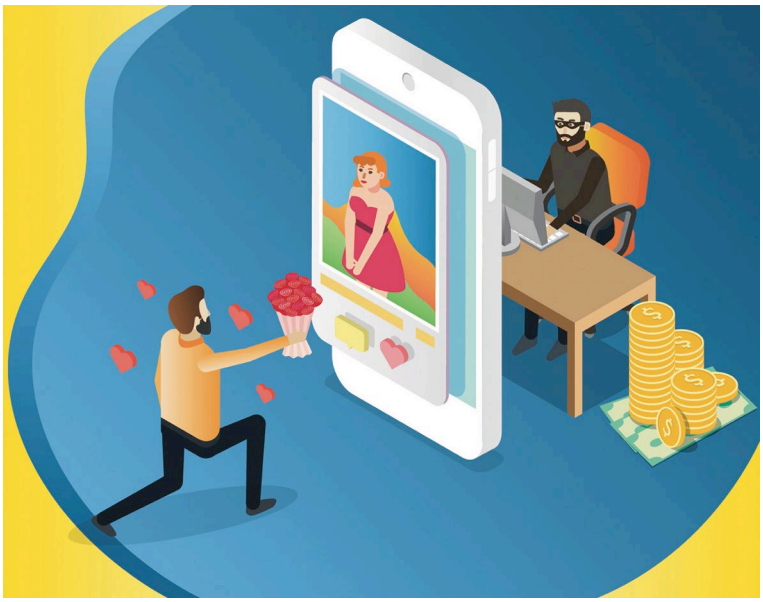
Pour une professionnalisation du traitement des plaintes en matière de cyber criminalité à la Police cantonale de Genève.



Auteur : Patrick Ghion

Une des questions fondamentales dans le traitement des plaintes en matière de cyber criminalité a toujours été la pondération des avantages d'une gestion centralisée au regard d'une gestion dans les brigades à thème.

Jusqu'ici l'ensemble des plaintes en lien avec la cybercriminalité étaient traitées au sein des Brigades selon leur cœur de métier. Par exemple, les plaintes de type Romance Scam étaient traitées à la Brigade des infractions contre les personnes alors que les plaintes contre les escroqueries sur Internet étaient traitées à la Brigade des vols ou encore les affaires de Ransomware à la Brigade de répression du banditisme.

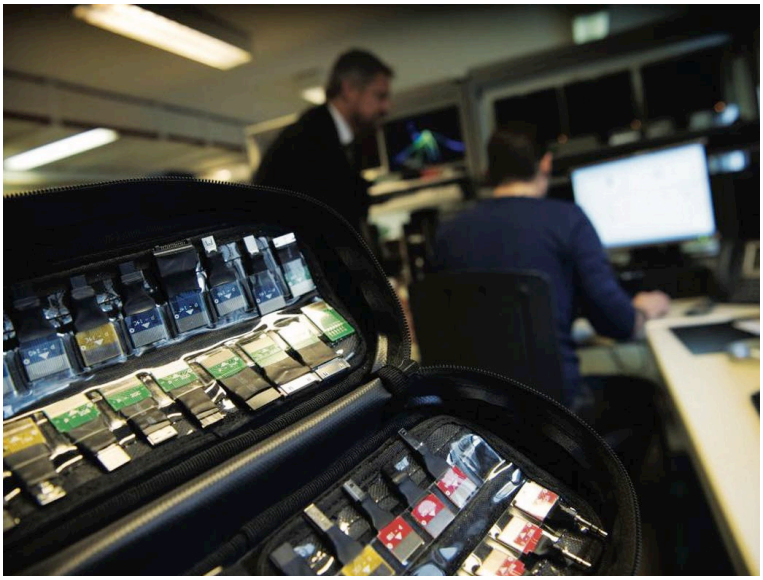


Le dilemme a longtemps été de savoir s'il était plus efficace de faire traiter les plaintes dans les brigades selon leur délit ou de regrouper toutes les plaintes cyber et de les faire traiter par des policiers spécialisés.

La Police cantonale de Genève a aujourd'hui fait le pas vers une brigade spécialisée dans les délits liés à la cybercriminalité en les regroupant au sein d'une même entité et en professionnalisant les policiers par une formation de niveau académique.

BIO

Le Capitaine Patrick Ghion travaille pour la Police Cantonale de Genève depuis 20 ans. Auparavant responsable de l'unité de lutte contre la criminalité informatique, Patrick Ghion est aujourd'hui chef de la section forensique de la police judiciaire de l'Etat de Genève, constituée de 4 brigades dont celle de lutte contre la criminalité informatique. Avant de rejoindre les forces de l'ordre, il a travaillé dans plusieurs banques suisses et a également vécu un temps comme instructeur de plongée en Asie. Père de deux enfants, ses principaux hobbys sont la plongée sous-marine et le pilotage d'avions.

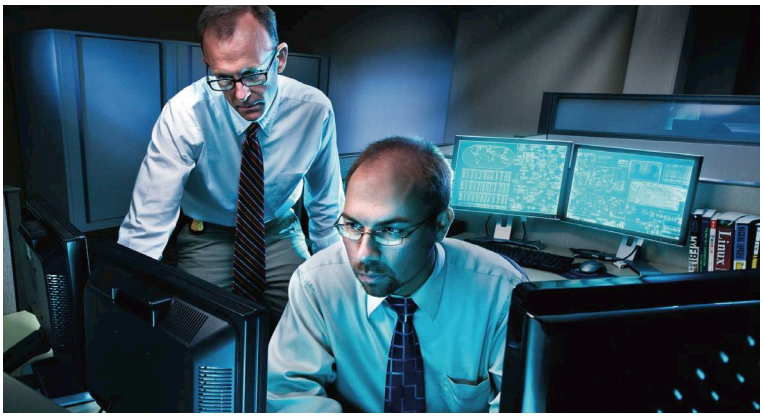


Des effectifs à la hauteur des enjeux

A terme, la Brigade des cyber enquêtes (BCE) va être composée de 17 inspectrices et inspecteurs spécialisés et d'une secrétaire. Créée au 1er septembre 2021 avec un effectif de 12 policières et policiers, des renforts sont attendus dans le courant de l'année 2022.

Les spécialistes qui constituent la Brigade des cyber enquêtes ont été choisis sur la base de leur motivation, de leur autonomie et de leur capacité à suivre une formation de niveau académique en lien avec leurs nouvelles fonctions.

Ce sont véritablement des enquêtrices et des enquêteurs qui forment un triptyque opérationnel avec les analystes de la Brigade de renseignement criminel (BRC) et les spécialistes forensiques de la Brigade de criminalité informatique (BCI).



Il est certain que le développement de la cybercriminalité à Genève et dans le monde ne va cesser de croître et on ne mesure pas encore les effets des nouvelles technologies à venir, telle que la 5G, l'intelligence artificielle ou encore l'utilisation des ordinateurs quantiques à des fins criminelles.

Toutefois, les effectifs de la police ne sont pas extensibles et leur nombre ne doit pas être le seul critère pour le développement de la brigade. C'est la raison pour laquelle, nous allons également travailler sur des processus automatisés, l'optimisation du traitement des plaintes et développer des partenariats publics privés (PPP) afin d'être véritablement au service de la population genevoise.



Un cahier des charges riche et varié

Les missions confiées à la Brigade des cyber enquêtes sont les mêmes que pour tout Inspectrice et Inspecteur de Police judiciaire. Établir les faits, rechercher et arrêter les auteurs de crimes et délits dans le domaine cyber sont les missions principales.

Les principaux thèmes traités seront ceux liés à la **Cybercriminalité économique,** tel que le traitement des affaires de phishing, d'escroqueries sur Internet, de



Romance Scam ou encore de fraudes à l'investissement en ligne. Un autre pan de leurs missions traitera certains aspects des **Cyber-délits sexuels,** tels que la pornographie interdite et les Sextorsions. Finalement, ils traiteront également les affaires de **Cyber-atteinte à la réputation et pratiques déloyales.** Outre les Cyber-atteintes à la réputation, elles comprennent également le Cyberbuylling/mobing par exemple.

A l'instar des autres Inspectrices et Inspecteurs de police, ils auront des missions annexes, tels que des protections personnelles de VIP et de patrouilles dans le terrain.

D'une manière générale, les escroqueries sur Internet occupent une place prépondérante dans les affaires qui occupent les services de Police. Je suis convaincu

que la technique a ses limites quant à la protection des utilisateurs. Il est naturellement très important d'avoir une protection antivirus à jour, un pare-feu efficace et des systèmes d'exploitation régulièrement mis à jour tout comme les logiciels utilisés.

La prévention : un aspect incontournable de la lutte contre la cyber criminalité

Toutefois, si l'on souhaite véritablement augmenter le niveau de conscience des utilisateurs, cela passe nécessairement par une prévention adéquate. Cela signifie des informations répétées et des messages différentiés en fonction de l'âge des utilisateurs par exemple. Le rôle des médias est capital dans cette prévention puisque ceux-ci peuvent toucher la population de façon régulière et à large échelle. Du côté de la Police cantonale de Genève, nous envisageons actuellement de renforcer nos partenariats publics privés afin de soutenir les messages de prévention et de limiter le préjudice lié à ces escroqueries.

Une formation spécifique indispensable

Grâce à l'appui de la Direction de la Police, l'ensemble des policiers cyber vont suivre une formation académique



sous la forme d'un ***Certificate of Advanced Studies Cybercriminalité, spécialisation cyberenquête*** (CAS CY-E) auprès de la HES-SO de Suisse occidentale.

Le programme très riche et actuel comprendra un tronc commun sur l'informatique générale et les réseaux Internet, le contexte cybercriminel et les mesures opérationnelles notamment.

La spécialisation cyberenquête quant à elle comprendra des cours sur l'univers cybercriminel tel que le Darknet, les réseaux cybercriminels, les flux financiers avec les cryptomonnaies et les néobanques.

Un des aspects novateurs qui a tendance à se développer sont les aspects de perturbation. En clair, si l'on est incapable d'interpeller les suspects pour des raisons techniques ou légales, il est important de pouvoir perturber les activités criminelles pour réduire le nombre de victimes.

Par conséquent, nous assistons à une véritable professionnalisation du traitement de l'enquête judiciaire en matière de cybercriminalité à la Police cantonale de Genève pour arriver un système cohérent et unique en Suisse, au profit de la population. ■



Cybermalveillance.gouv.fr : un concept novateur dédié à la prévention et l'assistance aux victimes de cybermalveillance.



Créé il y a maintenant 4 ans, le dispositif Cybermalveillance.gouv.fr est une construction originale qui a le triple objectif de sensibiliser les populations aux risques numériques, de leur apporter une assistance en prévention ainsi que lorsqu'elles sont victimes et d'observer l'évolution des cybermenaces pour les anticiper et y répondre.

Auteur : Jérôme NOTIN

Une volonté de l'État de répondre au besoin des populations

Le dispositif Cybermalveillance.gouv.fr est issue de la stratégie numérique du Gouvernement présentée le 18 juin 2015 et dont les objectifs ont été ensuite détaillés dans la Stratégie nationale pour la sécurité numérique publiée le 16 octobre 2015.

L'État est à l'époque parti du constat que s'il était plutôt bien en mesure de protéger ses propres infrastructure ou les infrastructures vitales du pays, il se devait d'apporter une réponse structurée et coordonnées aux autres composantes de la société qui étaient souvent désarmées face à une cybercriminalité en plein essor.

C'est de cette volonté qu'est né en octobre 2017, le dispositif national de prévention et d'assistance aux victimes de cybermalveillance : Cybermalveillance.gouv.fr.

BIO

Jérôme Notin est le directeur général du groupement public Action contre la cybermalveillance (GIP ACYMA) qui opère la plateforme Cybermalveillance.gouv.fr et dont il a été le préfigurateur au sein de l'Agence nationale de sécurité des systèmes d'information. Précédemment, il a exercé durant plus de 20 ans des responsabilités dans plusieurs entreprises du secteur privé du domaine de la cybersésurité et du développement du logiciel libre.

Un dispositif original porté par un partenariat public-privé

Conscient qu'il n'était pas et ne devait pas être le seul acteur à s'impliquer dans cette mission d'intérêt public, l'État a voulu pour la conduire, l'organiser sous la forme d'un groupement d'intérêt public, le GIP ACYMA (pour Action Contre la CYber MAlveillance).

Créé conjointement par l'Agence nationale de sécurité des systèmes d'information (ANSSI) et le ministère de l'Intérieur, ce dispositif regroupe aujourd'hui plus de 50 acteurs étatiques et de la société civile engagés pour contribuer à sa mission. On retrouve ainsi parmi ses membres des ministères et agences, des associations professionnelles, de consommateurs ou encore d'aide aux victimes, des opérateurs, des éditeurs, des assureurs, des banques…



Les missions du dispositif s'articulent en trois axes qui s'alimentent entre eux dans une boucle vertueuse : la prévention, l'assistance aux victimes, et l'observation de la menace.

Les services offerts par Cybermalveillance.gouv.fr sont principalement délivrés au travers de la plateforme éponyme. Ils s'adressent à tous les types de publics qui ne sont pas couverts par les autres dispositifs de l'État, qu'il s'agisse des particuliers, des entreprises, des associations, des administrations et des collectivités, et en particulier ceux d'entre-eux qui ne disposent pas de connaissances ou de supports suffisants en cybersécurité.

L'indispensable prévention

Prévenir les populations contre les risques liés à la cybermalveillance et les bonnes pratiques à mettre en œuvre pour les palier constituent l'une des principales missions du dispositif Cybermalveillance.gouv. fr.

Au travers des échanges qu'il peut avoir avec ses différents publics, le constat de Cybermalveillance. gouv.fr est que, dans la grande majorité des cas, les cyberattaques pourraient être évitées ou pour le moins limitées dans leurs effets, si des mesures d'hygiène informatique ou de réaction élémentaires étaient appliquées. C'est ce défi que le dispositif essaie de relever au quotidien dans la manière dont il conduit ses actions de sensibilisation en s'efforçant de délivrer des messages et conseils accessibles au plus grand nombre.

Dans ce domaine, Cybermalveillance.gouv.fr propose gratuitement sur son site de nombreux supports pédagogiques originaux et sous différents formats destinés à toutes les catégories de publics, tels des fiches pratiques pour apprendre les gestes essentiels pour se sécuriser ou réagir face à un incident, mais aussi des vidéos didactiques, des infographies...

Le dispositif est également très présent sur les réseaux sociaux (Facebook, Twitter, LinkedIn, Youtube, Dailymotion), qu'il utilise pour faire connaître ses actions, ses productions, et également pour alerter les populations lorsqu'il détecte de nouvelles menaces d'ampleur.

Des campagnes de sensibilisation sont également menées que ce soit dans le cadre de partenariats ciblés ou même par la réalisation de spots télévisés, à l'instar de celles conduites depuis 2018 sur les chaînes du groupe France Télévisions avec notre partenaire l'Institut National de la Consommation .



Cybermalveillance.gouv.fr a également de nombreuses initiatives pour porter ses messages de prévention au plus près de ses publics en participant chaque année à de nombreuses publications, conférences et salons et ce jusque dans les territoires. A titre d'exemple, Cybermaveillance. gouv.fr participe et soutien le congrès Charente-Maritime Cyber Sécurité (CMCS) depuis sa création en 2018.



ExpertCyber : un label par les professionnels pour les professionnels

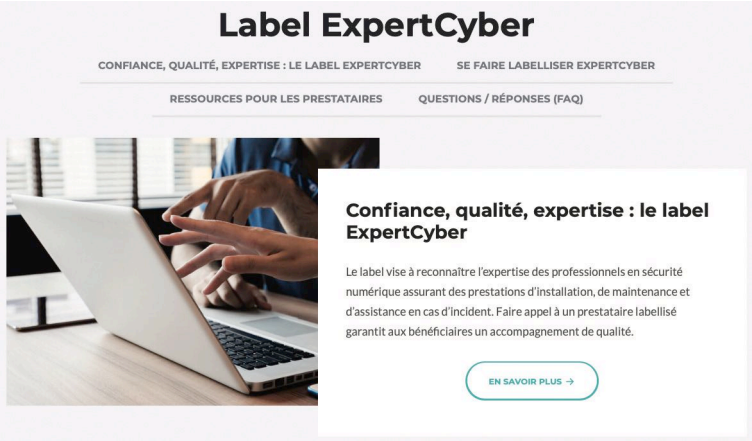
Sécuriser un système ou une infrastructure numérique requiert des compétences spécifiques dont les entreprises, les collectivités ou leurs prestataires de développement et maintenance informatique ne disposent que rarement en interne.

Mais les entreprises et collectivités qui souhaitent se faire accompagner ne savent souvent pas à qui s'adresser en proximité tant l'offre est hétérogène et de qualité variable.

Pour répondre à ce besoin de ses publics professionnels, Cybermalveillance.gouv.fr a créé en 2020, avec le soutien de l'AFNOR et en partenariat avec des organisations professionnelles, le label ExpertCyber. Ce label vise à donner un premier niveau de reconnaissance des compétences des prestataires de cybersécurité dans la sécurisation des systèmes numériques, leur maintien en condition opérationnelle de sécurité et le traitement des incidents.

Le service d'accès à ces prestataires labellisés a été ouvert sur la plateforme Cybermalveillance.gouv.fr dans le cadre des annonces du Président de la république sur la stratégie nationale de cybersécurité de février 2021.

Début septembre 2021, 110 prestataires répartis sur le territoire national ont déjà obtenu le label ExpertCyber et sont en mesure d'accompagner les entreprises et collectivités dans leurs projets de sécurisation de leurs informations et infrastructures numériques.



L'assistance aux victimes

Si la prévention est primordiale, l'assistance aux victimes reste l'objectif premier du dispositif Cybermalveillance.gouv.fr.

Une solution novatrice a été mise en œuvre pour atteindre cet objectif. Au travers de la plateforme sur Internet www.cybermalveillance.gouv.fr, les victimes peuvent décrire leur problème par les effets qu'ils observent, en répondant à une série de questions, jusqu'à arriver sur un diagnostic probable de l'incident qu'elles rencontrent.

Avec ce diagnostic, des conseils de réaction leurs sont fournis pour les aider à remettre en service leur système ou pour les orienter vers les services compétents à contacter, ou encore sur les démarches à entreprendre pour déposer plainte.

Enfin, si l'incident le justifie, les victimes se voient également proposer de pouvoir recourir à des prestataires spécialisés de proximité référencés sur la plateforme et susceptibles de pouvoir leur porter une assistance technique pour résoudre leur problème. À ce jour, Cybermalveillance.gouv.fr référence près de 1 200 prestataires spécialisés sur le territoire national qui peuvent intervenir tant auprès des particuliers que des professionnels en fonction de leur champ d'actions et compétences.

Depuis le lancement du dispositif, ce sont plus de 300 000 personnes, particuliers ou professionnels, qui sont venus ainsi chercher de l'assistance sur la plateforme Cybermalveillance.gouv.fr et l'outil de diagnostic et d'assistance en ligne couvre 50 formes différentes de cybermalveillances.

Un poste d'observation privilégié de la menace

L'assistance aux victimes apportée par le dispositif Cybermalveillance.gouv.fr est un capteur unique d'informations sur la réalité de la cybermalveillance qui va bien au-delà des informations jusqu'alors recueillies au titre des dépôts de plainte. En effet, sur les actes de cybercriminalité peu de victimes déposent plainte, que ce soit par ignorance ou parce qu'elles estiment que le préjudice est trop faible pour se lancer dans une telle procédure. Sans compter que bien souvent, elles se sentent un peu honteuses de s'être faites berner et peinent à aller l'avouer aux forces de l'ordre.

Cette observation permet au dispositif d'adapter rapidement son offre d'assistance et de sensibilisation pour pouvoir répondre aux préoccupations des victimes frappées par les nouveaux phénomènes cybercriminels.

L'observation de la menace permet également au dispositif de détecter des phénomènes de masse émergents, comme l'exploitation d'une nouvelle faille de sécurité ou de nouveaux modes opératoires cybercriminels, et ainsi d'alerter non seulement les populations, mais également les pouvoirs publics.

Cette collaboration étroite, tant avec le ministère de l'Intérieur que le ministère de la Justice, tous deux membres du dispositif, a permis de voir instruire plusieurs affaires qui ont déjà pu déboucher sur l'interpellation de cybercriminels. ■

Cybermalveillance.gouv.fr en chiffres :

- 1,2 millions de visiteurs en 2020
- 105 000 recherches d'assistance
- 1 200 prestataires référencés
- 110 prestataires labellisés ExpertCyber

CROE, le guide pour la cyber-résilience du monde de la finance.

Auteur : Yahya ARROUBAT

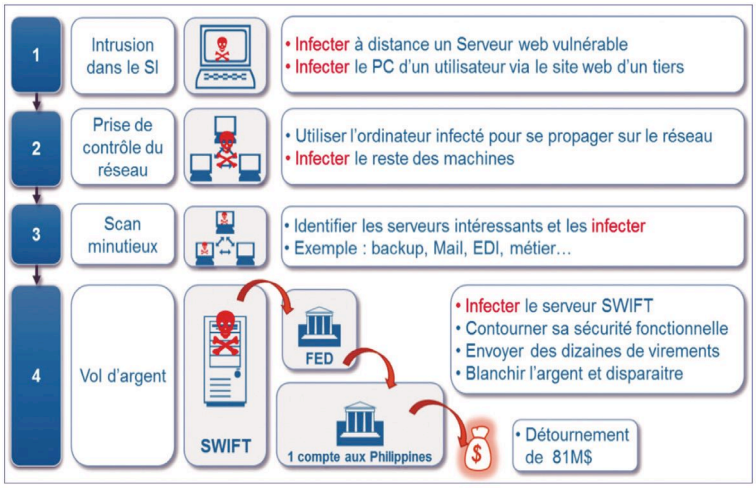
Une Cyber menace grandissante

Les fournisseurs des technologies de l'information ne cessent d'innover pour produire des biens et services aussi simples qu'évolués, offrant ainsi de nouvelles opportunités aux individus et organisations. Cependant, les systèmes d'information de plus en plus ouverts et hyper connectés peuvent présenter des vulnérabilités les exposant ainsi à des menaces de cyber-attaques. La gestion de ce risque est tout aussi vitale que l'adoption des bonnes pratiques en cyber-sécurité, encadrées de près par une cybergouvernance adéquate.

D'année en année nous constatons la sophistication grandissante des cyber-attaques.

A titre d'exemple, le dernier rapport de l'ENISA sur le panorama des cyber-menaces[1], révèle faits et chiffres à l'appui, plusieurs cas de cyber attaques perpétrées entre janvier 2019 et avril 2020. Cette publication classe la Finance au quatrième rang des secteurs d'activité les plus ciblés par la cybercriminalité.

Autre exemple plus spécifique au secteur financier, est le spectaculaire cyber-détournement d'une somme de 81 millions de dollars US, perpétré



Reconstitution à partir des sources Bankinfosecurity.com, Kaspersky.com, latribune.fr

BIO

Yahya ARROUBAT est responsable de département au sein de Bourse de Casablanca, en charge de la sécurité de l'information et de la continuité d'activité. A ce titre, il a réalisé la mise en place des systèmes de management de la sécurité de l'information (SMSI) et de la continuité d'activité (SMCA) et leur certification conforme aux normes ISO, respectivement 27001 et 22301. Au cours de son passage par la DSI, il avait piloté plusieurs projets d'infrastructure IT, dont la mise en place du management de services selon ITIL et la réalisation du premier réseau national boursier. Sur le plan associatif, il est membre de l'AUSIM (Association des Utilisateurs des Systèmes d'Information au Maroc) où il contribue activement au sein du club #AUSMOSE Sécurité. Il est également membre actif du BCI North & West Africa Community, bientôt chapitre régional du Business Continuity Institute.Yahya ARROUBAT est détenteur d'un Master en systèmes d'information, et de plusieurs certifications internationales.
Il a commencé sa carrière dans l'enseignement informatique, puis une SS2I avant de rejoindre Bourse de Casablanca. Il est l'auteur du livre blanc intitulé "DNSSI, Conformité avec le Décret 02-15-712. Apport de la Norme internationale ISO 27001".

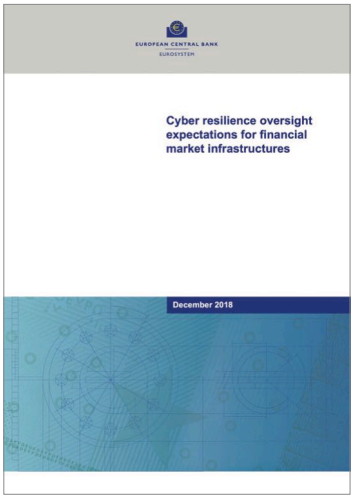
en 2016 contre la banque centrale du Bangladesh. La figure ci-dessous, reconstitue les étapes du vol préparé en sept mois, sans que l'institution concernée ne s'en rende compte. A chaque phase correspondait un scénario minutieusement préparé. Les malfaiteurs ont su mettre à leur profit le social engineering, le scan, l'exploitation des failles logicielles et le développement de scripts spécifiques à chacun des systèmes traversés.

La Cyber résilience

Les situations évoquées plus haut peuvent toucher tout organisme sans prévenir. D'où l'intérêt d'admettre la possible survenance, à tout instant, d'un cyber incident majeur. La préparation et la réponse à de telles situations ne fait pas seulement appel aux compétences en cyber sécurité et en continuité d'activité. Elle fait appel également aux autres fonctions et entités de l'organisme pour que ce dernier puisse se relever rapidement et être résilient aux évènements perturbateurs.

Les autorités de régulation du secteur financier et les organisations internationales auxquelles elles sont affiliées accordent une grande importance à la cyber résilience car elle constitue un réel enjeu de stabilité financière. A ce titre, la banque centrale européenne avait élaboré un guide connu sous le nom de CROE.

Le guide CROE



En 2018, la Banque Centrale Européenne avait publié le guide intitulé ***"Cyber resilience oversight expectations for financial market infrastructures"*** (CROE[2]). Ce document sera plus tard adopté par les banques centrales en tant que guide de référence pour la Cyber résilience des IMF.

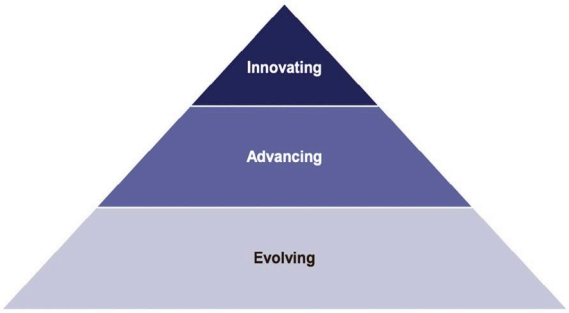
Le CROE est basé sur les Principes pour les infrastructures des marchés financiers (PFMI[3]) ainsi que sur le document Guidance on cyber resilience for FMIs[4]. Ceci pour garantir un ensemble complet et cohérent d'attentes. En outre, lors de son élaboration, les auteurs ont également pris en compte les documents d'orientation et les cadres internationaux existants (Le cadre de cyber sécurité du NIST[5] ; ISO/IEC 27002[6] ; COBIT 5 ; La norme de bonnes pratiques de l'ISF pour la sécurité de l'information et l'outil d'évaluation de la cyber-sécurité du FFIEC).

Bien que les IMF puissent utiliser des modèles de maturité d'autres normes et cadres internationaux à leurs fins internes, les niveaux d'attente définis dans le CROE fournissent aux autorités de contrôle la référence pour déterminer les capacités de cyber-résilience de leurs IMF par rapport au Guide.

Le guide CROE vise trois objectifs :

- Fournir aux IMF des actions détaillées pour opérationnaliser les orientations, et pour assurer l'amélioration continue de la cyber-résilience.
- Fournir aux régulateurs des attentes claires pour évaluer les IMF qui leurs sont assujetties.
- Fournir la base d'une discussion significative entre les IMF et leurs autorités de contrôle respectives.

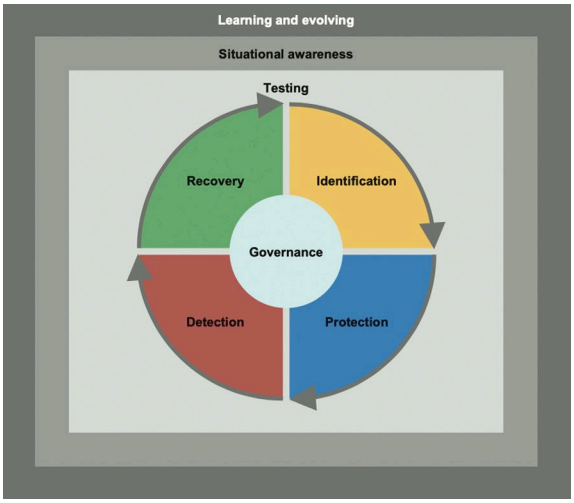
Le CROE décrit trois niveaux de maturité :



Les trois niveau de maturité du CROE

- Evolving : des capacités essentielles sont établies, évoluent et sont maintenues dans l'ensemble de la IMF pour identifier, gérer et atténuer les cyber-risques, conformément à la stratégie et au cadre de cyber-résilience approuvés par le Conseil d'administration. La performance de ces pratiques est surveillée et gérée
- Advancing : l'IMF doit être *Evolving* et mettre en œuvre des outils plus avancés qui sont intégrés dans tous les secteurs d'activité de l'IMF et ont été améliorés au fil du temps pour gérer de manière proactive les cyber-risques posés à l'IMF.
- Innovating : l'IMF doit être Advancing et ses capacités renforcées selon les besoins dans un contexte de cyber-menaces en évolution rapide, afin de renforcer la cyber-résilience de l'IMF et son écosystème tout en collaborant de manière proactive avec ses parties prenantes externes.

Les points de contrôle du CROE sont au nombre de 289, répartis dans le tableau ci-dessous, par domaine et niveau de maturité.



Les huit domaines du CROE

	Nombre d'attentes par niveau de maturité			
Domaines du CROE	Evolving	Advancing	Innovating	Total
Governance	25	13	8	46
Identification	7	4	2	13
Protection	43	21	11	75
Detection	11	8	3	22
Response and recovery	29	14	11	54
Testing	20	12	10	42
Situational awareness	13	7	4	24
Learning and evolving	7	5	1	13
Total	155	84	50	289

Répartition des attentes du CROE

A titre d'exemple, la première attente du domaine de la gouvernance, indique que *"L'IMF devrait établir un comité de pilotage interne et interdisciplinaire composé de la direction générale et du personnel approprié (employés et/ou sous-traitants) de plusieurs unités opérationnelles (finances, gestion des risques, audit interne, opérations, cyber-sécurité, technologies de l'information, communication, ressources juridiques et humaines, dont certaines peuvent être externes), pour développer collectivement une stratégie et un cadre de cyber résilience."*

Démarche de mise en conformité avec le CROE

Le guide CROE est assez consistant et son opérationnalisation ne devrait pas être l'action unilatérale d'une personne ou d'un département.

La mise en œuvre de ce type de référentiels requiert la mobilisation de ressources internes et, s'il le faut, externes. Une enveloppe budgétaire est également nécessaire pour permettre l'acquisition de biens (matériels, logiciels…) et de services (formation, recrutement…). En conséquence, l'appui de la Direction Générale et le soutien du Conseil d'administration sont absolument nécessaires. D'autant plus, ces deux dernières sont nommément désignées parties prenantes clé dès le premier domaine du CROE, spécialement dédié à la gouvernance.

Une première étape consiste à former une équipe pluridisciplinaire qui serait le noyau dure de l'équipe



du projet de mise en œuvre du CROE. Sa mission, serait de comprendre ce guide et d'élaborer un questionnaire d'autoévaluation, afin de déterminer les écarts à combler pour se conformer au niveau de maturité cible "Evolving", "Advancing" et pourquoi pas "Innovating".

En deuxième lieu, identifier pour chaque unité fonctionnelle, les interlocuteurs à interviewer lors de l'autoévaluation. Ces personnes devront être briefées sur l'objectif de l'autoévaluation avant de procéder à la collecte des données, leur analyse et la restitution.

Il faut préciser que l'existence au préalable d'un cadre de référence, relatif à la cyber sécurité ou à la continuité d'activité, qu'il soit issu d'une norme ou d'une réglementation, serait un atout majeur et ferait gagner un temps précieux.

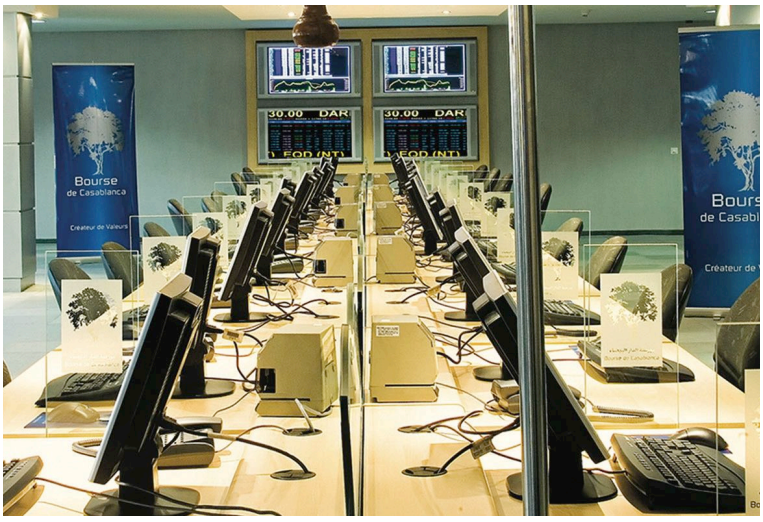
En dernier lieu viendra l'élaboration d'une feuille de route de mise en conformité, visant à combler les écarts identifiés par rapport au niveau de maturité ciblé, généralement exigé par une banque centrale ou tout autre organisme de supervision des IMF.

Gérer cette feuille de route en mode programme serait un facteur clé de succès. La bonne pratique serait d'aller doucement mais surement et surtout de s'autoévaluer périodiquement (par exemple chaque année).



Quel impact sur la Bourse de Casablanca ?

L'IMF Bourse de Casablanca est la société gestionnaire de la Bourse des valeurs. Sa mission est d'assurer le fonctionnement, le développement et la promotion du marché boursier marocain.



La Bourse de Casablanca dispose d'un SMSI certifié conforme à la norme ISO 27001, depuis 2014 et d'un SMCA certifié conforme à la norme ISO 22301 depuis 2018.

Compte tenu de ses activités, la Bourse de Casablanca est soumise à plusieurs autorités de régulation dont celle de Bank Al-Maghrib[7]. Cette dernière avait organisé, début 2020, un atelier pour présenter le guide CROE, sa genèse et un survol de ses composants et avait exigé de s'autoévaluer selon ce référentiel.

Après une première autoévaluation, en 2020, de son dispositif de cyber résilience selon la démarche précitée, une restitution a été faite aux différents responsables, membres de la Direction Générale et représentants du Conseil d'Administration.

L'équipe de projet a ensuite proposé une feuille de route conforme aux exigences de la banque centrale. Il s'agit de la mise en conformité totale avec le niveau "Evolving", en 2021, pour ensuite entamer la seconde tranche relative au niveau "Advancing", en 2022.

En conclusion

Le guide CROE est une mine d'or pour les institutions financières. Ses attentes permettront sans doute d'anticiper les incidents de cyber-sécurité et surtout aideront les institutions à se relever dans les délais convenus, suite à une cyber-attaque.

Pour en savoir plus

Abréviations

- BIS : Bank for International Settlements (www.bis.org)
- COBIT : Control Objectives for Information and related technology (www.isaca.org)
- CPSS : Committee on Payment and Settlement Systems
- CROE : Cyber resilience oversight expectations for financial market infrastructures
- ENISA : L'Agence de l'Union européenne pour la cyber sécurité (www.enisa.europa.eu)
- FFIEC : Federal Financial Institutions Examination Council (www.ffiec.gov)
- FSB : Financial stability board (www.fsb.org)
- IEC : Commission électrotechnique internationale (www.iec.ch)
- IMF : Infrastructure du marché financier (financialmarket infrastructures)
- ISO : Organisation Internationale de Normalisation (www.iso.org)
- NIST : National Institute of Standards and Technology (www.nist.gov)
- OICV-IOSCO : International Organization of securities commissions (www.iosco.org)
- SMCA : Système de management de la continuité d'activité
- SMSI : Système de management de la sécurité de l'information
- ISF : Information Security Forum (www.securityforum.org)



Définitions

Afin de faciliter la coordination et la communication internationales, le FSB a développé un Cyber Lexique[8], qui définit entre autres les termes cybernétiques suivants :

- **Cyber :** se rapportant à, au sein ou par le biais des informations interconnectées infrastructure d'interactions entre les personnes, les processus, les données et les systèmes d'information.
- **Cyber-événement :** Tout événement observable dans un système d'information. Les cyber-événements peuvent parfois indiquer qu'un cyber incident est en train de se produire.
- **Cyber-incident :** un événement informatique qui:
  - Met en péril la cyber sécurité d'un système d'information ou des informations du système traite, stocke ou transmet ou bien;
  - Viole les politiques de sécurité, les procédures de sécurité ou les politiques d'utilisation acceptable, qu'elles d'une activité malveillante ou non.
- **Cyber-risque :** La combinaison de la probabilité d'occurrence des cyber-incidents et de leur impact.
- **Cyber-résilience :** La capacité d'une organisation à continuer à remplir sa mission en anticiper et s'adapter aux cyber menaces et autres changements pertinents dans l'environnement et en résistant, en contenant et en se rétablissant rapidement des cyber-incidents.
- **Cyber-sécurité :** Préservation de la confidentialité, de l'intégrité et de la disponibilité des informations et/ou systèmes d'information par le biais du cyber média. De plus, d'autres propriétés, telles que l'authenticité, la responsabilité, la non-répudiation et la fiabilité peuvent également être impliquées.

Résférences

1 ENISA, Threat Landscape 2020 - Main Incidents [www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents], 20/10/2020

2 BCE, Cyber resilience oversight expectations for financial market infrastructures [www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf], 29/11/2018

3 CPSS-IOSCO (Avril 2012), Principles for financial market infrastructures, [www.bis.org/cpmi/publ/d101a.pdf],

4 CPMI-IOSCO (June 2016), "Guidance on cyber resilience for financial market infrastructures", [www.bis.org/cpmi/publ/d146.pdf]

5 NIST, Cybersecurity framework [www.nist.gov/cyberframework]

6 ISO/IEC 27002, Code de bonne pratique pour le management de la sécurité de l'information [www.iso.org/fr/standard/54533.html], Octobre 2013

7 Bank Al-Magnrib, Banque centrale du Maroc [www.bkam.gov.ma]

8 Lexique du FSB [www.fsb.org/wp-content/uploads/P121118-1.pdf], 12/11/2018 ■

L'industrie numérique au cœur de la PFUE.



Auteur : Sébastien GARNAULT

BIO

Diplômé de Sciences-Po Rennes et de l'Université Paris-II Panthéon-Assas en 2009, Sébastien Garnault débute sa carrière au Secrétariat général des Affaires européennes (SGAE - Premier ministre). À la suite d'un passage au Parlement européen en 2010, il intègre la même année le cabinet de lobbying Boury & Associés en tant que chargé d'études. En 2012, il prend la direction de la filiale M&M Conseil, puis devient associé de Boury, Tallon & Associés en 2013. Parallèlement, Sébastien Garnault lance TPG Communication avec Raymond Soubie. La société est spécialisée dans la mobilisation de très hautes personnalités. À l'issu d'un voyage d'un an en Afrique en 2015, il créé sa société en 2016. Première agence événementielle en conseil stratégique dédiée à la transformation numérique, à la tech et au cyberespace, il lance la même année la CyberTaskForce afin de renforcer les liens entre les experts et les décideurs pour participer à l'accélération de la prise de conscience et la montée en compétence sur ces défis. En 2018, Sebastien Garnault organise pour la France la première Cyber Defence Pledge Conférence de l'OTAN. Il lance en 2019 la Paris Cyber Week, qui rassemble les principaux décideurs européens de haut niveau issus du public et du privé autour des grands défis de la transformation numérique sécurisée. En 2020, Sébastien Garnault lance avec 8 jeunes européens European Cyber Young Leaders.

Sortant peu à peu de la sidération créée par la crise sanitaire, les États européens peinent à retrouver une dynamique commune. L'Union européenne cède aux sirènes du compromis permanent pendant que d'autres, à l'Est comme à l'Ouest, se recentrent sur leur résilience au siècle passé, sur leur mutation face aux nouveaux enjeux et sur leur défense face aux nouvelles menaces.

Un contexte international bouleversé

Pour la plupart des jeunes adultes, la situation internationale est éternelle et figée. Et pour ceux des nés dans les années 80, elle est même immuable. De toute leur existence, les digital native n'ont connu qu'un Occident tout puissant, mené par des États-Unis triomphant. Pourtant, bercés par le progrès et nourris au numérique, ces jeunes quadras découvrent la partie immergée de l'iceberg qui se dévoile peu à peu à mesure que la supériorité occidentale s'estompe. Aucune guerre ne les a touchés, aucun conflit d'ampleur n'est venu bouleverser leur quotidien, moins encore à les rationner, à ce point tel que l'épidémie de COVID 19 est devenu leur guerre, leur crise mondiale, leur drame et finalement leur aliénation. Qu'en sera-t-il du prochain virus s'il devient mortel pour 30% de la population comme le fut en son temps la variole, qui ne triait pas en fonction de l'âge et de l'état de santé pour mettre un terme aux espoirs de ceux qu'elle infectait ?

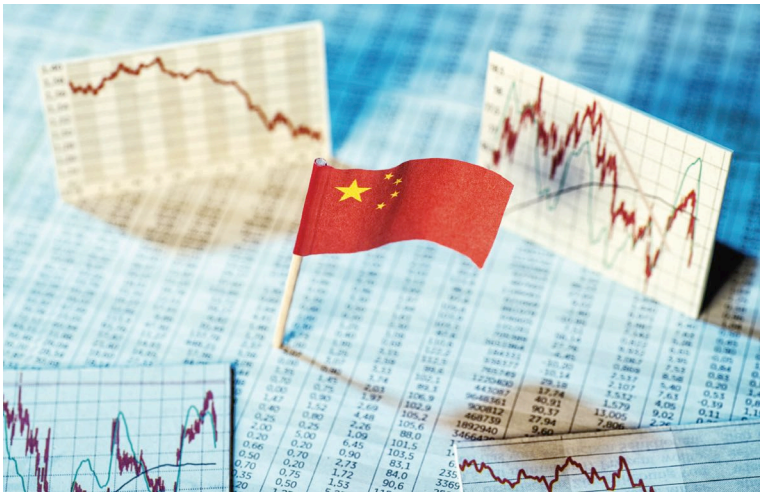
Même les conséquences de la crise financière de 2008 leur semblent vaporeuses. Lorsqu'éclate la crise des subprimes et que Lehman Brothers ferme ses portes, les conséquences mondiales de ce que l'on appelle alors la sphère financière restaient impalpables, ne permettant pas une prise de conscience des conséquences concrètes des interdépendances entre États et des enjeux géopolitiques qui, quelques années plus tard, se révèleraient autrement plus précis. "Plus jamais ça", qu'ils disaient, et tout reprit comme avant.

La crise ukrainienne a d'ailleurs démontré que la guerre telle que nous l'avions toujours connue reste possible et que, sans défense, sans maitrise,



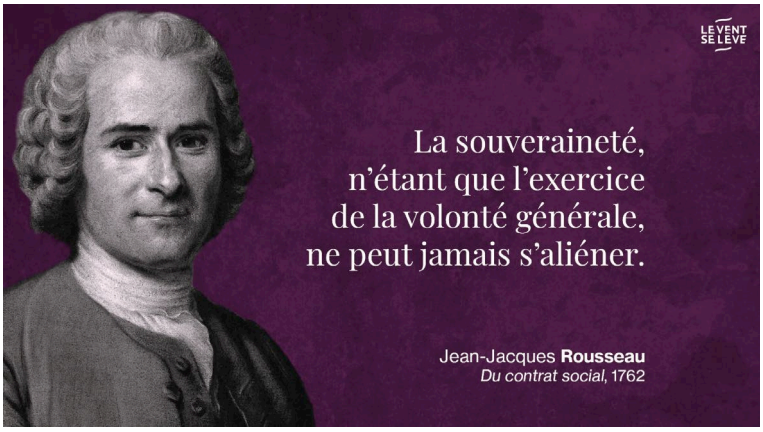
sans alliés économiques, l'on pouvait encore être soumis. L'incursion russe démontre s'il en faut que la conquête des territoires ne s'est pas terminée en 1945. Elle est en pause dans le monde physique, et dans le monde occidental.

Toutefois, la crise sanitaire a permis une nouveauté. Une puissance s'est réveillée. Mise au jour, elle s'impose à mesure que sa puissance militaire augmente. Au cœur du sujet et au centre du jeu, l'Empire du milieu s'est révélé à la fois leader, modèle et arbitre de monde d'après. Le nouvel ennemi est né. Pourtant, dès l'élection de Barack Obama, les USA avaient annoncé cette naissance en réservant le premier déplacement officiel à ce qui était encore l'usine du monde. Des millions qui ont été injectés dans le commerce mondial, c'est la Chine qui en a constitué le tiroir-caisse. Les premiers millions pour les masques, les deuxièmes pour les matières premières, les suivants pour les produits pharmaceutiques. Et la situation est apparue, nous n'avons plus industrie, nous ne produisons plus.



En France, c'est l'idée de souveraineté qui s'émancipe alors, sans qu'elle ne soit associée au nationalisme, cette fois. Malgré tout, l'on arrive encore à la démembrer : souveraineté sanitaire, souveraineté économique, souveraineté industrielle, … Traitant en silo ce qui est un tout. Il n'y a qu'une souveraineté, et elle s'applique à l'espace cynétique comme cybernétique.

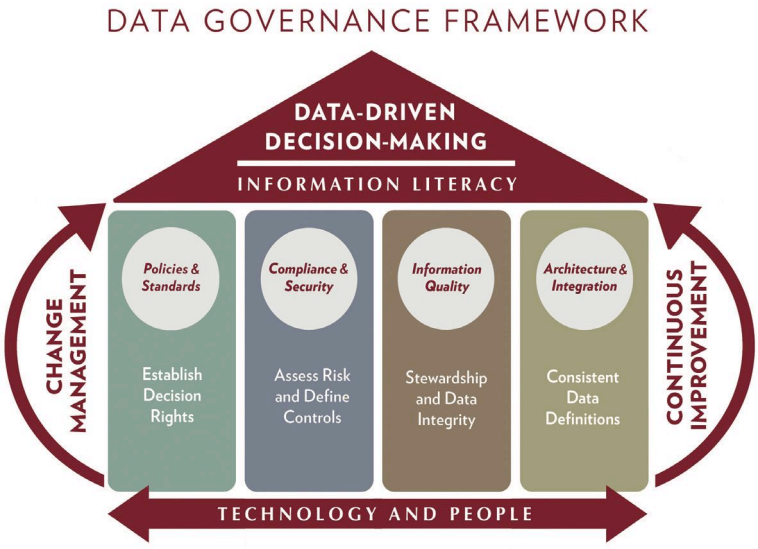
Et les Européens commencent à comprendre, regardant vers le "grand frère" américain qui tourne le dos. Cette approche segmentée empêche une approche holistique des défis industriels qui se posent à nous, numériques en tête. Les États-Unis, quant à eux, jouent leur avenir et regardent, avant tout, leurs intérêts dans notre monde de la réalité augmentée et de la vérité alternative.



La tectonique des plaques cyber

Qui pourrait les blâmer. Protéger ses intérêts est à la fois le rôle et le moteur des Nations. Rien de nouveaux sous le soleil. Mais du côté obscur, celui du cyberespace que l'on ne voit pas, les frontières n'existent pas, ou pas encore. Alors l'esprit de conquête remis au goût du jour en France est total. Fièrement affiché, nous allons reprendre ce que nous avons cédé jadis. Pourtant, le cyberespace est à la fois la scène de l'innovation de la révolution industrielle en cours, le théâtre d'opérations de la transformation des États et le nouveau Monde des Citoyens. Il s'agit, surtout, d'un espace philosophique, où se mêlent idéologies, intérêts, Libertés, duperies et menaces. Pour le France, c'est aussi l'occasion d'y projeter les Lumières. Mais les moyens manquent, et nous venons d'engager des sommes astronomiques pour un rendement inexistant.

"La guerre numérique a bel et bien commencé", rappelait dès 2019 la ministre française des Armées **Florence Parly** et l'enjeu, c'est un nouveau partage du Monde. Cette tectonique des plaques cyber laisse entrevoir les grands axes des rapports de forces du 21e siècle entre des superpuissances qui visent le gouvernement du cyberespace et des États qui recherchent le parapluie de ces nouveaux champions, comme le rappelle souvent **Guillaume Poupard**, directeur général de l'ANSSI. D'ailleurs, cybernétique vient du grec et signifie "Gouverner". Le gouvernement des systèmes d'information, voici le défi et le graal du rapport de force.



Avec l'arrivée des États, chacune des plaques a donc son territoire, sa Loi et ses géants, sauf l'Europe. Que se passera-t-il en cas de conflit majeur ? Ces géants qui s'installent et gagnent nos marchés seront-ils des outils au service des clients ou une industrie en guerre ? Bien sûr, les géants du numérique peuvent rester non-alignés en temps de Paix, et sont probablement de bonne foi. Mais ce ne sera pas le cas si un conflit ouvert s'ouvre, et il s'annonce.

D'ailleurs, lors de la dernière Paris Cyber Week, GRTGaz a livré un témoignage édifiant : Donald Trump a demandé à l'industrie numérique de conserver la pleine capacité du service aux entreprises américaines. Il n'était pourtant question que de virus. Alors en période de conflit armés. Voilà pourquoi l'Europe doit se prendre en main et investir dans son industrie numérique. La



coopération publique-privée est la clef du rapport de force qui s'établit désormais.



La France peut proposer une voie pour faire avancer le continent vers l'indépendance qu'il connait depuis maintenant plusieurs siècles. Poser les pierres d'un édifice commun pour se défendre ensemble dans le 21e siècle, le défi est de taille. L'Europe peut se défendre, encore faut-il qu'elle le veuille et que les États membres s'y engagent. Voici selon moi tout l'enjeu de la présidence française de l'Union européenne qui démarre le 1er janvier 2022. Le temps passe. ■

L'antivirus ne vous protège pas. Il laisse des fichiers vous infecter. Du nouveau dans le paysage français : Viruscamp.



viruscamp

Viruscamp améliore la prévention et la veille des menaces pour permettre aux organisations de prioriser leurs actions correctives et leurs investissements. Les nombreuses données collectées sur l'activité des antivirus activés et les sources de menaces sont les aides à la décision qui manquent encore, dans un secteur en surchauffe.

Auteur : Stéphane THOREL

Multiplier les défenses pour faire face à la menace grandissante sur les SI et accompagner les nouveaux usages nous permet de sécuriser la transition digitale dont notre économie s'éprend. Viruscamp est le fruit de nos développements les plus ambitieux pour les secteurs Banque et Assurance. Aujourd'hui donner accès pour tous les acteurs publics et privés à une solution novatrice, performante et souveraine est notre mission principale.

Il est nécessaire de faire évoluer la protection des systèmes d'information.

Il n'est plus possible d'évoluer dans des environnements fermés. Tous les échanges devenus numériques repoussent le concept de périmètre sécurisé et intègre. Les usages informatiques ont considérablement évolué. Encore récemment, la pandémie mondiale a accéléré les menaces sur les identités et les données échangées en continu. Du cadre personnel au professionnel, du lieu de travail au jardin de pavillon, du réseau d'entreprise au wifi public, tous les usages vont vers une même direction :



perte de maîtrise du réseau et besoin de mettre en place de nouveaux contrôles.

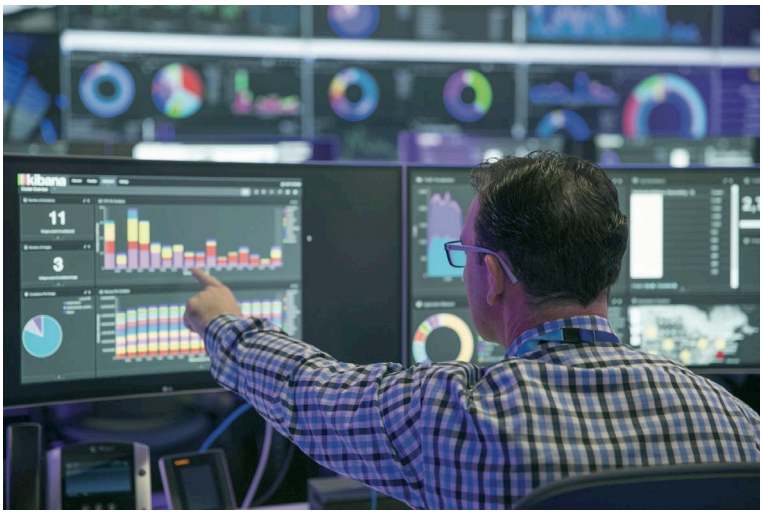
"Le modèle Zero Trust, basé sur le principe que l'ensemble du réseau et de ses intermédiaires ne sont pas fiables, définit le concept du *"divide and rule"* (diviser pour régner). Partant de ce constat, il faut apporter de meilleures réponses à la surveillance et la protection de tous les flux de données et les traitements numériques".

Détecter toujours plus efficacement les sources d'une menace est primordial.

Plusieurs stratégies et organisations sont mises en place pour renforcer l'ensemble des outils, interfaces, procédures et systèmes. Elles sont définies

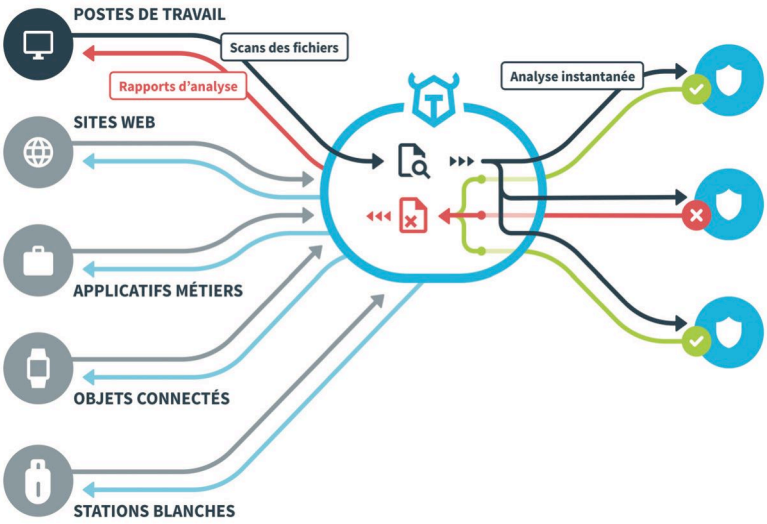
dans le but de prévenir, détecter ou manager les menaces. Les pare-feux de nouvelle génération, proxy anonymes, antivirus et anti-spam résument les solutions proposées, associées à des procédures systématiques de sauvegardes ou réplications des données dans le cadre d'un plan de continuité. Les antivirus dits comportementaux sont plébiscités ces dernières années dans la détection de scénarii complexes.

Viruscamp agit dès la soumission d'une menace. Les technologies employées permettent de travailler en rupture de flux sur tout type de données entrantes dans l'organisation puis circulant ou en repartant. La solution prévient l'arrivée et la prolifération d'une menace par fichiers ou données corrompues. Le fichier est le plus souvent introduit bien en amont de l'exécution d'une menace. Il est celui qui va générer ou profiter d'une faille à venir.



Avec Viruscamp l'analyse en continu et temps réel des flux de données et fichiers est assurée par une plateforme révolutionnaire mettant en commun toutes les compétences d'antivirus du marché. Vous choisissez plusieurs acteurs, que nous nous chargeons de mettre sur une même ligne de défense et ainsi nous multiplions la pertinence et l'efficacité de la détection de virus.

Fini le dilemme de choisir le meilleur antivirus : nous avons développé une plateforme qui permet de tirer parti de l'ensemble des acteurs.



BIO

Stéphane est Directeur du développement et des partenariats pour Biig et Viruscamp. Expert des nouveaux usages digitaux, il rejoint plusieurs acteurs majeurs du digital en qualité de Directeur des stratégies auprès de grands comptes. Il tire parti de ses expériences des contextes créatifs, techniques et décisionnels pour accompagner le développement de Biig qui édite Viruscamp. Précédemment directeur de programmes pour des ministères et pour le privé, il s'engage aujourd'hui pour distribuer une solution novatrice et promouvoir une cybersécurité souveraine. Soutenir le développement de nouveaux services et manager les organisations pour y parvenir sont ses motivations principales. C'est pour cela qu'il est en dialogue pour Viruscamp, avec les institutionnels, clients et partenaires du secteur. Il rend compte des enjeux utilisateurs à l'équipe produit menée par Manuel Barraud DSI et concepteur de la solution.

La concurrence américaine ne satisfait pas aux exigences de souveraineté et de respect de la RGPD. C'est parce que nous sommes sensibles à la protection et l'intégrité de traitement de vos données que nous proposons notre solution à toutes les Entreprises publiques et privées. Chacune dispose d'une offre adaptée et accessible pour répondre à ses enjeux.

L'idée acceptée que nous challengeons.

Concentrer les moyens sur le ralentissement d'une menace active parfois sur le constat du vol de données revient à visionner les vidéos de son cambriolage. L'analyse préventive au moment de l'échange de données permet d'agir sur la diminution des intrusions et exploitations de failles futures. 30% des dispositifs numériques sont corrompus par l'intrusion d'un programme malveillant, dont la fonction est d'attendre le moment de s'exécuter et rompre la chaine de confiance numérique. 32% des vols sont commis par substitution d'identité.

"Vraisemblablement nous conservons tous, à notre insu, un fichier malveillant qui agira demain en notre nom et depuis sur nos propres outils et interfaces."

L'exigence des responsables aujourd'hui et des institutions demain.

Parce que nous construisons un monde ouvert avec des technologie intelligentes et des services



numériques de qualité, l'enjeu de la digitalisation et de la protection de nos échanges sont dans toutes les feuilles de route. La compétitivité et la pertinence des offres dans le monde de l'Entreprise sont à ce prix. La souveraineté des Etats et l'équilibre des forces dans le monde ne peuvent souffrir d'une sécurité faillible ou corrompue. L'Etat Français classe à bon rythme des établissements et administrations OIV et OSE. Il travaille à la création de Hub sectoriel pour la gestion des datas, preuve de l'augmentation des enjeux de sécurité de l'ensemble des flux et données échangé et non plus des enjeux SI. Le temps de la mutualisation et la convergence a cette exigence.

Le "toujours plus sécurisé" dans un monde ouvert pose des défis technologiques et sociétaux de tailles. La défense idéale des systèmes informatiques est une utopie que personne n'atteindra probablement.



MADE IN FRANCE

La solution Viruscamp éditée par Biig

La sécurité informatique est un tel enjeu que notre entreprise a décidé de mobiliser ses savoir-faire pour offrir une alternative face à un acteur américain. Nous nous plaçons en acteur 100% français dans le développement d'une solution d'analyse multi antivirus. Nous mettons à disposition une plateforme compatible avec tous les environnements pour connecter applicatifs, web, mail et matériel station blanche avec les bases signatures les plus performantes. Viruscamp pour tous. Tous les antivirus pour votre sécurité ! ■

Quand le sport abrite le crime : pari sportif en ligne, blanchiment et corruption.



MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Gendarmerie Nationale

Auteur : Stéphane MORTIER

Le pari sportif n'est pas une innovation de notre temps, déjà au 19ème siècle, les courses hippiques étaient le théâtre de paris en tous genres, ce qui finit par donner, en France, le Pari Mutuel Urbain (PMU) toujours célèbre aujourd'hui. La diversification des paris n'a pas tardé et de nos jours, il est possible de miser sur presque tous les types de sports et événements sportifs se déroulant n'importe où dans le monde. Les technologies évoluant, le pari sportif en ligne s'est facilement imposé grâce à Internet. Les enjeux économiques sont énormes. En effet, des centaines de millions (toutes monnaies confondues y compris crypto-monnaies) circulent chaque jour. Le secteur offre en contrepartie des milliers d'emplois et apporte à des millions de parieurs le plaisir de jouer et, éventuellement, de gagner de l'argent.



Le sport, quant à lui, ne se pratique pas en ligne (bien que la tendance à considérer comme un sport la pratique de certains jeux vidéo pourrait remettre en cause ce postulat) mais bien sur un terrain, une route, un circuit, une salle de sport, une piscine,…

Jusqu'ici, tout va bien, des sportifs s'affrontent lors de compétitions, des parieurs tentent leur chance sur un résultat ou un classement espéré...et des spectateurs ont payé un droit d'entrée ou un abonnement pour regarder à distance leur sport favori ! Cela est bel et bien lié et peut connaître certaines dérives.

Premièrement, la législation sur le pari en ligne reste incomplète à travers le monde et une régulation à l'échelle de la planète se fait attendre. Ensuite,

BIO

Docteur en sciences de gestion (Paris 1 Panthéon-Sorbonne), Stéphane est spécialiste de l'intelligence économique et de l'Afrique et à ce titre, il enseigne à l'École de Guerre Économique de Université de Likasi (RDC), où il est Conseiller du Recteur, en sus d'être membre de l'Association pour l'Unification du Droit en Afrique (UNIDA). Il est également membre de la communauté des chercheurs du Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale (CREOGN)

la tentation est grande de vouloir gagner, "à tout prix", lorsqu'on a parié… Mais ça ne s'arrête pas là, pourquoi ne pas utiliser le pari sportif pour abriter une activité de blanchiment d'argent ? Dans un tel cas, le système va s'autoalimenter puisque la corruption va s'immiscer dans la pratique sportive.



En 2005-2006, en Belgique, éclate une affaire de corruption dans le milieu du football : l'affaire Yé ! Dans toutes les sociétés officielles de paris en ligne le respect des législations en vigueur et de codes d'éthiques sont des obligations. Mais des réseaux criminels ont repéré un moyen à exploiter pour blanchir de l'argent. Ces réseaux pratiquent alors la corruption pour influer sur les résultats des match de football en l'occurrence. A partir de 2004, un prétendu investisseur chinois, Zheyun Yé, s'intéresse de près au football belge et approche plusieurs clubs (Beerschot, Mons,…) mais sans succès. Ne voulant pas rester sur un échec, il s'associe à Pietro Allata, un agent de joueurs (soupçonné d'être proche des milieux mafieux). Tous deux arrivent à établir des liens avec deux clubs principaux (Saint-Trond et La Louvière). Des joueurs auraient été corrompus pour jouer "en dessous" de leurs capacités… En d'autres termes, contre rémunération, les matches ont été truqués ! En octobre 2005, Saint-Trond s'incline 1-3 face à La Louvière, ce sera le match de trop ! Il apparaît que de fortes sommes d'argent sont pariées en Asie sur certains matches et les spécialistes constatent des incohérences dans le jeu des joueurs… Les journalistes sportifs, passionnés, se posent de plus en plus de questions et vont découvrir qu'à chaque match "bizarre" correspond une visite de Zheyun Yé ou de Pietro Allata ! Ils iront jusqu'en Chine pour tenter de comprendre et découvriront que Monsieur Yé y est un acteur important du milieu des paris sportifs en ligne et surtout que les parieurs adorent le club belge de La Louvière… A bon entendeur, pariez !

Une enquête sera ouverte en 2006, avec des condamnations de joueurs, de clubs, des intéressés, avec des rebondissements, des appels, des mandats de recherche, des incarcérations,… Mais aussi des rétrogradations en division 2 pour certains clubs. Bref une catastrophe pour le sport et son image.



Ce n'est évidemment pas le fait qu'un match de football puisse être truqué qui nous intéresse ici mais bien que le pari en ligne puisse amener des dérives impactant l'activité et la pratique de la compétition sportive.

Cet exemple du football belge met au jour plusieurs problématiques :

- le blanchiment de l'argent sale se fait au moyen de vecteurs numériques (pari en ligne) ;
- la réussite de l'opération de blanchiment implique la corruption de sportifs ;
- l'argent blanchi est le fruit d'une compétition truquée ;
- les paris en ligne sont réalisés dans une zone où la législation est moins aboutie ;
- la compétition sportive perd de son intérêt…



On évoque souvent la cybersécurité comme étant un ensemble de moyens techniques pour éviter une intrusion dans un système de traitement de données, un vol ou une destruction de données, une prise de contrôle à distance,… Mais il est pourtant impératif de voir au-delà. En effet, la criminalité, qui plus est organisée, utilise le cyberespace pour exercer ses activités, elle l'utilise surtout à la fois comme outil, comme vecteur. Et cet exemple du football belge en est une belle illustration.

Le GAFI propose la définition suivante du blanchiment d'argent :

"De nombreux actes criminels visent à générer des bénéfices pour l'individu ou le groupe qui les commet. Le blanchiment de capitaux consiste à retraiter ces produits d'origine criminelle pour en masquer l'origine illégale. Ce processus revêt une importance essentielle puisqu'il permet au criminel de profiter de ces bénéfices tout en protégeant leur source".

Cela correspond exactement aux problématiques soulevées dans notre exemple. Le pari en ligne consiste à retraiter le fruit d'une activité criminelle (argent sale) et permet au criminel de bénéficier des gains issus de ses paris (argent propre). Le problème réside que pour être certain de gagner, le criminel use de la corruption pour influer sur les résultats de la compétition : le crime appelle le crime. Le processus de blanchiment utilise bien ici un vecteur "cyber" : le pari en ligne !

Au delà des faits de blanchiment, de corruption,...c'est l'image de sport qui est ternie, c'est l'admiration qu'ont les jeunes de leurs idoles sportives qui s'effrite, c'est l'espoir d'une compétition juste qui s'envole, c'est un idéal qui disparaît !



Toutefois, une législation contraignante encadre les paris en ligne et contribue à la lutte contre ce type de dérive. En France, la réglementation a instauré l'autorité nationale des jeux ou ANJ dans un souci de protection des consommateurs. Pour prévenir les risques de fraude, l'ANJ délivre des licences aux opérateurs pour pouvoir proposer leurs prestations en France. Cette licence est soumise à un certain nombre d'obligations comme le plafonnement des sommes engagées, l'auto-exclusion et le versement automatique des gains sur un compte bancaire.

ANJ
AUTORITÉ NATIONALE DES JEUX

Un régulateur au service d'un jeu sûr, intègre et maîtrisé

En Chine, la législation interdit toute forme de jeux d'argent et paris en ligne. Seul un système de loterie géré par le gouvernement central est autorisé. Ce régime ne s'applique toutefois pas à Macao et Hong Kong en raison de leur statut administratif spécial. La règle générale est que pour tout jeu en ligne ou pari en ligne visible sur internet depuis le territoire d'un État, la législation de cet État s'y applique. Les barrières existent donc mais leur contournement est plus ou moins facile (ou facilité) en fonction des situations. En tout état de cause, le meilleur moyen juridique de lutte reste la lutte contre le blanchiment.

Crime organisé, corruption et blanchiment, pari en ligne, sport : une organisation, des activités criminelles, un vecteur, une (ou plutôt des) victime(s). Notre exemple du football belge, et il ne s'agit que d'un exemple parmi d'autres, démontre que dès l'entrée dans le 21ème siècle, la criminalité organisée a su saisir les opportunités que lui offrait le cyberespace. Est-ce là une simple adaptation des modes opératoires aux évolutions technologiques ou est-ce une capacité d'anticipation et une volonté de toujours veiller à se dissimuler derrière un panel de paravents numériques évolutifs et difficilement contrôlables ?

Il était un temps où les mafias contrôlaient un territoire, il en est un autre où elles maîtrisent le cyberespace…



A-t-on enrayé le phénomène sur les territoires physiques ? Pourra-t-on l'enrayer dans le cyberespace ? Telle est la question.

Quant au sport, assistons-y et vivons-le tout simplement, il restera beau et probe… On parie ? ■



Vestiaire : nouvel espace de violence.



Auteur : Tristan IZAMBARD

Qu'est-ce que le harcèlement et le cyber-harcèlement

Le harcèlement est une violence répétée, continue : des insultes, des humiliations, la mise à l'écart, des rumeurs, voire même des coups qui sont infligés de façon répétée sur une longue période, par une personne ou un groupe de personnes à l'égard d'une autre. Les attaques peuvent être verbales, physiques, psychologiques ou numérique. Il faut dire STOP !

Le cyber-harcèlement ou harcèlement numérique se produit de la même manière au travers des téléphones portables, forums, chats, jeux en ligne, réseaux sociaux sous formes d'insultes, rumeurs, commentaires haineux, diffusion de photos et vidéos publiées de façon non consentie par la personne victime et diffusés sur le web par un ou plusieurs internautes, la diffusion est très souvent massive et touche un large public.



Bien que la violence soit virtuelle, celle-ci est tout aussi porteuse de conséquences néfastes pour la victime autant d'un point de vue physique que moral.

Ses fait son punissable par la loi, notamment la Loi du 24 juin 2020 visant à lutter contre les contenus haineux sur internet par la député Laeticia Avia.

On a pu mesurer qu'en moyenne 1 adolescent sur 10 est victime de harcèlement à un moment de sa scolarité, et ceux dès l'école primaire. On harcèle pour montrer une supériorité, pour appartenir à un groupe.

La moquerie est quelque chose d'universel mais pourtant chaque enfant a le droit à une scolarité sans violence, ni moquerie trop abusive. Aider les enfants et adolescents au travers de nos interventions est notre objectif.

La couleur des maux

Visitez notre site! https://www.lacouleurdesmaux.fr

BIO

Tristan Izambard, jeune lycéen âgé de 17 ans à l'époque, a créé en 2019 L'association La Couleur des Maux, dans le but de lutter contre toutes formes de harcèlement scolaire. Ayant pu constater la situation par lui-même sur le terrain et pris conscience des problématiques y étant présentes de manière redondante, il s'est engagé contre le harcèlement dans son établissement scolaire et souhaite désormais pouvoir aider à plus grande échelle et toucher un plus large public. Après avoir commencé à œuvrer à l'échelle locale, il a décidé d'agrandir son horizon d'action à travers La Couleur des Maux pour aider un maximum de personnes étant confrontées au harcèlement. À 19 ans, il dit être bien déterminé à sensibiliser chaque individu de la société, et c'est bien la raison de sa présence au CMCS 2021 : *"le harcèlement n'est pas une fatalité, et encore moins un mythe".*

Comment déceler le harcèlement ou cyber-harcèlement dans le sport

Le sport a toujours, en tout temps et tout lieu, été mis en avant pour sa bienfaisance et ses valeurs, qu'elles soient médicales, éducatives ou sociales. Mais si le sport peut favoriser l'intégration, il peut aussi être un lieu d'exclusion, de discriminations sociales, raciales, sexistes... et lieu de harcèlement.

Souvent, ça commence par un "on n'est pas des tapettes, on est les meilleurs" ce qui vient prétendre que le sportif, qui aspire au dépassement de soi, pourrait être qu'un homme virile ? Voir guerrier ? Le cliché de l'homme fort avec des gros muscles ? Et qu'on pourrait retrouver des catégories d'hommes selon les différences quelle qu'elles soient ?

L'injure en est la première forme de mise à l'écart, qui va générer des souffrances. L'impression d'exclusion va se faire ressentir au travers de "slogans" discriminant comme "allez négro", "plus vite les tapettes", "vous êtes des hommes ou pas"… Parmi tout ça, les questions de genre et d'orientation sexuelle occupent une place toute particulière quant aux formes qu'elles prennent et à la violence par laquelle elles peuvent se traduire.

Le sport doit être vecteur d'égalité et faire transcender les différences afin que tous les êtres humains soient libres et égaux. Il faut que chaque individu qui souhaite pratiquer une activité physique et sportive soit libre de pouvoir le faire partout, quels que soient ses origines, sa couleur de peau, son orientation sexuelle ou son genre, son niveau de pratique…

Une situation de harcèlement ou de cyber-harcèlement met la personne victime en infériorité face à ou aux auteurs porteur des injures, moqueries, mais aussi face au spectateur responsable des likes et partage.

Sur les réseaux, liker c'est harceler ! Quand je clique sur j'aime à la publication, je donne de l'importance au post et montre par la mon soutien à celui-ci.

La personne victime en infériorité va alors avoir une perception dégradée d'elle-même.



Ça va jouer sur son moral (envie suicidaire, perte de l'appétit..) et aussi sur son physique (mutilation, perte de poids…)

Le harcèlement et cyber-harcèlement sont des délits pénaux. La loi dit que ces deux comportements sont des délits sanctionnés pénalement, y compris lorsqu'ils sont commis dans le champ du sport.

"D'une part, en vertu de l'article 222-33-2 du code pénal, le harcèlement moral est un délit puni de deux ans d'emprisonnement et de 30 000 euros d'amende. De plus, cette peine peut être aggravée dans certaines situations.

D'autre part, en vertu de l'article 222-33 du code pénal, le harcèlement sexuel est puni de deux ans d'emprisonnement et de 30 000 euros d'amende. Cette peine peut également être aggravée dans certaines situations, dans lesquelles la sanction pénale est portée à trois ans d'emprisonnement et à 45 000 euros d'amende."

Le cyber-harcèlement lui est assimilé à une forme aggravée de harcèlement moral. Ainsi il est puni par la loi au sens de l'article 222-33-2-2-4 du code pénal. En cas de circonstances aggravantes, il s'agit d'un délit pouvant alors être puni de trois ans d'emprisonnement et de 45 000 euros d'amende." (extrait du site sport.gouv.fr)

De plus, le harcèlement en ligne est puni que les échanges soient publics (sur un forum par exemple) ou privés (entre "amis" sur un réseau social).

Les conséquences juridiques d'un tel comportement sont donc bien réelles dans la mesure où la loi prévoit que le cyber-harcèlement est sous le même régime juridique que le harcèlement.

Comment agir dans le sport ?

Pour agir face au harcèlement et au cyber-harcèlement, il faut accepter d'en parler à une personne de confiance (membres de la famille, professeurs, collègue de travail, médecin traitant…) mais aussi à une structure spécialisée dans le domaine requis et/ou aux autorités compétentes (gendarmerie, police..).

Au vu de la gravité des faits et des conséquences physiques et psychologiques qui peuvent en découdre, il est important que la personne victime puisse parler, librement, de ce qu'elle a vécu. Se libérer afin de sortir de ce cercle vicieux. Le harcèlement n'est pas une fatalité et toute personne victime doit pouvoir arriver à se libérer.

Il s'agit d'une première étape, certes compliquée, mais nécessaire afin de pouvoir faire suivre une démarche de signalement des faits auprès des autorités compétentes en vue d'engager des poursuites, notamment pénales, contre le ou les auteur(s) de ces comportements. ■



Une info-présentation utile, disponible sur : https://cnosf.franceolympique.com/cnosf/actus/4819-prvention-des-violences-sexuelles-dans-le-sport-.html

Sport : Les cybercriminels attaquent même les petits clubs !

Face à la menace, Asklépian propose des accompagnements sur-mesure pour se mettre en conformité avec le RGPD.



Auteur : Fabien FERNANDEZ

Alors que les Français peuvent enfin profiter des grands événements sportifs, il y a un sujet dont on parle encore trop peu dans l'univers du sport : la data.

Pourtant, elle est partout ! Même les plus petits clubs se retrouvent à gérer des données sensibles avec les adhésions, les licences et les certificats médicaux.

A l'heure du "tout-numérique", la dématérialisation est devenue la règle. Toutes les structures du sport (clubs, comités départementaux, ligues & districts, fédérations, entreprises et écoles du sport, INSEP...) doivent donc protéger les données de leurs salariés et des sportifs, qu'ils soient pratiquants bénévoles ou sportifs de haut niveau.

Ils sont ainsi obligés de se conformer au RGPD, même s'ils n'en ont pas toujours conscience. Nombre d'entre eux s'exposent à des sanctions financières, comme peut en témoigner la Fédération Française d'Athlétisme qui avait eu le tort de rendre certaines données publiques (résultats sportifs) sans en aviser au préalable les principaux concernés.



L'enjeu est d'autant plus important que les outils technologiques, qui permettent de décupler les performances (vidéosurveillance, arbitrage...), sont strictement encadrés. En février dernier, la CNIL a notamment rappelé à l'ordre un club qui expérimentait la reconnaissance facile pour faire respecter l'interdiction commerciale de stade.

Ces contraintes doivent pourtant être vues comme des opportunités : respecter le RGPD, c'est aussi améliorer la sécurité des donnés en cas

"Les enjeux pour les pirates sont multiples : obtenir des bases de données qualifiées, des données sensibles, paralyser des systèmes, des finances... C'est le revers de la médaille. En France, tous les acteurs du sport sont visés, y compris les plus petits clubs, plus vulnérables et donc plus faciles à cibler. Et ce n'est qu'un début ! Il faut s'attendre à de nombreux cyberattaques de masse à l'approche des jeux Paris 2024."



SPORT

Les cybercriminels attaquent même les petits clubs ! Face à la menace, Asklépian propose des accompagnements sur-mesure pour se mettre en conformité avec le RGPD



de cyber-attaques. Or ces dernières se multiplient : l'Agence mondiale antidopage, le Comité olympique international ou le Tribunal arbitral du sport ont déjà été piratés (source), tout comme des confédérations sportives (source), des clubs (AS Saint Etienne, un club de Premier League,...), des entreprises (notamment Go Sport et Courir - source)...

Heureusement, cette situation n'est pas une fatalité ! Afin d'aider toutes les organisations du sport à respecter leurs obligations, Asklépian les accompagne dans leur mise en conformité au RGPD et/ou à l'externalisation des compétences de DPO (délégué à la protection des données).

Le sport, un univers "tout numérique" aux nombreuses failles de sécurité

Asklépian accompagne les structures du sport par l'identification de leur système comme un réel outil de pilotage et d'optimisation. Son objectif : sécuriser les données via la mise en place de solutions techniques, organisationnelles et juridiques.

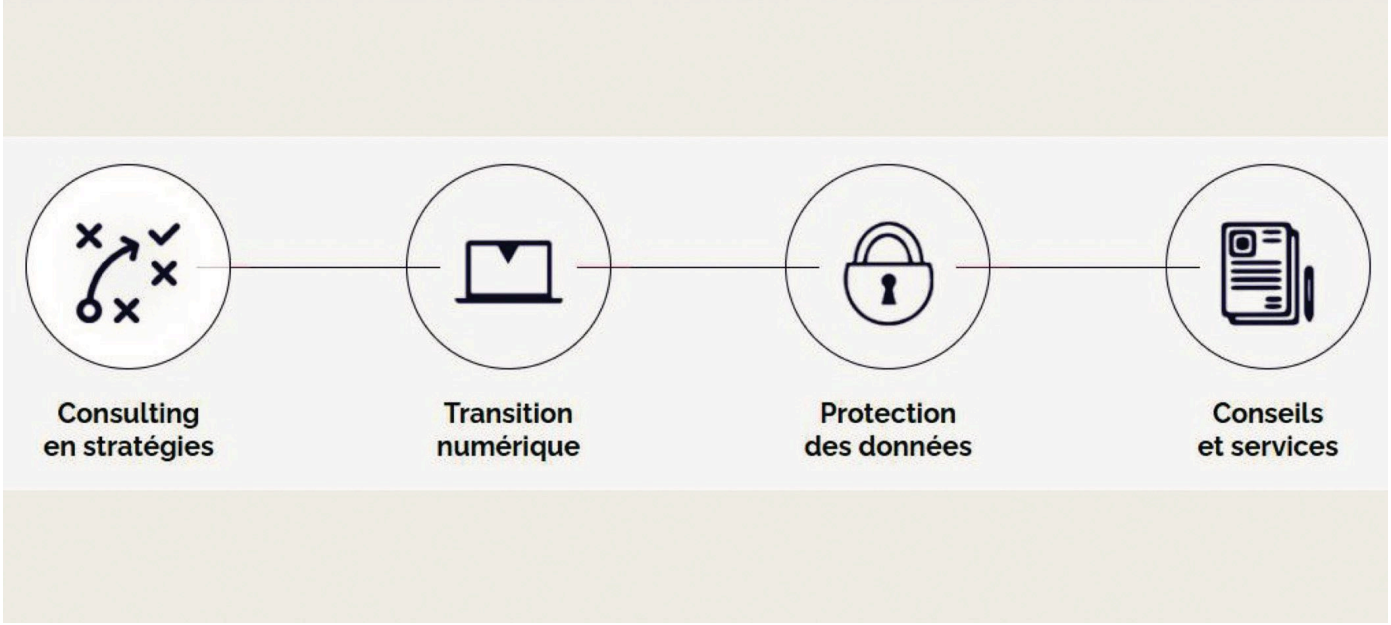
Car en matière de data, de nombreuses questions concrètes se posent :

- Comment cadrer les données sensibles ? Comment sensibiliser les bénévoles et les salariés ?
- Comment protéger les appareils informatiques de bénévoles traitant les données des pratiquants collectées par un club ?
- Comment gérer les responsabilités sur les transferts de données entre les instances d'une fédération ? Ou avant une rencontre sportive ?
- Comment prospecter en respectant les exigences réglementaires ?
- Comment gérer les informations de billettiques et de fidélisation ?

Si des solutions existent, elles sont souvent trop complexes et techniques pour être appliquées sans l'assistance d'un expert qualifié et reconnu. De plus, en cas de cyber attaque, il faut pouvoir redémarrer rapidement et dans les meilleures conditions.

Cela suppose de pouvoir s'appuyer sur une documentation spécifique qui va démontrer que des mesures ont été prises en amont et qu'elles ont été mises en œuvre dans un système maîtrisé.

Asklépian intervient alors pour proposer **un accompagnement sur-mesure grâce à des outils & services adaptés.**



BIO

Fabien Fernandez est un des premiers DPO certifiés sous l'agrément de la CNIL. Il est titulaire d'une licence pluridisciplinaire en Sciences Fondamentales Appliquées de l'Université de Bourgogne avec des surspécialisations en informatique. Fort de dix ans d'expérience dans des fonctions publiques étatiques ou territoriales, Fabien Fernandez a un parcours riche et varié qui lui a donné de solides connaissances de l'organisation administrative de la France dans différents domaines techniques. En 2015, il a accompagné la mise en œuvre de la réforme du collège auprès du corps d'inspection des services déconcentrés de l'Éducation nationale. Fabien Fernandez a également travaillé pendant huit ans auprès de la Fédération Française du Sport Adapté et du Comité Paralympique International, pour les réformes de la réglementation sportive et de la classification des athlètes.En 2018, il a participé à la mise en œuvre de la réforme de décentralisation du stationnement sur l'ensemble de la ville de Bordeaux, accompagnant l'application du RGPD. En 2019, Fabien Fernandez fonde Asklépian. Il souhaite développer également une offre de proximité pour que les TPE puissent aussi avoir l'opportunité de se mettre en conformité tout en étant accompagnées à moindre coûts. En effet, le nombre de cyberattaques contre les TPE/PME explose : les sessions collectives seront alors un outil collaboratif et de partage d'expériences.

Une approche sur-mesure adaptée aux besoins de chacun

Reconnu pour son expertise et son savoir-faire, Asklépian intervient à différents niveaux :

- Mise en conformité RGPD en session individuelle durant 9 mois

Ces sessions, adaptées au planning surchargé des professionnels du sport, peuvent être organisées de façon collective ou individuelle.

Pendant 9 mois, à raison d'un atelier par mois, ils vont ainsi être aidés, guidés, conseillés, relus et corrigés par un délégué à la protection des données certifié.

Ils profitent de :

- 9 séances collectives ou individuelles pour définir leurs objectifs, les trames documentaires et co-construire leur projet de mise en conformité ;
- 9 phases de travail individuel ;
- 9 phases de conseils personnalisés (relecture et correction).

- Mise en conformité RGPD clé en main

Très appréciée, cette prestation permet de n'avoir à se soucier de rien ! Les équipes d'Asklépian vont se charger de tout : elles réalisent tous les audits préalables, toute la documentation, effectuent des recommandations et accompagnent leur mise en œuvre

Durée : de 9 mois à 1 an.

- Externalisation de compétences DPO

Les activités du délégué à la protection des données externalisées consistent à apporter une expertise sur le RGPD :

- Informer et sensibiliser, diffuser une culture " Informatique et Libertés " ;
- Veiller au respect du cadre légal ;
- Informer et responsabiliser, alerter si besoin, son responsable de traitement ;
- Analyser, investiguer, auditer, contrôler ;
- Établir et maintenir une documentation au titre de " l'Accountability " pour documenter toute la conformité ;
- Assurer la médiation avec les salariés et les patients ;
- Interagir avec l'autorité de contrôle ;
- Être le point de contact entre tous les acteurs sur tous les sujets autour de la protection des données (CNIL, responsables, sous-traitants, clients, salariés…) ;
- Accompagner la mise en place de mesures techniques et organisationnelles.
- Sa présence peut notamment permettre d'éviter le prononcé d'une amende ou même d'une astreinte par la CNIL, qui interdirait alors aux professionnels du sport de continuer le traitement des données.

Back-office pour aider à la constitution documentaire

Mise à disposition d'assistants DPO pour la rédaction documentaire au titre de l'Accountability prévue dans la RGPD (documentation avec cartographie interactive, excel, csv et pdf). Le client pilote sa conformité avec l'assistance et l'aide d'une équipe technique dédiée.

Prestations de conseils à la demande

- Préconisations et recommandations pour juger du degré de conformité de l'organisation, mettre en évidence les éventuelles non-conformités (gravité, impacts possibles pour les personnes concernées, origine, responsabilité, etc.), et afin de vérifier le respect du cadre légal ou la bonne application des procédures, méthodes ou consignes relatives à la protection des données personnelles.
- Etudes de cas
- Analyses juridiques et technologiques…

Asklépian, une approche à 360° du RGPD

Asklépian est une référence en matière de sécurité informatique et des réseaux. Ses compétences de Délégué à la protection des données (DPO) sont d'ailleurs certifiées par l'AFNOR selon l'agrément CNIL.

Asklépian est également membre de l'Association Française des Correspondants à la protection des Données à caractère personnel, ce qui lui permet de signer une charte de déontologie afin de promouvoir une culture de l'éthique parmi les DPO désignés auprès de la CNIL au titre du RGPD.

Au plus proche des besoins de ses clients, cette société dynamique dispose notamment d'un logiciel pour la gestion d'un système de management opérationnel des données à caractère personnel contenant l'ensemble des registres RGPD, ainsi que d'un service de communication spécifique.

Un véritable pôle de compétences

Service "Organisationnel"

Les équipes accompagnent à mettre en oeuvre les mesures organisationnelles adéquates et cohérentes dans les organisations pour sécuriser les données à caractère personnel en optimisant les systèmes, mais aussi en définissant, formalisant et simplifiant les procédures.

Service "Juridique"

Il intervient pour sécuriser juridiquement la documentation lors de contractualisation avec des sous-traitants ou de rédactions de mentions d'information, légales ou politiques… Chaque semaine, une veille juridique est également produite en interne pour apporter les meilleurs conseils et un suivi optimisé.

Service "Sécurité des systèmes d'information et Cybersécurité"

La Dream Team propose une stratégie de sécurisation des systèmes d'information (SI), sécuriser les infrastructures, présente et pilote un plan de continuité et de reprise d'activité, audite et identifie des vulnérabilités du SI.

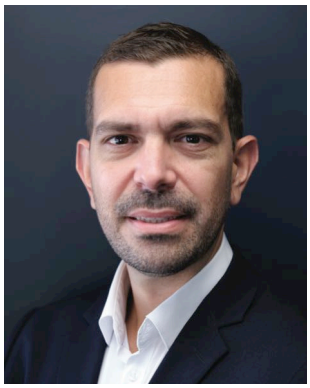
Services "Supports"

Les équipes Asklépian accompagnent la traçabilité du projet de A à Z pour la mise en conformité et/ou d'externalisation des compétences de délégué à la protection des données, assurent le bon déroulement du suivi personnalisé de la relation contractuelle…

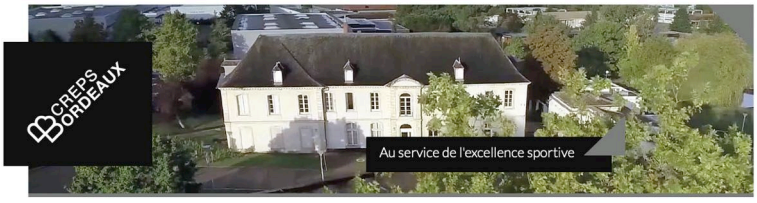
Afin de valoriser l'engagement de ses clients auprès de leurs équipes et partenaires, Asklépian met à disposition sa cellule communication pour la réalisation de nombreux supports de communication autour du RGPD, du DPO et de la sensibilisation. Toutes les réalisations peuvent être personnalisées à leur image. ■



SportTrooper, un produit onepoint transformant les entraînements sportifs.



Auteur : Benoit LACOUR



Dans le cadre de l'appel à projet SportTech porté par la région Nouvelle-Aquitaine, onepoint et le CREPS de Bordeaux ont regroupé leurs compétences pour travailler à l'optimisation de la préparation mentale de l'équipe de France de tir au pistolet.

Ce projet permet de rapprocher des acteurs du sport et du numérique du territoire régional, afin de favoriser et soutenir l'émergence de projets numériques innovants ayant un impact positif sur la performance sportive.



SportTrooper est une solution d'entraînement sur-mesure immergeant le tireur dans l'univers de la compétition sur son lieu quotidien d'entraînement afin de mieux gérer son stress.

Elle comprend :

- Un dispositif immersif : un entraînement augmenté pour une immersion totale du tireur grâce à un écran courbé à large champ visuel dédié à l'affichage d'une vidéo 360.
- Une mesure du stress : le tireur, lors de son entraînement sur-mesure, est équipé de capteurs permettant de mesurer son stress. La récolte de ces données enrichit la recherche scientifique.
- Une application : l'entraînement augmenté est lancé avec l'application SportTrooper développée par onepoint faisant l'interface entre le dispositif physique, les données capturées et l'application de suivi des entraînements.

Concrètement, voici le fonctionnement de SportTrooper :

Le tireur est sur son stand de tir, face à une cible et avec son pistolet. Il est équipé de différents capteurs permettant de récolter des données (rythme cardiaque, degré de sudation, mouvements du pistolet).



Il s'entraine, immergé dans le dispositif, lancé par l'application SportTrooper. Il visualise des lieux de compétition et entend les sons, comme dans un environnement de match.

Par la suite, les données récoltées et analysées permettent d'établir le lien entre l'état physiologique du tireur et la qualité de son tir. Cela permet à l'entraîneur et au psychologue du sport d'identifier ce qui génère du stress chez les tireurs, les résultats étant comparés à ceux d'un entraînement classique.

Le tireur se verra alors proposer des entraînements spécifiques et personnalisés en "injectant" différents éléments visuels et sonores à des moments précis, pour augmenter ou réduire les effets du stress.

En tant qu'architecte des grandes transformations des entreprises et acteurs publics, onepoint apporte toute son expertise scientifique et technique au projet.

BIO

Benoit Lacour est un expert en cybersécurité et réglementation pour la protection des données personnelles au sein de la société onepoint.
Spécialisé en sécurisation des systèmes d'informations et protection de la donnée personnelle, il intervient dans de nombreux domaines comme les analyses de risques, les audits techniques et organisationnels.
Fort d'une expérience de 17 ans acquise au sein du ministère des Armées, il a occupé plusieurs fonctions à responsabilité dans les domaines stratégiques et techniques.
Il intervient dans de nombreux groupes d'expertises au sein du Club EBIOS, de la Fédération Française de la Cybersécurité et au CLUSIR Aquitaine

L'expertise scientifique …

Le rôle du pôle R&D de onepoint est de traiter des enjeux liés au bien-être des individus dans les environnements numériques professionnels : impact des technologies sur la qualité de vie au travail, conception d'un assistant d'aide à la prise de décision, prise en compte des profils cognitifs (tels que la gestion du stress ou encore la motivation) dans les équipes projets, etc...

… alliée à l'expertise technique

L'application SportTrooper a été développée grâce à l'expertise technique de onepoint. Elle fait l'interface entre le dispositif physique, les données capturées et l'application de suivi des entraînements.

Côté serveur, un composant développé en Python permet la récupération et le traitement des informations des capteurs. Un deuxième composant utilise node.js pour communiquer avec le client web. Finalement, l'interface, utilisant Vue.js permet à l'entraineur de suivre en direct les tireurs enregistrés dans le dispositif et de personnaliser leur entrainement.

onepoint.
beyond the obvious

Lien vers la page onepoint sur internet : https://www.groupeonepoint.com/fr/sporttrooper-un-produit-onepoint-transformant-les-entrainements-sportifs/ ■

Congrès partenaires

CHARENTE-MARITIME
CYBER SÉCURITÉ
— CMCS-CONNECT.FR —

CYBERSECURITY
PUBLIC - PRIVATE
DIALOGUES
— CYBERSECURITY-DIALOGUES.ORG —

FIC
— FORUM-FIC.COM —

Une publication

web for business
swiss webacademy

et

MIRAT DI NERIDE
Cyber Sécurité

Note copyright :
Copyright © 2021
SwissWebacademy, Mirat di Neride
et auteurs.
Tous droits réservés.
Le matériel original publié
dans ce volume appartient à la
SwissWebAcademy et à Mirat di Neride

Rédaction (pour la présente édition) :
Laurent Chrzanovski et
Didier Spella

Relecture et corrections :
Martine Spella, Laurent Chrzanovski

Rédaction :
(pour tous les numéros de la revue)
Laurent Chrzanovski et Romulus Maier (†)

ISSN 2559 - 1789
ISSN-L 2559 - 1789

Adresses :
Şcoala de Înot nr.18,
550005, Sibiu, Roumanie
48 Rue Chanzy
17300 Rochefort, France

https://swissacademy.eu/
https://mirat-di-neride.com





Découvrez notre édition spéciale pandémie et cyber

- **sous sa forme originale de revue**
  pdf gratuit sur:
  swissacademy.eu/cybercovid/
- **en format ebook chez votre libraire numérique**
- **en livre imprimé chez votre libraire**

LA ROCHELLE



CHARENTE-MARITIME
CYBER SÉCURITÉ
— CMCS-CONNECT.FR —