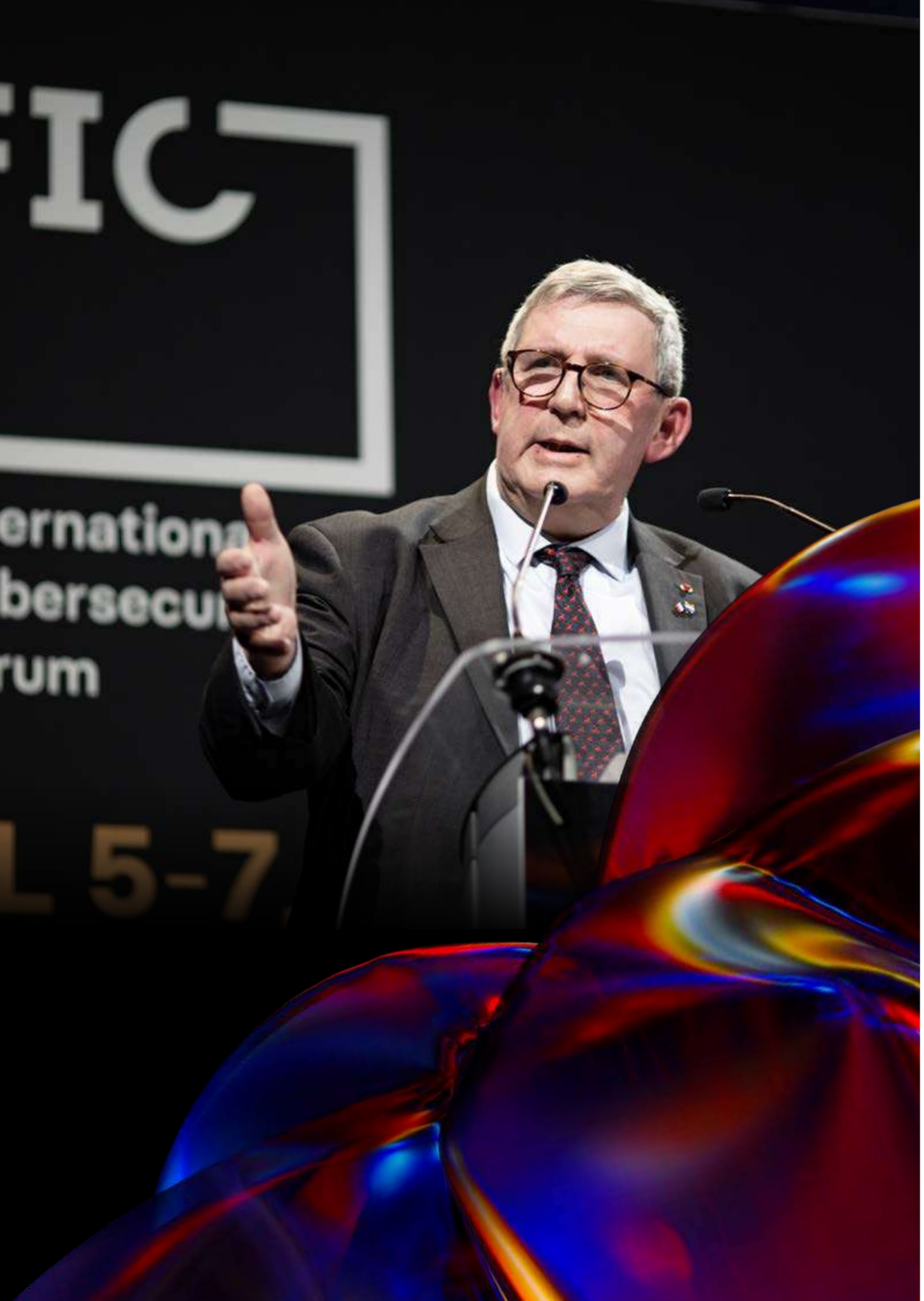
LE FORUM INTERNATIONAL
DE LA CYBERSÉCURITÉ

DEVIENT

FORUM INCYBER EUROPE

sommaire

Temps forts du Forum InCyber 2023



Cloud computing :
la confiance en question(s)

Général d'armée (2S) Marc WATIN-AUGOUARD
Président du Forum InCyber

Guillaume TISSIER
Directeur général du Forum InCyber

Le *Cloud* public est le moteur de la transformation numérique. Avec un taux d'adoption de seulement 40% en Europe, le potentiel de marché pour les offreurs et les gains de productivité pour les clients finaux sont colossaux. Pourtant, le choix d'une solution ne saurait se résumer à des critères fonctionnels et financiers, tant celui-ci est engageant sur le long terme.

En mots simples, le *Cloud* public revient à « utiliser l'ordinateur d'un autre » auquel les organisations confient non seulement leur patrimoine informationnel mais aussi parfois leurs processus métier les plus stratégiques. La cybersécurité et la confiance que l'on peut - ou non - accorder à l'opérateur, sont donc essentielles. La première s'évalue, se mesure, se compare, tandis que la seconde repose sur une appréciation nettement plus subjective que les contrats suffisent rarement à conforter. Résultat : nous sommes souvent contraints de faire confiance par « défaut ».

Sur ces deux volets, les risques sont multiples. Même si la mutualisation des moyens qu'autorise le *Cloud computing* est un avantage en matière de cybersécurité, la concentration des données constitue aussi une vraie faiblesse en termes de résilience : une attaque sur un hyperviseur peut par exemple créer un risque systémique.

Au plan stratégique, la dépendance qu'il crée, voire le « *lock-in* » que génèrent parfois les contrats, peuvent aussi affaiblir les organisations, voire à terme bouleverser les chaînes de valeur traditionnelles.

La confiance est enfin mise à mal par la multiplication des lois à portée extraterritoriale, a fortiori dans un contexte géopolitique tendu.

Alors que 70% des données européennes sont stockées et traitées en dehors du continent, principalement par les hyperscalers américains, la menace d'une prise en otage de celles-ci au gré des tensions internationales apparaît de plus en plus réelle.

Pour faire face à ces menaces et toucher, à son tour, les dividendes de la révolution *Cloud*, l'Europe ne peut plus se satisfaire de cette situation d'extrême dépendance. D'autant qu'elle dispose de nombreux atouts : des acteurs performants et innovants, une industrie traditionnelle puissante, un marché potentiel important etc.

Quelles stratégies et politiques mettre en place pour lui permettre d'accélérer le développement de sa propre industrie *Cloud* ? Quelles priorités en termes de technologies et de secteurs ? Comment l'Europe peut-elle concilier les exigences d'une transformation numérique rapide et sa volonté, désormais assumée, d'asseoir sa souveraineté numérique ? Comment assurer la cybersécurité et la résilience des infrastructures *Cloud*, dont la surface d'exposition aux risques croît de façon exponentielle ? Comment créer la confiance ?

la menace cyber
en chiffres

MENACES

13 fuites de données par jour
Source : Baromètre 2023 des fuites de données Forum InCyber / CNIL

30% des collectivités locales ont déjà été victimes de *ransomware*
Source : CLUSIF

53% des organisations ont subi une attaque sur leur infrastructure *Cloud* au cours de l'année écoulée
Source : Netwrix

79% des entreprises ont subi au moins une violation de données dans le *Cloud* au cours des 18 derniers mois
Source : CapGemini

43% des entreprises françaises touchées en 2022 (contre 54% en 2021) *Source : CapGemini*

74% des flux financiers liés aux attaques par *ransomware* pointent vers la Russie
Source : Chainalysis

13 000 vulnérabilités signalées en 2022 (–30% par rapport à 2021)
Source : NIST

62% des organisations attaquées en 2022 par un *ransomware* payent la rançon
Source : Hiscox

1 La France compte en moyenne 1 personne chargée de la cybersécurité pour 1 500 salariés
Source : Wavestone

la menace cyber
en chiffres

RÉPONSES

2024
La directive NIS 2, entrée en vigueur en 2022, fixe de nombreuses exigences en matière de cybersécurité et sera transposée dans les États membres d'ici la fin de l'année 2024

x10
Le nombre d'organisations concernées par NIS 2 sera multiplié par dix

2022
La Commission européenne a proposé en septembre 2022 une première version de la loi sur la cyber-résilience qui s'appliquera à tous les produits et services contenant du contenu numérique

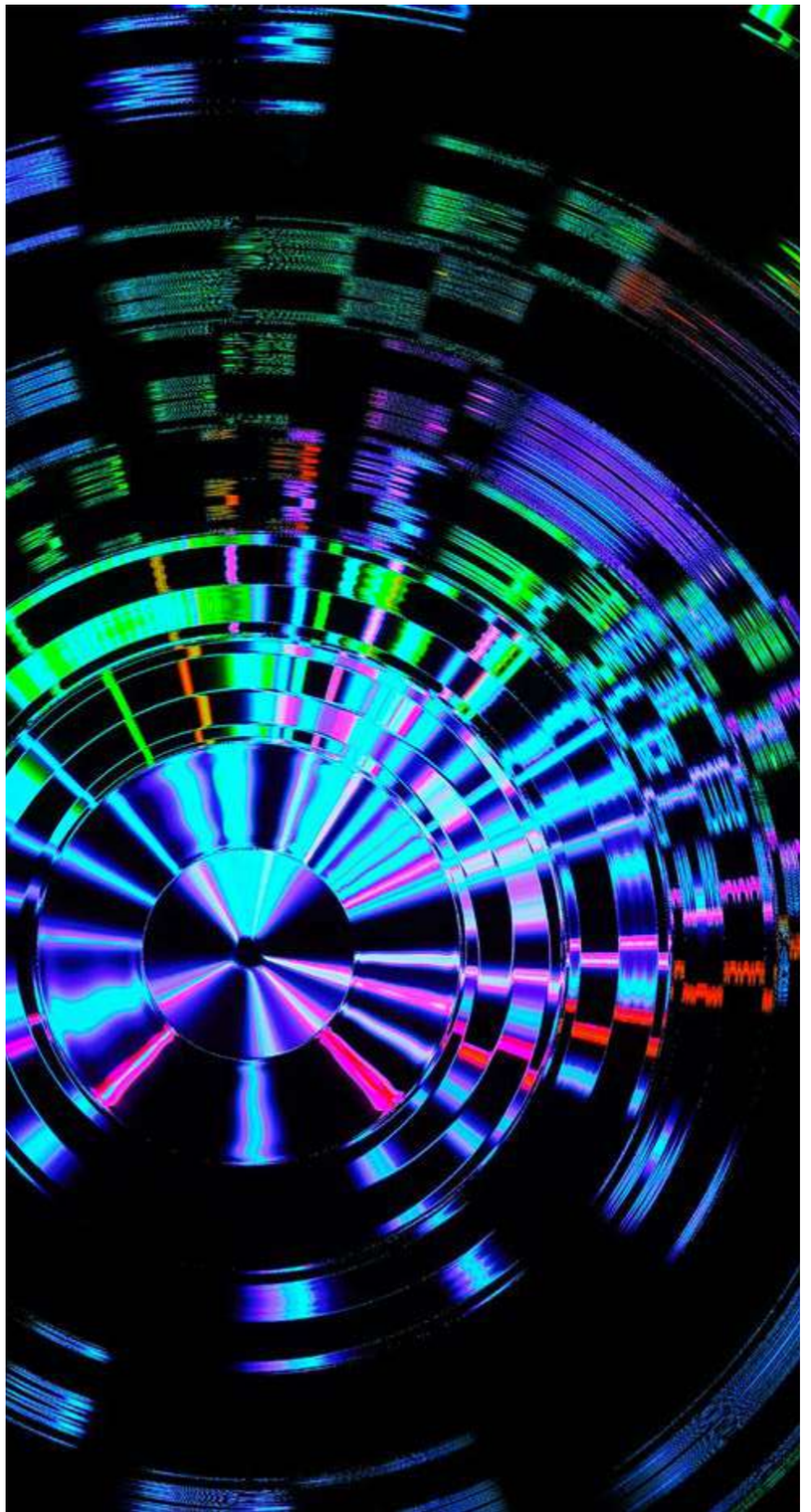
81%
81% des entreprises ont déployé des systèmes EDR *(Endpoint Detection & Response)*
Source : CESIN

12
CSIRT régionaux sont en cours de création

700
collectivités locales ont bénéficié d'une formation en cybersécurité

en 2022
les start-ups européennes ont levé 2,4 milliards d'euros (+20%), soit 16% des montants levés dans le monde en cybersécurité
Source : Tikehau Capital / Baromètre Forum InCyber

2023
Lors du Forum InCyber 2023, le Commissaire européen Thierry Breton annonce la mise en place d'un *« Cyber Solidarity Act »* et d'un dôme cyber européen composé de plusieurs centres opérationnels de cybersécurité



tendances

Vincent STRUBEL

Directeur général de l'ANSSI

Agence Nationale de la Sécurité des Systèmes d'Information

FORUM INCYBER 2023

Il faut passer de la haute couture au prêt-à-porter pour élargir et massifier nos actions.

Un marché mondial de 250 milliards € en 2022

dont 34 milliards €
pour l'Europe

dont 3 milliards €
pour la France

MARCHÉ

tendances

contenus des

plénières

programme

Il est absolument indispensable de coordonner à un niveau européen la cybersécurité, vous pouvez compter sur moi pour le faire avec détermination et sans relâche.

Thierry BRETON

Commissaire Européen au marché Intérieur

VOIR LA VIDÉO

plénière d'ouverture

Nous assumons pleinement de défendre une logique de souveraineté numérique pour développer des champions européens du *Cloud*.

Jean-Noël BARROT
Ministre délégué au Numérique
FRANCE

VOIR LA VIDÉO

La force de la cybersécurité est l'union. L'État ne peut pas répondre seul aux attentes de la cybersécurité. Le Forum InCyber c'est le partenariat public-privé par excellence.

Jean-Noël DE GALZAIN
Président d'Hexatrust
FRANCE

VOIR LA VIDÉO

Merci au Forum InCyber, le plus grand salon de la cybersécurité d'Europe, de réunir tant de profils et de leur permettre de se rencontrer.

Ludivine DEDONDER
Ministre de la Défense
BELGIQUE

VOIR LA VIDÉO

La préparation civile commence par la préparation personnelle. Chaque acteur doit assumer la responsabilité de sa cybersécurité. Les États ne peuvent pas assumer toutes les responsabilités. Chaque acteur doit faire son travail.

Carl-Oskar BOHLIN
Ministre de la Défense civile
SUÈDE

VOIR LA VIDÉO

En ce qui concerne la responsabilité des États, nous disposons d'un cadre normatif pour prévenir les comportements non responsables. La boîte à outils de la diplomatie contient différents outils : le processus le plus direct consiste à tendre la main à un pays, mais nous pouvons aller jusqu'à demander à un pays de prendre des sanctions.

Nathalie JAARSMA
Ambassadrice des Pays-Bas pour la politique de sécurité et le cyberespace *PAYS-BAS*

VOIR LA VIDÉO

À l'OTAN, nous avons mis en place le projet DIANA : nous payons des start-ups pour travailler avec nous, ce qui leur permet de mettre un pied dans notre stratégie. Nous leur donnons accès à nos contrats, ce qui leur permet de travailler dans notre domaine. C'est une situation gagnant-gagnant : elles ont besoin de paix pour travailler, nous avons besoin d'elles pour la paix.

James APPATHURAI
Secrétaire général adjoint chargé des questions de sécurité émergentes – OTAN

VOIR LA VIDÉO

La question ne se résume pas au bon ou au mauvais Cloud : ce n'est pas une solution clé en main, cela ne dispense pas les entreprises de se préoccuper de leurs sauvegardes, leurs mises à jour...

Vincent STRUBEL

Directeur général de l'ANSSI

VOIR LA VIDÉO

plénière #1

Et si le ciel nous tombait sur la tête ?

La difficulté avec les réseaux sociaux, c'est qu'ils génèrent des communautés qui sont d'intérêt, pas de solidarité. Nous sommes dans l'ère de la souveillance : n'importe qui peut diffuser n'importe quoi. Il y a tant d'information que nous sommes perdus. On ne sait pas comment se repérer au sein de cet océan.

Jean-Gabriel GANASCIA

Professeur à la faculté des sciences de Sorbonne Université
et Président du comité d'éthique du CNRS

VOIR LA VIDÉO

plénière #2

La confiance est-elle soluble dans le numérique ?

À ceux qui sont convaincus que la bataille n'est pas perdue, mettons nous ensemble, rassemblons les acteurs pour concurrencer les GAFAM.

Alain ISSARNI

PDG de Numspot

VOIR LA VIDÉO

plénière #3

L'Europe veut-elle faire sa révolution ?

incyber.org

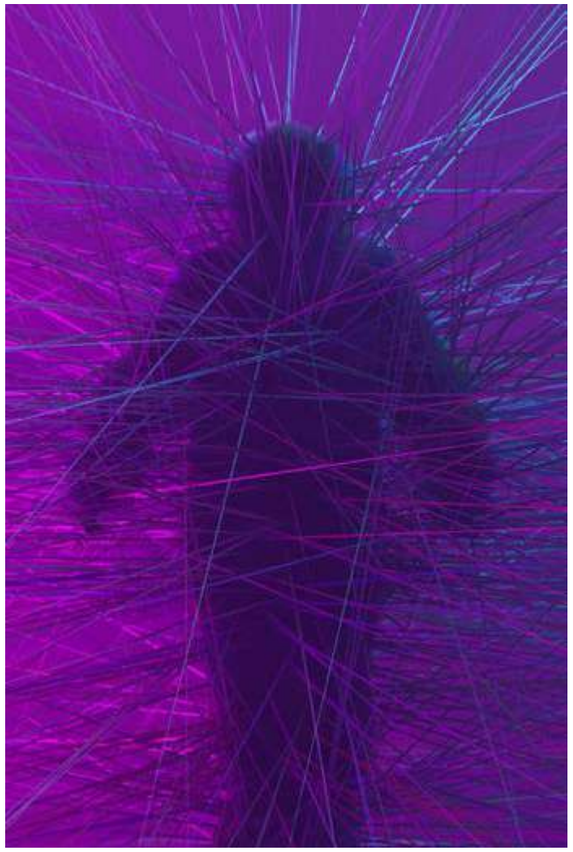
revue de presse

Ces articles ont été rédigés par les journalistes d'InCyber.org
à partir des tables rondes et conférences du Forum InCyber Europe 2023

Les gangs de *ransomware* sont-ils des entreprises comme les autres ?

CYBER CRIMINALITÉ

XAVIER BISEUL



Ces derniers mois, un grand nombre de groupes de *ransomware-as-a-service (RaaS)* ont disparu ou réduit leur activité. Leurs revenus sont, par ailleurs, en baisse en raison de la chute des cryptomonnaies, une plus grande maturité des entreprises et le renforcement du cadre réglementaire. Un contexte défavorable qui remet en cause la pérennité de cette mafia du XXIe siècle.

Les organisations cybercriminelles sont des entreprises comme les autres. Elles naissent, se développent et parfois meurent. Leur taux de mortalité est même particulièrement élevé si on en juge les déconvenues qu'ont récemment traversé les principaux gangs de *ransomware*s.

En septembre 2021, le gang Babuk se sabordait après que les clés de déchiffrement de son rançongiciel ont été publiées sur le *darkweb*.

En mars 2022, le groupe Conti disparaissait après avoir pris position en faveur de la Russie dans la guerre contre l'Ukraine. En janvier 2023, le collectif Hive mettait fin à ses activités après la saisie de leur plateforme par le FBI et Europol. Le même Europol a réussi un beau coup de filet en arrêtant deux membres de DoppelPaymer, en mars dernier.

D'autres gangs célèbres restent en vie mais ont subi quelques revers. En septembre, le builder de LockBit – soit le kit de création de son logiciel malveillant – a fuité sur les réseaux sociaux après que le leader du groupe a refusé de verser son salaire à un développeur. L'activité de Revil a, elle, drastiquement chuté après l'attaque en mai 2021 de Colonial Pipeline, le principal opérateur d'oléoducs américain.

Ces événements posent la question de la pérennité des groupes de *ransomware*. Ces gangs mafieux du XXIe siècle semblent suivre le même schéma que leurs équivalents du monde physique. Ils s'enrichissent rapidement, mènent une grande vie puis finissent par disparaître après le coup de trop ou le faux pas fatal.

L'homme, le maillon faible

Même s'ils se retranchent derrière le modèle industriel du *ransomware-as-a-service* (RaaS), proche du celui du SaaS légal, avec la revente du kit de création à des affiliés et une assistance commerciale 24/7, ces groupes restent vulnérables. Ironie de l'histoire, l'homme reste la principale faille de vulnérabilité.

« Leur modèle de masse repose sur des techniques optimisées et une répartition des tâches entre acteurs. Cette chaîne ne peut pas être automatisée à 100%, il y a toujours des humains derrière », observe Livia Tibirna, analyste cyber threat intelligence chez Sekoia.io.

Même si un gang liste les organisations à cibler et celles à épargner, leurs affiliés commettent des bévues comme s'en prendre à des établissements de santé. LockBit aurait ainsi présenté ses excuses et envoyé une clé de déchiffrement gratuite à un hôpital pour enfants de Toronto, attaqué par erreur. Par vantardise, les groupes de RaaS signent également leurs méfaits ou laissent des indices sur les forums de discussion.

Un écosystème essentiellement russophone

En dépit des rivalités qui apparaissent parfois au grand jour, comme entre LockBit et REvil, un code de l'honneur évite les luttes fratricides. *« L'écosystème reste essentiellement russophone, avec des règles non écrites de camaraderie. La plupart des groupes ne s'attaquent pas entre pays ex soviétiques. Cela n'a pas changé avec la guerre en Ukraine »*, note Livia Tibirna.

Des collaborations inédites voient même le jour. Hive, LockBit et BlackCat ont ainsi orchestré une attaque ciblant à trois reprises le même réseau comme le relevait l'éditeur Sophos. Le contexte géopolitique a néanmoins pu déstabiliser les équipes en place. *« Pour échapper à la mobilisation militaire, des cybercriminels russes se sont expatriés en Turquie ou en Iran, s'exposant au risque de se faire arrêter par les forces de l'ordre internationales »*, poursuit l'experte.

Pour Karim Abillama, directeur avant-vente international business chez NetWitness, la détection et le suivi de ces gangs peut toutefois prendre des années : *« Ces groupes sont très structurés et font preuve de sophistication, notamment dans le mode de paiement, tout en conservant un mode d'entrée banal basé avant tout sur le spearphishing. »*

Les *ransomwares*, la partie émergée de l'iceberg

En termes de ciblage, la menace reste avant tout opportuniste. Il s'agit de faire le tour des portes d'entrée avant de s'introduire dans le système d'information. *« Les gangs ont le choix soit d'attaquer des proies faciles soit d'aller à l'assaut de plus gros poissons pour augmenter leurs profits. Les deux cas de figure existent »*, complète Karim Abillama.

La demande de rançon se double, par ailleurs, systématiquement de la menace de divulguer les données exfiltrées. Karim Abillama note même une tendance à la réextorsion. Les cyber-gangsters reviennent sur les lieux de leur crime en rançonnant une nouvelle fois la victime. Plus d'un tiers des entreprises attaquées par des *ransomware*s en 2022 l'avaient déjà été par le passé, avance ainsi un rapport de Barracuda Networks.

Livia Tibirna note aussi une plus grande souplesse dans les relations entre les groupes de RaaS et leurs affiliés : *« Avant, il n'était pas bien vu que des affiliés s'approvisionnent auprès de groupes différents. Aujourd'hui, cela passe mieux. Ils peuvent recourir à deux ou trois logiciels malveillants différents. »*

L'experte rappelle aussi que les rançongiciels, menace particulièrement visible et médiatisée, ne constituent que la partie émergée de l'iceberg : *« Derrière il y a toute industrie qui s'est constituée dans la revente de données ou le blanchiment de Bitcoins. »*

Des revenus en baisse

En dépit de cette volonté de maximiser les profits, les experts de la table ronde dédiée à ce sujet au Forum InCyber 2023 ont observé une baisse des revenus générés par cette industrie du *ransomware*. Plusieurs facteurs contribuent à cet effritement du marché. Livia Tibirna évoque la plus grande maturité des entreprises qui ont (enfin) généralisé les systèmes de sauvegardes et la chute du cours du Bitcoin et des autres cryptomonnaies.

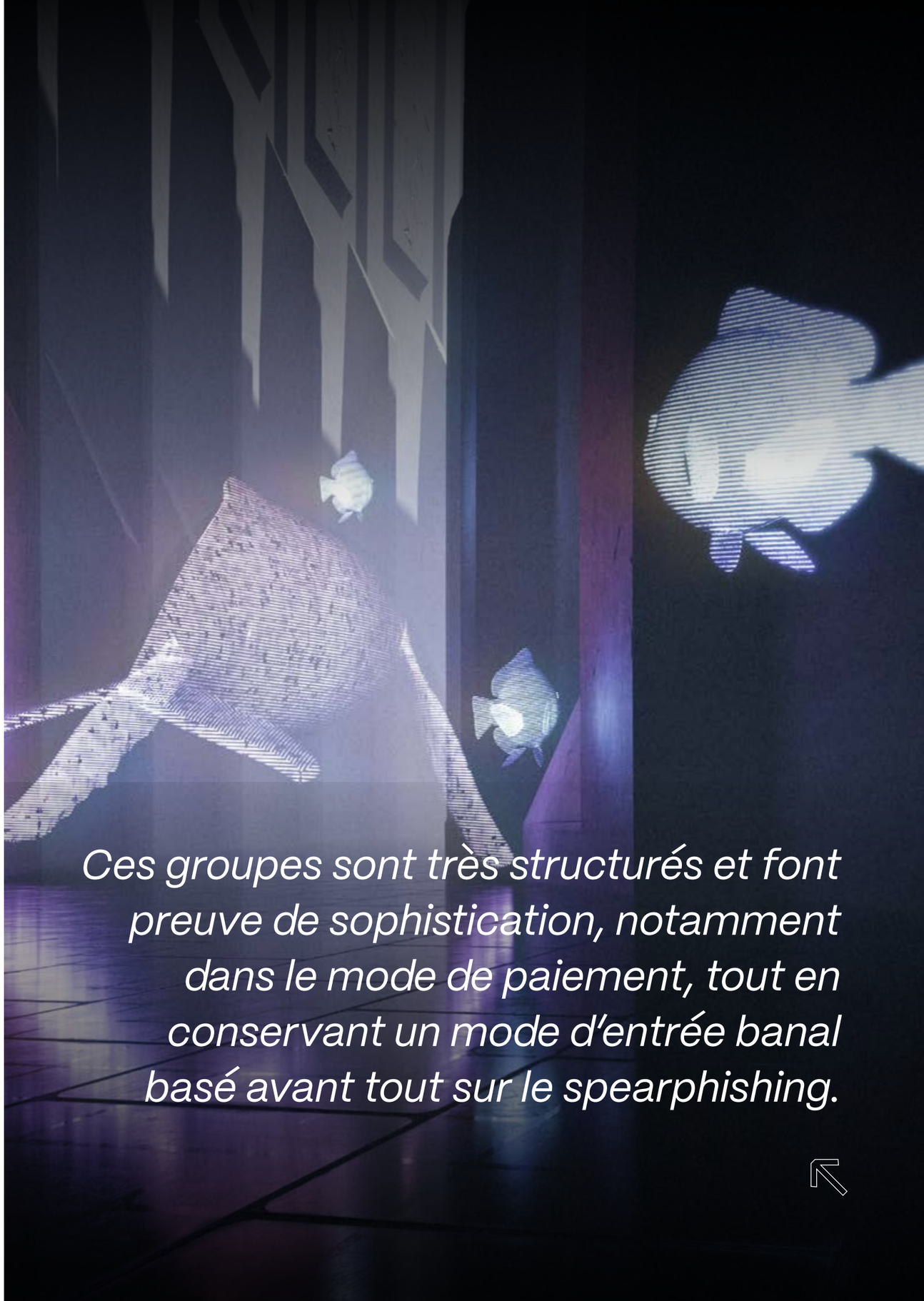
Le cadre légal a aussi évolué. Aux États-Unis, l'attaque contre Colonial Pipeline, en mai 2021, a servi d'électrochoc. Elle a montré qu'au-delà leur activité lucrative, des gangs pouvaient perturber le fonctionnement d'États ennemis. Peu de temps après, le patron du FBI, Chris Wray, exhortait, selon Reuters, les entreprises et les institutions publiques à ne pas payer les rançons demandées pour ne pas alimenter le crime.

Plus récemment, le 1er mars 2023, l'administration de Joe Biden exposait sa stratégie nationale en matière de cybersécurité. Avec une doctrine claire : tout attaque par *ransomware* qui ciblerait une infrastructure critique du pays serait considérée comme une menace pour la sécurité nationale. Seize secteurs clés ont été identifiés, dont la santé et l'énergie.

Il s'agit pour Cody Barrow, *vice president for intelligence and director of threat intelligence* d'EclecticIQ *« d'un sérieux avertissement pour les auteurs de cyberattaques et leurs complices »*. Le *ransomware* devenant un enjeu de sécurité nationale, plus de ressources gouvernementales seront mobilisés

« La coopération internationale est aussi appelée à s'intensifier, les États-Unis collaborant davantage avec les pays alliés », estime-t-il. Les groupes de *ransomware* auront eu au moins le mérite de favoriser l'échange d'informations au sein du monde occidental.

LIRE L'ARTICLE EN LIGNE



L'OSINT a le vent en poupe

TRANSFORMATION NUMÉRIQUE

GEORGES BONFILS

À l'initiative d'Antoine Violet-Surcouf, associé de Forward Global, les professionnels du secteur se sont à nouveau réunis à Lille, le 5 avril dernier, à l'occasion du Forum International de la Cybersécurité (Forum InCyber). Après une première édition très suivie en 2022, les organisateurs de la Journée OSINT ont voulu mettre en lumière cette année le caractère collégial et communautaire du travail de renseignement auprès de sources ouvertes.

Piqûre de rappel : l'OSINT (*Open Source Intelligence*) désigne les enquêtes effectuées à partir de sources ouvertes dans divers contextes : maintien de l'ordre, cyber-protection, journalisme et *fact checking*. Cette expression comprend d'autres disciplines telles que le GEOINT qui porte sur l'analyse des données géographiques, ou le SOCMINT qui analyse les réseaux sociaux.

L'OSINT et la guerre en Ukraine

La journée a débuté avec le témoignage d'un responsable du service ukrainien *« State Bureau of Investigation (SBI) »*. Créé en 2015, les activités de ce bureau ont connu une recrudescence depuis le début du conflit en février 2022 pour compter actuellement près de 1 600 collaborateurs. Dans le contexte exceptionnel de l'invasion russe, ce service a notamment pour objectif de lutter contre la corruption, d'identifier les citoyens ukrainiens qui collaborent avec les forces russes et de collecter des preuves sur les crimes de guerre commis en Ukraine, tout en cherchant à en identifier les auteurs.

Pour cela, les membres de l'agence peuvent s'appuyer sur le *SBI Recognition System*, un outil de reconnaissance faciale, ainsi que sur les images prises par les forces ukrainiennes, les membres du réseau du SBI et parfois les publications des soldats du camp adverse. Un travail de reconstitution de la réalité du théâtre d'opérations à partir de traces digitales pour disposer d'une connaissance stratégique résumé ainsi par un intervenant : *« OSINT works best as a collaborative tool »* (l'OSINT fonctionne mieux en mode collaboratif).

L'OSINT, une méthode utile pour les entreprises

Les pratiques de l'OSINT se révèlent aussi être un outil d'aide utile à la décision au sein des entreprises. Au cours d'une table ronde animée par François Jeanne-Beylot, président du Synfie (Syndicat français de l'intelligence économique), Hortense Grelier, cheffe du service veille et innovation de SEB, explique que le renseignement en sources ouvertes permet de fournir un soutien opérationnel grâce aux informations transmis aux différents services du Groupe.

L'approche apparaît différente pour d'autres entreprises. Selon Henri de Banizette, coordinateur en charge de la sûreté économique pour Auchan Retail International, l'enjeu principal consiste à assurer la pérennité de l'activité, parfois dans des environnements à risques, comme pour l'évaluation de tiers lors d'opérations de fusion / acquisition ou l'appui aux services enquêtant sur des cas de fraudes ou de contentieux.

Sylvain Hajri, fondateur de la communauté OSINT-FR et de la société Epieos, a voulu proposer de son côté une approche différente de l'OSINT avec une méthode *« red team »*. Il s'agit de prendre la place d'une « partie adverse » pour identifier des failles et obtenir des *feedbacks* qui serviront, *in fine,* à renforcer les mesures de défense physique ou numérique de l'organisation observée.

Travail d'analyse et cadre légal

Alexis Pinon, directeur des investigations digitales de Forward Global, a rappelé l'importance du travail d'analyse en OSINT. L'existence d'informations disponibles en grande quantité et les outils disponibles pour les approfondir (reconnaissance faciale, renseignements sur un pseudo ou une adresse IP…) permettent notamment de trouver des informations personnelles. Il est donc nécessaire d'utiliser à bon escient les outils disponibles, et de se méfier des biais et des « faux-positifs ».

Sous l'angle juridique, Marc-Antoine Ledieu, avocat et RSSI, a rappelé le cadre légal à connaître pour pratiquer l'OSINT. Il faut selon lui se poser les questions suivantes : le système d'information qui héberge la *data* est-il destiné à être accessible à tous les internautes ? A-t-on le droit de copier les données recueillies ? De les utiliser ? Il a également insisté sur la distinction entre les notions d'*open data* (données détenues par les pouvoirs publics pour être réutilisables) et de *leaks* (informations privées telles que le secret des affaires, les données personnelles ou encore les informations relevant de la propriété intellectuelle).

OSINT : quels outils et quelles méthodes ?

L'analyste connu sous le pseudonyme de « Palenath » a fait une démonstration de sa méthode pour localiser des personnes recherchées par Interpol à partir de leurs activités sur les réseaux sociaux. Pierre-Antonin Rousseau, Coordinateur du club OSINT & Veille de l'AEGE, est parvenu à remonter aux auteurs présumés d'un *scam*, par rebonds successifs sur les différentes sources en ligne.

Emmanuel Kessler, chef d'équipe partenariat et sensibilisation d'Europol, est revenu sur le travail de l'équipe d'OSINT du European Cybercrime Centre, pour appuyer les investigations numériques menées par ses enquêteurs. Ce travail prend notamment la forme de bulletins d'informations hebdomadaires sur les cyber-incidents les plus récents, les évolutions de *malware* repérées ou encore les questions juridiques touchant au domaine cyber ainsi que des rapports thématiques ciblés pouvant aider les enquêteurs au cours de leurs missions.

Julien Métayer, co-fondateur de la plateforme OZINT, a voulu changer de perspective lors de sa présentation en adoptant le point de vue des « cibles ». Selon lui, les personnes qui pratiquent l'OSINT n'ont pas la même vision d'une information en ligne qu'un internaute lambda ; et par conséquent, toutes les informations mises en ligne, même les plus anodines, peuvent par exemple contribuer à une tentative d'intrusion via un hameçonnage.

Djihad, Ukraine et sites de rencontre

Qu'est-ce qui peut bien réunir le djihad, l'Ukraine et les sites de rencontre ? L'OSINT évidemment. Damien Ferré, le fondateur de Jihad Analytics, a présenté son travail d'analyse des propagandes d'Al-Qaïda et de l'État islamique (EI). Sa présentation a été l'occasion de distinguer la communication très centralisée de l'EI de celle décentralisée des différentes cellules d'Al-Qaïda réparties à travers le monde, ayant leurs propres modalités de communication et susceptibles d'échanger entre elles.

Deux des fondateurs du projet Fox ont présenté leurs méthodes de recherche pour fournir des renseignements sur la présence de troupes russes en Biélorussie. La première étape consistait à identifier les blindés russes acheminés jusqu'à la ville de Smolensk, et la seconde de géolocaliser les soldats russes à l'aide de leur propre outil de SOCMINT développé par l'équipe.

Emmanuelle Welch, détective privée, a qualifié les applications de rencontre d'outils de recherche alternatifs. Au moyen d'un logiciel permettant de modifier la géolocalisation du propriétaire d'un compte, l'enquêtrice dispose d'un outil supplémentaire pour géolocaliser des personnes recherchées. Cela lui permet également de réaliser des audits de sécurité opérationnelle pour les organisations sensibles, en vérifiant les informations que peuvent divulguer certains de leurs membres inscrits sur ces sites.

Toutes ces interventions, qui se sont déroulées dans une salle comble, donnent une idée des nombreux sujets que cette discipline traite et des possibilités qu'elle offre pour les spécialistes de la sûreté, de la veille stratégique et de la cybersécurité. L'importance de fédérer le travail des « OSINTers » a régulièrement été rappelée tout au long de la journée. Rendez-vous est d'ores et déjà pris en mars 2024 pour la prochaine édition de la Journée OSINT.

LIRE L'ARTICLE EN LIGNE

4 enjeux essentiels pour survivre dans le *Far West* des noms de domaine

LUTTE ANTI-FRAUDE

OLIVIER CIMELIÈRE

Le nom de domaine (DNS) est tout sauf un gadget anodin. Il est celui qui va véhiculer sur le Web le nom d'une entreprise ou d'une marque de produit. Il est celui qui va traduire l'adresse IP chiffrée d'un site Internet en un nommage intelligible et mémorisable pour n'importe quel internaute.

À ce nom de domaine s'ajoute ensuite une extension qui va catégoriser le site selon un périmètre géographique (.fr pour la France, .de pour l'Allemagne, .it pour l'Italie ou encore le .com pour le monde) ou une activité sectorielle (.org pour les ONG, .tv pour les médias, etc). *In fine,* le nom de domaine est véritablement la signature numérique d'un acteur économique, gouvernemental, associatif ou autre.

ENJEU N°1 : déposer des noms de domaine, oui mais lesquels ?

Avocate spécialisée en propriété industrielle au cabinet Lexing Alain Bensoussan Avocats, Virginie Brunot connaît bien la première étape du dépôt de nom de domaine pour éviter que celui ne soit enregistré par un tiers (et donc inutilisable pour soi) ou pire par quelqu'un de mal intentionné qui détourne le trafic Web vers un faux site à des fins illégales. Pendant longtemps, les entreprises ont donc adopté une stratégie simple (mais relativement coûteuse) : enregistrer massivement le plus d'adresses possibles pour limiter ainsi les risques d'usurpation et se protéger.

Aujourd'hui, cette position est devenue intenable économiquement au fur et à mesure des nouvelles extensions apparues sur le marché qui sont au nombre d'environ 1 500 dans le monde entier. Pour Virginie Brunot, il convient donc de s'interroger sur les DNS essentiels à l'entreprise (généralement, le .com, le .fr pour un acteur français et éventuellement le .tv ou .media s'il s'agit par exemple d'un organe de presse).

Une fois le dépôt effectué auprès d'un bureau d'enregistrement agréé, il est recommandé de mettre en place une veille fine sur de nouveaux dépôts qui interviendraient sur des DNS non retenus par l'entreprise. Objectif : savoir qui est derrière cet acte et anticiper éventuellement un potentiel risque de malveillance si l'adresse devient active par la suite.

ENJEU N°2 : minorer le risque d'usurpation de DNS

C'est sans doute le point le plus crucial dans la gestion d'un portefeuille de noms de domaines. Si les DNS laissés libres (car jugés non essentiels) ne doivent pas pour autant être laissés sans surveillance, il en est de même pour les noms de domaines approchants (à un caractère près par exemple).

Le risque d'être victime de *typosquatting* est particulièrement fort et nombreux sont les escrocs à y recourir. Directrice commerciale du bureau d'enregistrement chez NameShield, Muriel Bochaton note que ce genre d'action représente près de 15% des litiges liés aux noms de domaine. Avec des conséquences non négligeables : l'internaute peut être victime d'une rançon ou son appareil infecté par un *malware* dès que la connexion avec le site pirate est établie.

Le risque est d'autant moins neutre que la vérification de l'identité des demandeurs pour enregistrer des DNS n'est pas forcément contraignante. En France, hormis le « .gouv.fr » strictement interdit à tout acteur en dehors de l'État français, les autres extensions restent disponibles. Elles le sont sur le principe du « premier demandé, premier servi » selon les règles édictées par l'ICANN *(Internet Corporation for Assigned Names and Numbers),* l'autorité de régulation mondiale d'Internet.

Même en France, l'AFNIC (Association française pour le nommage Internet en coopération), en charge du « .fr », a fini par assouplir ses exigences et s'aligner sur la position internationale. L'identité des demandeurs est donc vérifiée *a minima* sur la base de leur bonne foi morale et sans toujours fournir des éléments comme un nom de contact, une adresse physique ou un téléphone.

C'est là où il convient de bien choisir son bureau d'enregistrement quand on procède à un dépôt de DNS. La plupart des acteurs sont des entités privées à vocation commerciale. Certains encouragent fortement les demandeurs à faire des enregistrements sur les nouvelles extensions qu'ils créent et vendent mais se dédouanent ensuite lorsque des abus du genre cybersquatting surviennent et restent aux abonnés absents.

ENJEU N°3 : quels recours pour protéger ses DNS ?

Avant même d'envisager le piratage ou le cybersquatting, il est une action à mener impérativement et qui est pourtant assez souvent oubliée selon Nicolas Pawlak, ingénieur civil de la défense au ministère des Armées : la date d'expiration du dépôt de DNS. Si le renouvellement n'est pas effectué dans le temps imparti, l'adresse redevient disponible pour quiconque. Il s'agit donc de planifier rigoureusement les échéances pour éviter un tel cas de figure qui peut rendre un site Web inutilisable.

Ensuite, face à un abus constaté, l'entreprise dispose de plusieurs recours pour rendre inactif le site litigieux. En France, elle peut formuler une requête auprès de l'AFNIC pour que celui-ci soit bloqué dans un premier temps puis supprimé si le délit est avéré. La procédure prend entre 2 et 7 jours selon la complexité du cas. D'autant plus que les dossiers ne sont pas toujours évidents. À cet égard, Nicolas Pawlak a cité l'amusante anecdote autour du DNS « mamie est chaude.fr ». Sur le coup, un site pornographique était suspecté. En fin de compte, l'adresse renvoyait vers le site Web d'un boulanger de Versailles !

Le bureau d'enregistrement via lequel les DNS ont été déposés, peut aussi être un allié utile pour entreprendre les démarches face à une dérive avérée. L'hébergeur du site suspect peut également être sollicité mais sans garantie de temporalité courte. Enfin, une fois que le DNS délictueux ou usurpé est radié, l'entreprise peut aussi demander le transfert de ce dernier s'il est considéré comme essentiel dans la gestion de son portefeuille d'adresses.

ENJEU N°4 : s'astreindre à un nommage cohérent et une vraie gouvernance

Autant il est capital d'avoir des noms de domaine signifiants et facilement mémorisables, autant il est fortement conseillé d'avoir une stratégie de nommage homogène pour son portefeuille d'adresses. Jérôme Guihal de l'ANSSI déplore que certaines entreprises fassent preuve d'un certain laxisme dans le nommage de noms de domaines qu'elles vont ensuite utiliser.

Le cas de La Poste a été évoqué. Pour ses différents services en ligne, le numéro 1 français de la distribution de courrier n'hésite pas à enregistrer des noms de domaine où ne figure plus la mention « la poste.fr ». C'est le cas notamment pour les activités de Colissimo où le libellé du DNS est totalement différent.

Aux yeux de l'expert, il s'agit certes d'un risque moindre en termes de sécurité pure mais cela peut brouiller la compréhension des internautes. Ceux-ci peuvent en effet penser qu'il s'agit d'une énième opération de *phishing* ou de site frauduleux et ne pas cliquer sur la notification pourtant vraie qui leur a été envoyée.

Il ressort donc la nécessité absolue pour une entreprise de mettre en place une gouvernance dans la gestion de ses noms de domaines. Et ce pour éviter d'en perdre la jouissance, d'être piraté ou usurpé, voire d'introduire la confusion auprès de ses publics. À cela s'ajoute la précaution de bien choisir son bureau d'enregistrement pour disposer d'un partenaire fiable en toutes circonstances.

LIRE L'ARTICLE EN LIGNE

cocktail

hexatrust

HEXATRUST

CLOUD CONFIDENCE & CYBERSECURITY

MERCREDI 5 AVRIL 2023

Comment la guerre en Ukraine a accéléré la construction d'une cyberdéfense européenne

SÉCURITÉ ET STABILITÉ DU CYBERESPACE

XAVIER BISEUL

Le retour de la guerre à ses frontières a créé un électrochoc au sein de l'Union européenne. Ces derniers mois, elle multiplie les initiatives pour renforcer ses capacités de cyberdéfense et assurer une meilleure coopération entre États-membres.

Pour la première fois dans l'histoire contemporaine, une cyberguerre a précédé une guerre « traditionnelle ». Dans la nuit du 13 au 14 janvier 2022, quelques semaines avant l'invasion effectif des troupes russes sur son territoire, l'Ukraine était visée par des vagues de cyberattaques ciblant ses infrastructures vitales et des sites gouvernementaux. Le cyberspace ne connaissant pas de frontières géographiques, la Russie a utilisé des logiciels malveillants de type « *wiper* ». Ces *malwares* destructeurs ont fait des victimes collatérales parmi les entreprises et institutions européennes.

Bien avant de lui envoyer des chars d'assaut, l'Union européenne est venue, en ce début de conflit, au secours de l'Ukraine dans le cyberspace. Elle déployait hors de ses frontières sa force d'intervention rapide cyber. Ce Cyber Rapid Response Team, ou CRRT, dépend de la PESCO *(Permanent Structured Cooperation*), la structure permanente qui assure la coopération entre États-membres dans les domaines de la sécurité et de la défense.

Un « cyber bouclier » européen dès 2024

« L'Ukraine est un véritable 'wake up call' pour notre cyberdéfense », déclarait en novembre 2022 Thierry Breton. Le commissaire européen au Marché intérieur pointait alors le manque de souveraineté du Vieux Continent dans le domaine. *« Nous avons dû prendre pour nous défendre des ressources qui n'étaient pas européennes »*, a-t-il annoncé.

Quelque cinq mois plus tard, Thierry Breton a pu apprécier le chemin parcouru. La veille de son intervention au Forum InCyber 2023, il officialisait la création d'un « cyber bouclier » européen. Opérationnel début 2024, ce dispositif, qui disposera d'un budget d'un milliard d'euros, vise à détecter plus rapidement les attaques en amont. Il reposera sur un réseau de cinq à six centres SOCs *(Security Operations Centers).*

La nécessaire coopération entre pays alliés

Les efforts de l'UE en matière de cyberdéfense ne se limitent pas à ce cyber bouclier. Ces derniers mois, l'Europe a multiplié les initiatives pour tenter de rattraper son retard. La présidence française de l'Union européenne, qui s'est tenue au premier semestre 2022, a permis des avancées en termes de gouvernance. Il en résulte notamment la création de la Conférence stratégique des cyber commandeurs de l'Union européenne (CyberCo).

Plus récemment, le 10 novembre, la Commission présentait la politique de l'Union en matière de cyberdéfense et un plan d'action sur la mobilité militaire 2.0 *« afin de remédier à la détérioration de l'environnement sécuritaire à la suite de l'agression de la Russie contre l'Ukraine »*.

Au-delà du renforcement des capacités de protection, le plan rappelait le nécessaire effort de coordination entre *« les acteurs nationaux et de l'UE en matière de cyberdéfense, afin d'accroître l'échange d'informations et la coopération entre les cybercommunautés militaires et civiles »*. Il prévoit aussi la création d'un fonds d'urgence et une réserve de ressources cyber permettant de mobiliser des prestataires certifiés.

Quelques jours plus tard, dix-huit pays membres, dont la France, lançaient le programme MICNET *(Military Computer Emergency Response Team Operational Network)*. Géré par l'Agence européenne de défense (AED), il vise à approfondir la coopération entre les CERT nationaux.

« La guerre en Ukraine nous fait changer de paradigme »

Lors d'une table ronde au Forum InCyber 2023, Wiktor Staniecki, chef de division adjoint du Service européen pour l'action extérieure (SEAE), a insisté sur cette nécessaire coopération entre États-membres et l'accroissement des relations bilatérales entre cyber diplomaties : *« Notre résilience passe par l'échange d'informations et le partage de bonnes pratiques. »*

Il évoque aussi une possible coordination avec l'OTAN qui dispose, depuis 2008, d'un Centre d'excellence pour la cyberdéfense basée à Tallinn, en Estonie. Dans une déclaration conjointe datée du 10 janvier 2023, l'UE et l'OTAN évoquaient d'ailleurs la nécessité d'une coopération dans *« la lutte contre les menaces hybrides et les cybermenaces »*.

Responsable de l'unité *« Information Superiority »* à l'Agence européenne de défense (AED), Alessandro Cignoni plaide aussi pour *« une approche unifiée dans la stratégie cyber »*. *« La guerre en Ukraine nous fait changer de paradigme. Les actions doivent être enclenchées plus rapidement. Ce qui nécessite des efforts sur le long terme »*, a-t-il affirmé.

Directeur des affaires européennes du cabinet Rasmussen Global, Arthur de Liedekerke abonde dans ce sens : *« La cyber résistance que démontre actuellement l'Ukraine ne vient pas de nulle part, elle a nécessité des années de préparation. De même, les États de l'UE doivent se préparer collectivement. »*

Un cadre réglementaire plus exigeant

Les experts présents à cette table ronde insistent également sur l'apport du secteur privé à l'effort de (cyber) guerre. Le soutien de la *big tech* américaine à l'Ukraine a été beaucoup médiatisé. L'administration de Kiev a migré ses données sensibles dans les *Cloud* d'AWS (*Amazon Web Services*) et de Microsoft afin d'assurer la continuité de ses activités en cas de destruction de ses *datacenters*. Pour autant, *« les entreprises européennes de la cybersécurité ont aussi aidé l'Ukraine en faisant des dons de licences logicielles »*, rappelle Arthur de Liedekerke.

La cyber-résilience européenne passera aussi par un cadre réglementaire plus exigeant. Dévoilée le 16 décembre 2022, la nouvelle stratégie de cybersécurité de l'UE évoque deux nouvelles directives dont l'une (SRI révisée ou SRI 2) vise à hausser le niveau de protection des réseaux et des systèmes d'information des entreprises. La seconde portera spécifiquement sur la résilience des entités critiques.

LIRE L'ARTICLE EN LIGNE

Cybersécurité : l'identifiant et son mot de passe sont au cœur de la cybermenace

CYBER RISQUES

OLIVIER CIMELIÈRE

Plus que jamais, l'identifiant et le mot de passe associé demeurent la pierre angulaire des pirates informatiques. Une faille qu'il convient de traiter en priorité au risque sinon de voir l'entreprise paralysée. C'est le mot d'ordre majeur qui ressort d'une conférence donnée le 6 avril au Forum InCyber Europe 2023 par Sébastien Baron, directeur technique de CrowdStrike, éditeur de solutions de cybersécurité et Franck Perillier, directeur de la sécurité des systèmes d'information du groupe immobilier Emeria.

80% des failles de sécurité proviennent de la compromission de comptes d'utilisateurs. Ce résultat provient de deux études récentes convergentes réalisées respectivement par l'institut Forrester Research et l'opérateur télécoms Verizon. Autant dire qu'au sein de la chaîne d'attaque qu'adoptent les cyberattaquants pour pénétrer des systèmes informatiques, l'identifiant et son mot de passe restent un talon d'Achille sur lequel une attention toute particulière doit être portée en matière de sécurité.

Aux yeux de Sébastien Baron, directeur technique de CrowdStrike, cette combinaison est effectivement cruciale. Il n'est en effet pas forcément détectable par les traditionnelles solutions EDR qui sont installées sur les infrastructures informatiques des entreprises pour lutter contre les attaques DDoS, les virus ou encore les rançongiciels. Cela implique par conséquent d'avoir une autre approche sécuritaire.

Le marché noir des identifiants très prisé des pirates

Le représentant de CrowdStrike insiste d'autant plus sur ce point qu'identifiants et mots de passe constituent un véritable marché parallèle sur des plateformes de brokers du *darkweb* où les pirates informatiques viennent acheter des bases entières déjà dérobées pour procéder ensuite à leurs propres assauts informatiques.

Ces bases comportent généralement des identifiants, des mots de passe mais aussi des données de configuration et des cookies de sessions. Ils sont autant de passe-partout pour s'introduire frauduleusement et furtivement dans les systèmes d'information d'une entreprise ciblée.

En effet, une fois ces informations critiques récupérées, la technique d'intrusion est bien rodée. Le pirate informatique entre un compte existant. Une fois à l'intérieur, il peut opérer facilement et s'attaquer alors à l'*« active directory »* (service d'annuaire utilisé pour stocker des informations relatives aux ressources réseau sur un domaine). Il peut donc y créer de nouveaux comptes utilisateurs qu'il va doter de droits d'administration plus étendus. Ces mêmes droits permettent, *in fine*, de prendre le contrôle d'un ou plusieurs domaines de l'architecture informatique d'une entreprise. Mais aussi de siphonner les bases de données les plus sensibles.

La complexité du réseau augmente la menace

Selon l'édition 2023 du *« Global Threat Report »* de CrowdStrike, 12% des intrusions sont perpétrées avec un compte valide et 73% avec des nouveaux comptes créés.

Selon Franck Perillier, directeur des systèmes d'information d'Emeria, l'*« active directory »* est un actif particulièrement critique dans la sécurité informatique d'une entreprise. C'est lui en effet qui permet l'authentification pour qu'un utilisateur accède à différentes fonctionnalités selon son profil et les niveaux d'autorisation accordés.

Or plus l'entreprise est grande et internationale, plus l'architecture des systèmes est complexe avec une grande variété d'outils applicatifs aux mises à jour inégales et aux technologies différentes. Sans parler de l'intervention de multiples acteurs internes (développeurs, maintenance, simples utilisateurs, etc.) mais aussi externes (fournisseurs, clients, sous-traitants, etc.).

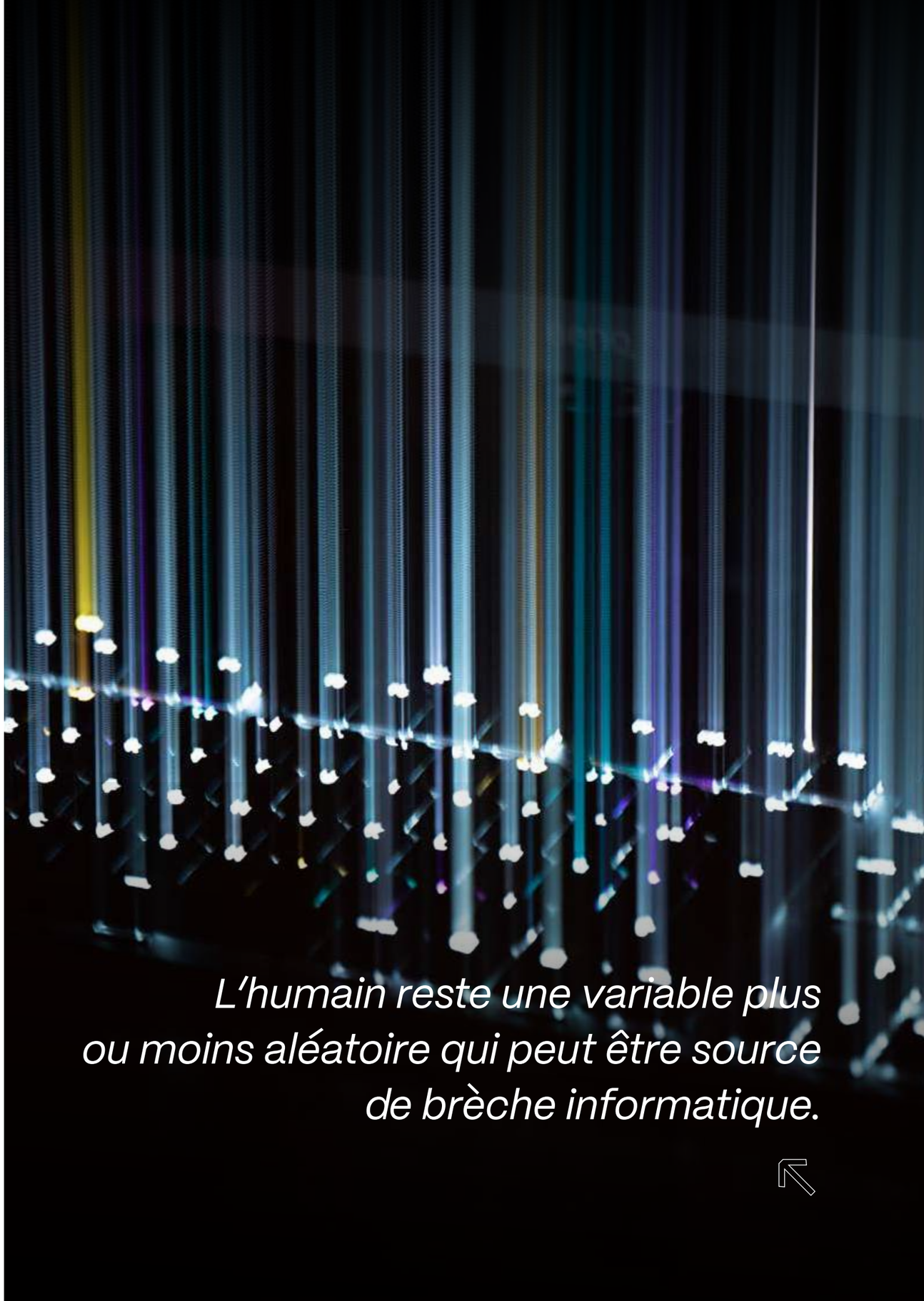
Observer les comportements tout en sensibilisant sans relâche

Cette multiplicité rend de fait vulnérable l'architecture informatique. Particulièrement lorsqu'un pirate informatique parvient à s'y faufiler. Pour Franck Perillier, une des parades consiste à analyser les comportements des différents comptes connectés et actifs dans le système grâce notamment à des solutions technologiques comme celle développée par CrowdStrike. Cela permet ainsi de repérer des comptes aux intentions suspectes (en observant en particulier l'historique des *logs*) et intervenir avant que l'intrus ne se mette en capacité d'attaquer plus amplement le réseau informatique et ses ressources.

Néanmoins, l'expert d'Emeria rappelle que la cyber-hygiène passe aussi par l'établissement de règles et de protocoles de sécurité que les différents utilisateurs se doivent d'appliquer. Or, note-t-il, l'humain reste une variable plus ou moins aléatoire qui peut être source de brèche informatique. Notamment à cause de mots de passe trop faibles comme le classique *« nom de la société + 123 »* que les cyberattaquants connaissent par cœur.

Si la sensibilisation ne fonctionne pas, il faut alors adopter un mode plus coercitif. La solution de CrowdStrike permet ainsi d'identifier les comptes ayant des mots de passe jugés comme non-efficaces et les contraindre à en changer. Tant que le renforcement n'est pas effectif, l'utilisateur ne peut plus opérer dans le système. Au cœur de la technologie, l'humain demeure fondamental.

LIRE L'ARTICLE EN LIGNE



CRQ : comment quantifier les cyber-risques en termes financiers

SÉCURITÉ OPÉRATIONNELLE

FABRICE DEBLOCK

Lors de l'édition 2023 du Forum InCyber, le standard FAIR *(Factor Analysis Information Risk)* a été présenté en atelier par la société C-Risk. Gros plan sur cette méthode de quantification des cyber-risques et de ses bénéfices pour les entreprises.

En matière de gestion et d'évaluation des risques de cybersécurité, il existe plusieurs méthodes possibles : ne pas analyser les risques du tout, les analyser de manière qualitative ou procéder à leur quantification *(Cyber Risk Quantification / CRQ).*

« Dans les entreprises, les décisions relatives à la cybersécurité reposent, quand elles existent, sur des analyses essentiellement qualitatives. Ces analyses sont soumises aux biais cognitifs, ces schémas mentaux qui nous permettent de prendre des décisions rapides face à des situations que nous croyons avoir déjà vécues ou que nous reconnaissons. Dans la plupart des cas, cette intuition, cette expérience et cette expertise sont très utiles. En revanche, dans des situations vraiment complexes et stratégiques, elles se révèlent souvent mauvaises conseillères », déclare Christophe Forêt, cofondateur et président de C-Risk.

Pour faire face à cette complexité, il existe des modèles qui facilitent, avec plus ou moins de justesse et de facilité, la quantification des risques cyber en termes financiers. *« Ces modèles permettent, grâce à l'utilisation de méthodes mathématiques, de peser le pour et le contre et d'aller chercher des avis contradictoires. L'objectif est de dégager des décisions plus objectives, davantage défendables et qui, si elles étaient répliquées par d'autres personnes, amèneraient à des conclusions statistiquement comparables »*, ajoute Christophe Forêt.

FAIR, un standard mis au point par un RSSI en 2005

Le standard FAIR (*Factor Analysis of Information Risk* / Analyse des facteurs du risque informationnel) fait partie de ces modèles de CRQ. Il s'agit d'un standard de l'*Open Group* mis au point en 2005 par Jack Jones, alors RSSI de la compagnie d'assurance Nationwide. Sa taxonomie décrit par le menu quels composants participent à la fréquence d'un sinistre et à l'ampleur des pertes financières à redouter en cas de survenance de ce sinistre.

« Le modèle FAIR permet d'exploiter des informations incertaines grâce à l'utilisation de plages de données estimées et de niveaux de confiance correspondants. La fréquence des sinistres, les contrôles et l'ampleur des sinistres (impact en termes financiers) y sont modélisés », note Christophe Forêt.

Le modèle aide à décomposer le risque en variables qui peuvent être estimées non pas en valeurs discrètes, mais dans des plages correspondant au « minimum », au « plus probable » et au « maximum ». Grâce à l'utilisation des simulations de Monte-Carlo, une même formule peut être évaluée des milliers de fois à l'aide de valeurs sélectionnées parmi les intervalles. Cela permet ensuite de générer une distribution probabiliste des montants des pertes futures potentielles.

« L'avantage avec les plages est de pouvoir dire, par exemple, que le risque lié aux ransomwares représente, pour une entreprise donnée, entre 500 000 et 4 millions d'euros. C'est beaucoup plus précis que des termes comme 'cela vous coûtera cher' ou 'c'est un risque rouge'. Cela permet de définir correctement ce qu'est un risque, c'est-à-dire une perte financière résultant d'un sinistre sur un actif », complète Christophe Forêt.

Des bénéfices multiples pour les entreprises

Un des principaux bénéfices de cette méthode est de pouvoir quantifier un nombre important de scénarios. *« Quand nous nous intéressons à un univers de risques, nous procédons dans un premier temps par triage. En quelques heures, nous pouvons donner des ordres de grandeur avant d'aller davantage dans le détail selon les cas d'usage. Et à partir du moment où nous nous apercevons qu'il y a un sinistre, nous essayons d'évaluer s'il peut y avoir des effets dominos, avec à la fois des coûts internes et externes, et des temporalités qui ne sont pas toujours celles des vendeurs de solutions »*, analyse Christophe Forêt.

La méthode de quantification permet ainsi d'accompagner un directeur des assurances qui cherche à savoir si la couverture qu'il a souscrite correspond à son exposition réelle aux risques cyber. *« Parfois, les entreprises se disent qu'elles ont 5 millions d'euros de couverture, avec une franchise de 'seulement' 500 000 euros. Mais si nous creusons, nous constatons que les 5 millions d'euros concernent l'ensemble des sinistres sur un cycle fiscal, et que la franchise s'entend par type de perte. Or, grâce à la quantification, nous savons qu'aucun des risques, par catégorie de perte, n'atteindra jamais le niveau de la franchise »*, détaille Christophe Forêt.

Autre exemple, celui des équipes de sécurité opérationnelles qui, sur la mise en œuvre de certaines solutions de protection, peinent à trouver un terrain d'entente. *« Typiquement, sur le chiffrement, ces équipes peuvent ne pas être d'accord sur la méthode à appliquer. Doivent-elles chiffrer les données, la base, l'OS… Et quels vont être les coûts associés ? En descendant plus finement dans la taxonomie, nous pouvons fournir des analyses plus fouillées afin d'éclairer les décideurs. Dans certains grands groupes, cela peut représenter des millions d'euros d'investissement »*, conclut Christophe Forêt.

LIRE L'ARTICLE EN LIGNE

gala
cyberleaders

CYBER LEADERS
LA REVUE STRATÉGIQUE DE LA CYBERSÉCURITÉ

JEUDI 6 AVRIL 2023

Course d'obstacles pour le *Cloud* souverain européen

SOUVERAINETÉ NUMÉRIQUE

STANISLAS TARNOWSKI

Malgré des avancées remarquables, le *Cloud* européen semble à la peine face à l'écrasante domination des GAFAM. L'analyse qu'en ont fait régulateurs, professionnels du *Cloud* et de la cybersécurité lors d'une table ronde au Forum InCyber 2023 ne vient guère dissiper cette impression. Avis de tempête sur le *Cloud* européen ?

En dépit de l'optimisme et du volontarisme affichés par les acteurs publics et privés du *Cloud* souverain européen, il y a encore loin de la coupe aux lèvres pour le ce projet hautement stratégique. C'est ce qui ressort en filigrane de la table ronde *« Vers un contre-modèle européen aux normes Cloud US ? »* organisée au sein du Forum InCyber 2023 à Lille.

Le constat qu'y dressait Solange Viegas Dos Reis, directrice juridique groupe chez OVH*Cloud*, était sans appel : *« En 2017, la part des acteurs européens dans le marché européen du Cloud était de 27%. Cinq ans plus tard, le marché a explosé et les mêmes acteurs européens ne pesaient plus que 13 % »*. Les Américains dominent le secteur de la tête et des épaules et l'Europe accuse son retard en termes de parts de marché et de technologies.

Et les défis sont loin d'être uniquement économiques, comme l'expliquait à la tribune Hugues Foulon, CEO d'Orange Cyberdefense. *« L'un des principaux problèmes pour certains de nos clients, ce sont les enjeux d'extraterritorialité, liés notamment au Cloud Act et au Patriot Act. Nous avons vocation chez Orange à ne pas être naïfs, à faire comprendre les conséquences des choix, quels qu'ils soient d'ailleurs. »*

L'extraterritorialité du droit américain ? Vous devenez justiciable des États-Unis dès lors que vous employez un bien ou un service américain, qu'il s'agisse d'un simple dollar ou d'une adresse Gmail.

Conséquence directe : tout utilisateur d'un service de *Cloud* d'une société américaine tombe sous le coup de la loi américaine et la confidentialité de ses données n'est dès lors plus garantie.

Face aux enjeux du *Cloud*, *« ne pas être naïf »*

« Nous parlons de protection des données et de son importance, mais nous oublions le lien avec les droits fondamentaux, c'est-à-dire le droit à la vie privée. Et la vie privée ne s'étend pas seulement aux individus qui vivent dans l'Union européenne, elle s'étend aussi aux personnes morales, comme les entreprises », détaillait Peter Sund, CEO du FISC (*Finnish Information Security Cluster*, l'association des entreprises finnoises de cybersécurité).

Le *Cloud* en Europe ? Un marché totalement dominé par des acteurs étrangers parfois intrusifs, dont le gouvernement peut s'arroger le droit d'accéder aux données de tout citoyen ou entreprise, tout le contraire d'un « *Cloud* de confiance ». Une expression très française, soulignait Rayna Stamboliyska, Uncertainty management specialist chez RS Strategy et animatrice de la table ronde, avant de demander aux intervenants ce que *« veut dire la confiance dans le Cloud et comment ils la mettent en œuvre dans leur quotidien, technique, technologique et opérationnel »*.

« Il se résume au fait que l'utilisateur a une liberté de choix grâce à l'interopérabilité des technologies, la réversibilité.

De plus, il est sûr que ses données seront protégées et ne seront pas utilisées à d'autres fins que celles qu'il a choisies », répondit Solange Viegas Dos Reis. Des principes opérationnels auxquels a souscrit Hugues Foulon, qui a plaidé pour *« des solutions pragmatiques qui permettent d'avancer et de gagner en autonomie stratégique. Et c'est ce qu'on a fait avec "Bleu" »*. Opérationnelle en 2024, cette co-entreprise d'Orange et de Capgemini, en partenariat avec Microsoft, visera précisément à fournir un « *Cloud* de confiance » ou « souverain » aux acteurs publics et privés à la recherche du plus haut niveau de sécurité et de confidentialité.

« Schrems II », les acteurs du *Cloud* au pied du mur

Une solution qui a « l'avantage d'être conforme *by design*. C'est la seule façon d'être conforme au RGPD », soulignait Bertrand Pailhès, directeur des technologies et de l'innovation à la CNIL. En effet, la technique à elle seule ne suffit pas: un cadre légal et réglementaire cohérent est également indispensable pour assurer la confiance dans le *Cloud*.

Et de ce point de vue, l'UE semble avoir pris le taureau par les cornes. *« L'Europe a mis un principe assez fort qui, je pense, fait consensus, qui est de dire la protection des données des Européens doit être garantie en tous lieux et en tout temps »*, se félicitait encore Bertrand Pailhès. Le RGPD, très protecteur des données personnelles, est ainsi élevé au rang de norme *de facto* sur laquelle les autres régions du monde sont invitées à s'aligner.

C'est le sens de l'arrêt « Schrems II », que la Cour de justice de l'Union européenne (CJUE) a rendu le 16 juillet 2020. Estimant que la protection des données personnelles aux États-Unis n'était pas au niveau, la CJUE a cassé le « *Privacy Shield* », le régime de transferts de données qui existait entre Washington et Bruxelles. Problème : aucun accord de substitution n'a été mis en place et le marché n'est pas prêt, selon le directeur des technologies et de l'innovation à la CNIL.

« La décision de la CJUE "Schrems II", c'est à partir du 17 juillet. À partir de demain, il est interdit de transférer les données vers les États-Unis. Il n'y a pas de période de mise en conformité », déplorait Bertrand Pailhès lors du Forum InCyber. *« C'est parfois complètement irréaliste de penser que parce qu'un juge à Luxembourg a décidé que le marché n'était pas conforme aux droits fondamentaux, tout le monde allait se mettre d'accord avec ça »*, ajoutait-il. Et le régulateur doit dans ce cas faire preuve de souplesse le temps qu'assez *« de solutions alternatives (sic) émergent »*.

Micmac législatif

Le législateur européen est donc plein de bonnes intentions, mais celles-ci ne se heurtent parfois au réel… À moins que ce ne soient des *« questions réglementaires qui soient, d'une certaine manière, complètement opposées les unes aux autres »*, relevait Peter Sund, pour qui *« il est toujours délicat d'arriver à un équilibre »* entre des objectifs contradictoires. Ainsi, la protection des données personnelles et les pouvoirs accordés à la police et à la justice pour enquêter sont-ils antinomiques. Il a pris l'exemple du dispositif baptisé *« un meilleur Internet pour les enfants »*, destiné à lutter contre la pédopornographie.

Pour ce faire, la Commission européenne prévoit que les autorités puissent avoir accès aux photos et autres matériels hébergés par les fournisseurs de services en ligne, notamment les messageries chiffrées. Alors que la sécurité du *Cloud* repose en bonne partie sur le chiffrement des données, cette mesure le ferait voler en éclats. *« Cela risque de semer la confusion et de créer une situation qui va à l'encontre des objectifs du Cloud »*, s'inquiétait Peter Sund, tout en reconnaissant l'importance de la lutte contre la pédocriminalité.

De fait, soulignait Bertrand Pailhès, les États-Unis se sont appuyés sur une législation robuste pour développer le *Cloud* : *« Elle a été lancée il y a dix ans, elle est hyper complète, le secteur est hyper réglementé et ça, et ça a permis en fait à l'écosystème américain du Cloud d'émerger, parce qu'il avait des règles claires sur ce qui était attendu de lui. »*

« L'Europe doit créer des champions »

Ce cadre favorable n'est que l'une des expressions d'une volonté politique forte, a abondé Solange Viegas Dos Reis : *« quand on voit aujourd'hui les champions du Cloud comme les Américains ou les Chinois, on se rend compte que ce sont des champions qui se sont renforcés sur leur marché domestique avec un très fort soutien étatique, en ayant des marchés publics, en requérant des financements et des soutiens à la recherche. »*

Une volonté qui a longtemps fait défaut de ce côté de l'Atlantique, tant le credo libéral (aucun coup de pouce ni entrave au marché) de la Commission restait fort. Mais cela pourrait changer: *« nous soutenons le "Buy European Act", qui permettrait d'avoir un soutien concret, financier, de donner à tous les acteurs du Cloud les moyens nécessaires à leur développement »*, lançait encore Solange Viegas Dos Reis.

Il serait temps que les lignes bougent, estimait d'ailleurs le CEO d'Orange Cyberdefense France. *« L'Europe doit créer des champions dans ce domaine »*, plaidait Hugues Foulon, qui soulignait de plus que la question ne s'arrêtait pas là. Le *Cloud*, ce n'est pas que des *data centers*, ce sont aussi des solutions logicielles en évolution rapide, de la cybersécurité, de la maintenance, bref, tout un environnement. Et selon lui, *« l'Europe n'a pas tout à fait conscience de ces gros enjeux de formation »*. Le continent manque encore de développeurs et d'experts en tout genre et sans ces compétences, *« ça sera compliqué de faire marcher un écosystème Cloud stratégiquement autonome »*.

« On va avoir du mal à créer "from scratch" un écosystème aussi performant que celui des leaders du marché. Je pense que c'est une aventure qui se compte plutôt en décennies », avertissait Hugues Foulon, qui plaidait pour une approche pragmatique, à l'exemple du partenariat entre « Bleu » et Microsoft. Sera-t-il même un jour possible de faire sans les GAFAM ? Les professionnels européens veulent y croire.

LIRE L'ARTICLE EN LIGNE

L'Europe n'a pas tout à fait conscience de ces gros enjeux de formation.

Cloud : l'Europe est-elle en retard ?

SOUVERAINETÉ NUMÉRIQUE

MARC AUXENFANTS

Pour faire et réussir sa révolution face à ses concurrents, l'UE doit se ressaisir, constituer un écosystème commun, renforcer sa résilience et ses régulations. Mais aussi et surtout croire en ses atouts, talents et compétences.

« Énormes enjeux financiers, vision d'investissements et de rentabilité à long terme, poursuite d'une détermination ciblée pour réussir, et recherche constante de l'excellence opérationnelle… ». Telles sont les conditions qui s'imposent aux aspirants leaders sur le marché mondial du *Cloud*, selon John Dinsdale, analyste en chef de Synergy Research, un groupe américain de recherches et d'études. Toutefois, *« aucune entreprise européenne ne s'est approchée de cet ensemble de critères et les six leaders sont tous des entreprises américaines »*, relève-t-il.

À eux trois, Amazon, Microsoft et Google occupent désormais 72% d'un marché *Cloud* UE qui pèse aujourd'hui 10,4 milliards d'euros. Tandis que leurs principaux concurrents européens, notamment OVH*Cloud* et Orange, ne représentent chacun que 2% de parts du gâteau.

Quels défis l'Europe doit-elle donc relever ? Quelles solutions doit-elle aussi déployer pour combler ses lacunes ? Jean-Claude Laroche, président du Cigref, explique ce retard par l'insuffisante implantation des acteurs européen sur le marché du *Cloud* : *« Nous sommes dans une situation de dépendance préjudiciable à tout point de vue, vis-à-vis de ces hyperscalers américains. Aussi bien pour protéger nos données et traitements, que sur le plan financier et que dans nos relations commerciales avec ces acteurs. Le défi est donc d'avoir nos champions industriels ! »*, précise-t-il.

« Il n'y a pas de temps à perdre ! »

Pour Michel Paulin, patron d'OVH*Cloud*, le retard n'est toutefois pas technologique : *« Si on prend l'ensemble des écosystèmes des acteurs européens dans les domaines de la cybersécurité, du Cloud et du logiciel, aujourd'hui, nous avons toutes les briques pour avoir des champions. Mais nous n'avons peut-être pas des acteurs de tailles aussi importantes que les chinois et américains, qui peuvent faire du 'one-stop-shopping', avec l'avantage de disposer d'un seul point concentrant la totalité des solutions. »*

L'Europe peut-elle (encore) s'imposer comme une actrice incontournable du *Cloud* ? Selon Thierry Breton (Commissaire européen pour le marché intérieur), la solution passe tout d'abord par la résilience : *« Alors que nous construisons un marché intérieur de la donnée industrielle, le Cloud est une question de souveraineté numérique et industrielle. L'Europe doit plus que jamais garantir le développement d'un espace numérique sûr et de confiance. Nous devons pour cela avoir des systèmes de gestion de données innovants, mais sécurisés. Nos partenaires rivaux systémiques investissent massivement. Il n'y a donc pas de temps à perdre ! »*

Le monopole des *hyperscalers* américains pose aussi la question de la transparence entre les fournisseurs de *Cloud* et les clients, estime Shahmeer Amir, hacker éthique pakistanais. Pour y répondre, il suggère que l'UE impose une transparence claire et forte, à travers une réglementation solide sur la protection des données, en particulier pour l'environnement *Cloud*. *« Ces cadres juridiques garantiront alors que toute cette infrastructure Cloud est surveillée, et qu'elle sera en mesure de résoudre ces problèmes en toute sécurité »*, assure-il.

« L'Europe doit être stratège »

Pour assurer une protection efficace et sécurisée de la propriété intellectuelle et des informations sensibles, Shahmeer Amir prône une politique européenne garantissant à la fois une diversité et une concurrence saine et perspicace entre les fournisseurs *Cloud* : *« Monopole implique manque de transparence. Et s'il y a un manque de transparence, les informations et données sensibles peuvent être piratées ou divulguées. »*

Pour Jean-Claude Laroche, un *Cloud* de confiance paneuropéen est donc nécessaire. Il doit garantir quatre exigences fondamentales : *« équilibrer la relation avec le prestataire, transparence, portabilité des solutions et interopérabilité ; avoir des solutions sécurisées sur le plan cyber ; avoir des solutions qui répondent à des problématiques sociétales, environnementales, maîtriser l'aspect environnemental du numérique dans le Cloud ; se protéger contre les ingérences des services de renseignement extra-européens. »*

Des impératifs listés dans le référentiel développé par le Cigref, et repris dans la certification française SecNumCloud. *« Nous souhaitons désormais qu'il y ait des exigences équivalentes au niveau européen. C'est absolument impératif si nous voulons un Cloud de confiance européen doté d'un haut niveau de certification et de cette protection contre l'extra-territorialité »*, préconise Jean-Claude Laroche.

Pour Michel Paulin, les exigences européennes de traçabilité et de transparence, notamment de l'EUCS et du *Digital Market Act*, offrent aux opérateurs européens un avantage concurrentiel pour le bénéfice des clients. Et en matière de protection des données, l'Europe est aussi clairement leader.

Comment toutefois créer un écosystème commun capable de rivaliser avec la Chine, les États-Unis, la Corée ou Israël ? *« Ces pays ont créé des champions, avec un État stratège qui a su définir une ambition à long terme et instaurer une réglementation, des certifications, des financements pour l'accompagner. Dans tous ces domaines, l'Europe doit être stratège »*, détaille-t-il.

Aussi il faut, selon lui, définir des financements : *« Faute de Nasdaq, il s'agit d'aider les entreprises à se doter de fonds propres et d'une capacité de financement pour se développer. L'IPCEI (Important Projects of Common European Interest) est un des mécanismes qui le permettra. »*. Il faut aussi développer les commandes publiques et privées (des grands groupes), pour déployer cet écosystème européen ; renforcer la recherche et le développement fondés sur des échanges public-privé, à l'image des Stanford, Harvard et MIT, et résoudre la pénurie de talents.

« Nous n'avons pas suffisamment d'ingénieurs en Europe. Et donc plutôt que de disperser nos subventions, autant les réinvestir dans les universités, pour former plus d'ingénieurs et de doctorants qui auront intérêt à rester sur le territoire européen », plaide Michel Paulin.

« La bataille n'est pas perdue »

Pour Shahmeer Amir, sensibiliser les gens, les utilisateurs, les entreprises et le gouvernement est fondamental : *« Bien souvent nous pensons que nous savons, mais ce n'est pas le cas. Aussi, il est toujours bon de se réunir autour d'une table, de poser des questions, d'écouter et puis de reprendre et combiner tous ces besoins et attentes dans une politique vérifiée, reconnue par au moins 90% des gens, qui sera ensuite appliquée. »*

« L'Europe doit se ressaisir. C'est une nécessité absolue. Il faut qu'il y ait au niveau européen une vraie stratégie et une vraie politique industrielle, qu'on se fixe des priorités et qu'on s'y tienne ! », *ajoute Jean-Claude Laroche. Toutefois pour Alain Issarni, président exécutif de NumSpot, la bataille n'est pas perdue : « Il y a les fatalistes et il y a ceux qui ne savent pas qu'elle est perdue : ce sont ces derniers acteurs qu'il faut viser ! »*

Il suggère donc de commencer petit, avec une ambition extrêmement forte : *« L'Europe veut-elle faire sa révolution Cloud ? J'espère que oui. Peut-elle la faire ? Assurément oui. Peut-elle faire l'économie d'une telle révolution ? Non. Nous devons donc faire émerger des alternatives crédibles dans le monde du Cloud et participer à cette révolution. Sinon, celle-ci se fera sans nous ! »*

LIRE L'ARTICLE EN LIGNE

Alors que nous construisons un marché intérieur de la donnée industrielle, le Cloud est une question de souveraineté numérique et industrielle.

EUROPEAN CYBER CUP

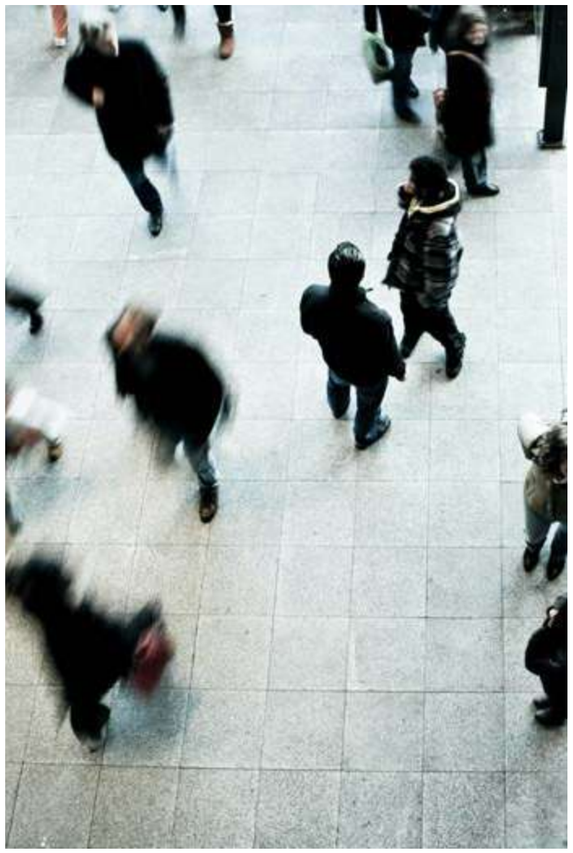
25 équipes 250 joueurs 6 épreuves

5 & 6 AVRIL 2023

Face aux cybermenaces, l'Europe s'organise, selon Thierry Breton

SOUVERAINETÉ NUMÉRIQUE

FABRICE DEBLOCK



Lors du Forum InCyber 2023, le commissaire européen en charge du Marché intérieur est intervenu en séance plénière. Il a détaillé l'ensemble des mesures prises depuis sa prise de fonction il y a maintenant trois ans.

À l'occasion de son discours, Thierry Breton a tout d'abord rappelé que les enjeux de cybersécurité ne peuvent aujourd'hui être adressés qu'au niveau européen et non plus au niveau d'un seul État membre.

Il a également souligné le fait que le *« marché numérique intérieur européen »* était le premier du monde libre, démocratique : *« Ce marché numérique intérieur dispose désormais d'une organisation et de règlements très structurants, comme le DSA, le DMA et le Data Act. Pour la première fois, nous avons un marché unique de la donnée fonctionnant avec des règles identiques pour tous. »*

Pour Thierry Breton, la révolution des données industrielles sera une vague bien plus importante encore que celle liée aux données personnelles. *« Cela va générer un nombre beaucoup plus important de données qui vont être à la base des évolutions qui sont devant nous, avec des métiers et des services nouveaux à la clé »*, a-t-il déclaré. Mais dans ce domaine, nous sommes aussi forts que le maillon le plus faible de la chaîne. Notre cyber-résilience ne peut donc devenir qu'un sujet éminemment européen.

« L'Europe à 27, en tant qu'acteur politique, économique mais aussi de sécurité globale, devient une cible croissante pour les attaques cyber de toutes natures, avec l'objectif - pour ceux qui sont derrière ces attaques - de déstabiliser nos systèmes », a ajouté Thierry Breton.

Le cyberespace fait désormais partie intégrante de la doctrine de défense européenne

Le commissaire en charge du Marché intérieur a par ailleurs précisé que la cybersécurité était désormais reconnue dans la nouvelle doctrine de défense européenne comme un des espaces contestés, au même titre que les espaces maritimes ou l'espace en tant que tel. Comme tout espace contesté, il nous appartient de le protéger en commun.

« C'est un changement de paradigme majeur. L'espace cyber fait dorénavant partie de notre doctrine de défense. Pour mieux gérer la menace cyber, nous avons besoin de technologies de pointe, d'infrastructures sécurisées communes, d'une coopération opérationnelle et de structures de gouvernance accrues, ainsi que de sanctions effectives », a-t-il noté.

C'est dans ce contexte que l'ambition portée par Thierry Breton s'organise autour de la mise en place d'un bouclier européen dont la vocation est de protéger, détecter, défendre et dissuader.

Technologie et réglementation, les deux piliers de la protection

Le volet « protection » s'organise autour d'un objectif clair : augmenter le niveau de résilience et de sécurité au sein du marché numérique intérieur européen, grâce à une approche technologique et réglementaire ambitieuse.

« Sur le plan technologique, nous travaillons au déploiement d'une feuille de route claire afin de pouvoir cartographier nos dépendances en matière de cyber, mais aussi de concentrer les financements européens nationaux au travers notamment du Fonds européen de défense », a précisé Thierry Breton.

Sur le plan réglementaire, la directive NIS a permis de mettre en place des exigences de cybersécurité sur l'ensemble des acteurs économiques essentiels dans les secteurs critiques, notamment dans les *datacenters* et les administrations publiques.

Autre composant réglementaire clé : le *« Cyber Resilience Act »*, proposé par Thierry Breton en novembre 2022. *« Ce texte met en place des exigences de cybersécurité minimales pour tous les produits et logiciels qui seront placés sur le marché intérieur. Pour 90 % des produits, il sera possible de faire des auto-déclarations de conformité. Mais pour une trentaine de produits les plus critiques, comme les pare-feux industriels, les routeurs ou les systèmes d'exploitation, nous avons défini un examen de conformité qui sera effectué par des tiers »*, a détaillé le commissaire européen.

Détection et défense renforcées

Sur le volet « détection », Thierry Breton a rappelé l'objectif de réduire drastiquement le temps de détection d'une attaque, afin qu'il soit, à terme, de quelques heures seulement et non plus de plusieurs mois (190 jours en moyenne pour les attaques sophistiquées).

À ce titre, la Commission européenne a proposé, en avril dernier, le *« Cyber Solidarity Act »*. Ce texte permet la mise en place d'une infrastructure de six ou sept SOC *(Security Operations Centers)* dans le but de créer une détection globale au niveau européen. *« En matière de gouvernance, ce 'cyber shield' sera un peu notre Galileo du cyber, en référence à notre architecture de connectivité et de positionnement par satellite Galileo »*, a-t-il déclaré.

Sur la partie « Défense », Thierry Breton a rappelé l'importance du « mécanisme d'urgence cyber » qui sera lui aussi porté par le *Cyber Solidarity Act*. Ce mécanisme reposera sur des principes de gestion de crise commune et d'assistance mutuelle. Il s'inspirera notamment du fonctionnement des protections civiles européennes qui, en cas de désastre majeur (incendie, tremblement de terre…) dans un pays de l'UE, lui viennent en aide de manière solidaire.

« Il s'agit d'un bras réactif qui reposera sur une réserve de plusieurs milliers d'intervenants pour engager des prestataires de service public ou privés, certifiés et de confiance, sur la base du volontariat, afin de soutenir tout effort de défense et de mobilisation face à une attaque. Cette réserve se tiendra prête à intervenir à la demande de tout État membre », a-t-il expliqué.

Une politique de sanctions actives et directes pour une meilleure dissuasion

Enfin, pour devenir un acteur global crédible au niveau continental de la cybersécurité, voire de la cyberdéfense, l'Europe doit pouvoir se doter d'une véritable doctrine en matière de cyberattaque et de cyberdéfense. *« Il s'agit d'accroître notre posture de dissuasion européenne en matière de cyber. Or, il n'y a pas de cyberdéfense sans capacité de dissuasion. Cette posture doit s'accompagner d'une politique de sanctions actives et directes. L'UE s'est déjà dotée d'une diplomatie cyber permettant d'établir des sanctions très fortes, en particulier quand l'attribution est bien qualifiée »* a exposé Thierry Breton.

Et le commissaire européen en charge du Marché intérieur de conclure : *« Mais toute dissuasion, pour être crédible, doit être accompagnée d'une véritable stratégie sur les capacités de réponse active, c'est-à-dire offensive, qui restent à la main des États membres. Nous avons mobilisé des moyens très importants, notamment dans le Fonds européen de défense, pour intervenir en amont et aider les États membres à financer des technologies clés. »*

Face aux menaces, l'Europe s'organise donc technologiquement, au niveau réglementaire, en matière d'infrastructures communes et de solidarité pour sa capacité de défense et de dissuasion. Elle intègre dans sa démarche l'ensemble des États membres mais aussi ses alliés de l'OTAN, au premier rang desquels se trouvent les États-Unis.

LIRE L'ARTICLE EN LIGNE

Il n'y a pas de cyberdéfense sans capacité de dissuasion.

Confiance dans le numérique : *« On ne peut plus en croire ses yeux »*

TRANSFORMATION NUMÉRIQUE

FABRICE DEBLOCK

Réseaux sociaux, IA, *big data*… Le numérique a bouleversé les structures sociales et mis à mal leur ciment, la confiance. Comment la redéfinir ? Lors d'une plénière du Forum InCyber, Jean-Gabriel Ganascia, Michel Bauwens et Éric Salobir ont convoqué l'histoire, la philosophie, la sociologie et leur expertise du digital pour répondre à cette question. Synthèse.

Quand trois intellectuels s'emparent du sujet de la confiance dans le numérique, le résultat ouvre des perspectives vertigineuses. Pour ceux qui n'ont pas eu la chance d'assister aux deux heures de plénière du Forum InCyber 2023 consacrées à ce thème, inCyber vous en offre un condensé. Nous laissons la parole à Jean-Gabriel Ganascia, professeur à la Sorbonne et président du comité d'éthique du CNRS, Michel Bauwens, informaticien et cyberphilosophe et Éric Salobir, prêtre et fondateur du réseau OPTIC, qui vise à promouvoir la technologie au service de l'humain et du bien commun.

Jean-Gabriel Ganascia : La confiance est-elle soluble dans le numérique ? C'est ambivalent, cela peut signifier *« est-ce que la confiance soluble disparaît dans le numérique ?. »* Donc il y a plus de confiance ou au contraire est-ce que cela veut dire qu'on veut faire un numérique de confiance ? Attention, la confiance, ce n'est pas la fidélité et ce n'est pas non plus la preuve : quand on a confiance en quelqu'un, on court le risque de se tromper. Il y a plusieurs types de confiance. Il y a la confiance dans les individus, il y a la confiance dans les institutions et puis il y a la confiance dans les machines.

Éric Salobir : En effet, et toute la difficulté dans le numérique de confiance, c'est d'être capable de susciter les conditions d'une confiance dans des choses que l'on ne voit pas, alors que par définition, on a toujours tendance à faire confiance en ce qu'on voit. Or, avec l'IA générative, par exemple, on se rend compte que l'on peut dire *« je n'en crois pas mes yeux »* et de fait, on ne peut plus en croire ses yeux. Le numérique a complètement bouleversé les conditions de la confiance.

Michel Bauwens : Au fur et à mesure que la société s'est complexifiée, l'homme a perdu la possibilité d'accorder sa confiance à son entourage, ses connaissances directes, le fameux Dunbar number.

Avec la *blockchain*, confiance distribuée

Aujourd'hui, on en est revenu dans un pair-à-pair, mais différent : on est dans la coordination non territoriale. On doit faire confiance en des gens avec qui on a une affinité de projet, de croyance, mais qui ne sont pas à côté de chez nous. Donc on est obligé de nous connecter avec nos pairs par des plateformes propriétaires pour lesquelles on est plus ou moins du bétail à extraire des data. Et donc c'est fondamental. Il n'y a pas d'institution qui représente cette nouvelle sociologie. Nous avons des institutions qui sont essentiellement géographiques, comme l'État-nation.

É. S. : la question, c'est pourquoi ces *business models* ont émergé. Finalement, on n'était pas prêt à être client, donc on est devenu produit. Et la question c'est *« comment est-ce qu'on va penser les nouveaux business models ? »*

J.-G. G. : Dans l'Antiquité la confiance, c'était la parole, un témoin valait plus qu'un écrit. Puis à mesure que les groupes se sont étendus, c'est devenu l'écrit. Désormais, la transformation majeure, c'est que cela va être la machine. Et avec la *blockchain* par exemple, on va avoir de nouveaux types de confiance et ce sont en plus des confiances distribuées parce qu'elles ne font plus référence à un tiers de confiance, à une institution, à une banque centrale pour la monnaie, à un État.

É. S. : Ce qui est gênant, c'est que cette confiance dans la machine s'opère au détriment d'une confiance dans l'humain : *« faites confiance dans la blockchain, comme ça vous n'avez plus à faire confiance à votre voisin »*.

ChatGPT, avatar du *« veau d'or »* ?

La confiance qu'on avait dans la monnaie fiduciaire de « fides », la foi, c'était à la fois la confiance dans la personne et dans l'économie, le groupe. Tout ça, ça disparaît dans une perspective assez Hobbsienne : si l'homme est un loup pour l'homme, je préfère passer par la blockchain.

Comment va-t-on bâtir une société sur ce genre de technologie ? Comment va-t-on tirer profit de ces technologies ? Je n'ai pas envie qu'à un moment le smart contract finisse par avoir la peau du contrat social.

J.-G. G. : Quand je parlais de la *blockchain*, il ne s'agissait pas de la confiance dans la machine, mais de la confiance par la machine. La confiance en la machine, c'est ChatGPT, qui est perçu comme un oracle. Il a un statut particulier, celui de la divination. Quand on vous dit *« j'ai consulté ChatGPT »*, c'est exactement de cela qu'on parle.

É. S. : Oui, on anthropomorphise cette machine en lui posant des questions. Elle semble dotée de parole, avec un décalage entre une perfection formelle – elle parle bien, donne l'impression d'être argumentée – et son absence complète de sens commun. ChatGPT peut raconter n'importe quoi, c'est un baratineur, mais ce n'est pas un problème. L'homme projette sa confiance dans l'IA comme le peuple avait fait son dieu du veau d'or dans la tradition hébraïque. Ce n'étaient pas les orfèvres qui en avaient fait une idole, mais les gens. Allons-nous collectivement bâtir le même rapport à la technologie ?

Les GAFAM, ces firmes « captalistes »

M. B. : Pour éviter cela, il faut construire de nouvelles institutions qui correspondent à cette réalité virtuelle. Dans le monde open source, on est en fait en train d'en créer, comme les FLOSS Foundations, qui gèrent l'infrastructure collective, non territorialement et souvent de façon démocratique. Je pense par exemple à la Linux Foundation. J'appelle cela des magistères du commun. Cela pourrait s'appliquer aussi à la *data*, avec des *data trust*, des *data commons* et des *data cooperative*, pour échapper en partie aux GAFAM, ces firmes « captalistes », qui captent notre attention et nos données.

É. S. : On constate en effet un appauvrissement des institutions préexistantes tandis que les nouvelles peinent à se mettre en place. Ces fondations sont formidables, mais malheureusement, elles sont trop à la marge. Pour créer de nouveaux tiers de confiance, je pense qu'il faut trois caractéristiques. La première, c'est l'indépendance, y compris financière, ce qui manque aux fondations libres.

La deuxième, c'est la transparence, que des experts puissent vérifier les algorithmes, les métaprompts dans ChatGPT ou l'utilisation de nos données. Et le troisième, c'est que cette gouvernance soit participative. Et là, monsieur, je vous rejoins largement. Le problème, c'est que nous nous situons à l'échelle mondiale. Ce ne sera pas un mais des tiers de confiance. La question est donc : *« quelle sera l'architecture nécessaire pour qu'ils puissent se parler tous ? »*

Réseaux sociaux et psychologie des foules

J.-G. G. : Ces piliers que vous avez énoncés me semblent tout à fait essentiels. La confiance se réécrit complètement dans nos sociétés numériques et c'est à nous de redéfinir tous les critères. Vous évoquiez la donnée. La difficulté, c'est qu'elle peut être dupliquée, falsifiée. Il faut donc réfléchir aux procédures que l'on va mettre en œuvre pour, indépendamment de son caractère extrêmement fluide, reconstituer la confiance.

M. B. : Au-delà de ces enjeux, je crois que nous devons introduire la notion de civilité en ligne, parce que le monde virtuel est très fragmenté. Chacun est dans sa petite tribu d'affinités qui a accès à des informations différentes. Chaque communauté se bat contre les informations qui viennent d'une autre tribu. On ne peut pas créer une société avec cette dynamique.

J.-G. G. : Nous avons bien des communautés, mais non plus au sens ancien, des communautés de personnes condamnées par le destin à vivre au même endroit, avec un devoir de solidarité. Aujourd'hui, ces communautés en ligne sont des communautés d'intérêts. Le problème, c'est la délibération collective. Au sein de ces groupes, on retrouve les concepts de la psychologie des foules de Gustave Le Bon et Freud. Un homme raisonnable devient au sein d'une foule ou d'un réseau social susceptible, agressif, s'enthousiasme d'un rien, etc. Il n'y a plus un espace public mais il y a des espaces qui sont entre le public et le privé.

Covid-19, une crise de confiance *« douloureuse pour les scientifiques »*

É. S. : Nous sommes passés d'un monde d'identité reçue *(« je suis untel, fils d'untel »)* à un monde d'identité choisie et de multi-identités. Chacun creuse son propre sillon. Si cela donne beaucoup de liberté, cela se fait un peu au couteau et contribue à cette dimension assez agitée, violente de l'espace public.

J.-G. G. : En témoigne la crise du covid, durant laquelle la confiance s'est effritée et nous autres, scientifiques, l'avons ressenti particulièrement douloureusement à l'époque.

Le scientifique par nature, c'est quelqu'un qui doute, mais on était ici face au grand public qui mettait le scientifique en situation d'otage de son propre doute. Il disait que si on n'était pas capable d'affirmer, c'est qu'on ne savait pas, etc.

M. B. : Je ne voudrais pas être trop négatif, mais on est entrés dans une ère de surveillance digitale. Quand je suis sur Facebook, je me sens comme en Chine, c'est-à-dire qu'on ne peut même plus partager des articles scientifiques, ils sont filtrés.

Il y a d'un côté les medias qui sont « monothéistes », dans le sens où ils suivent un narratif dominant et en ligne, les contrôles algorithmiques vous contrent. Même si on a une impression de fragmentation, on a vraiment de grandes difficultés aujourd'hui à avoir la parole. Et le danger, évidemment, quand il n'y a pas de parole, c'est la violence. Va-t-on s'en sortir comme les Romains, par la désagrégation de nos structures ou va-t-on réussir comme au XVI[e] siècle, où on a trouvé une solution capitale, l'État-nation ?

Médias « monothéistes » contre l'Internet « fragmenté »

J.-G. G. : Au-delà de cette fragmentation par groupes au sein des sociétés, le numérique fait aussi apparaître des clivages entre zones culturelles. J'ai par exemple participé au comité d'éthique de l'Unesco au moment où elle a mis en place l'éthique de l'intelligence artificielle. J'ai donc lu un certain nombre de chartes et je peux vous dire que les conceptions européennes ne sont pas les conceptions américaines ou chinoises.

É. S. : Tout à fait. Pour les Chinois, le mal absolu c'est le chaos, ce n'est pas la dictature et cela en dit beaucoup sur leur organisation sociale. Les Américains ont une vision très conséquentialiste. En gros, s'il n'y a pas de class action possible, tout va bien. En Europe, on applique le principe de Kant, *« la maxime de vos actes est maxime universelle »*, ce que vous faites, il faudrait que vous ayez envie que tout le monde le fasse.

M. B. : Même le système technologique est en train de se scinder en deux. Huawei ne peut plus investir ici, les Américains ont une loi qui punit les Américains qui travaillent pour les microchip en Chine jusqu'à quinze ans de prison. Même Internet est en train de se scinder.

À réinventer au niveau national et régional, la confiance dans le numérique au niveau global semble donc des plus hypothétiques.

LIRE L'ARTICLE EN LIGNE

Chaque communauté se bat contre les informations qui viennent d'une autre tribu. On ne peut pas créer une société avec cette dynamique.

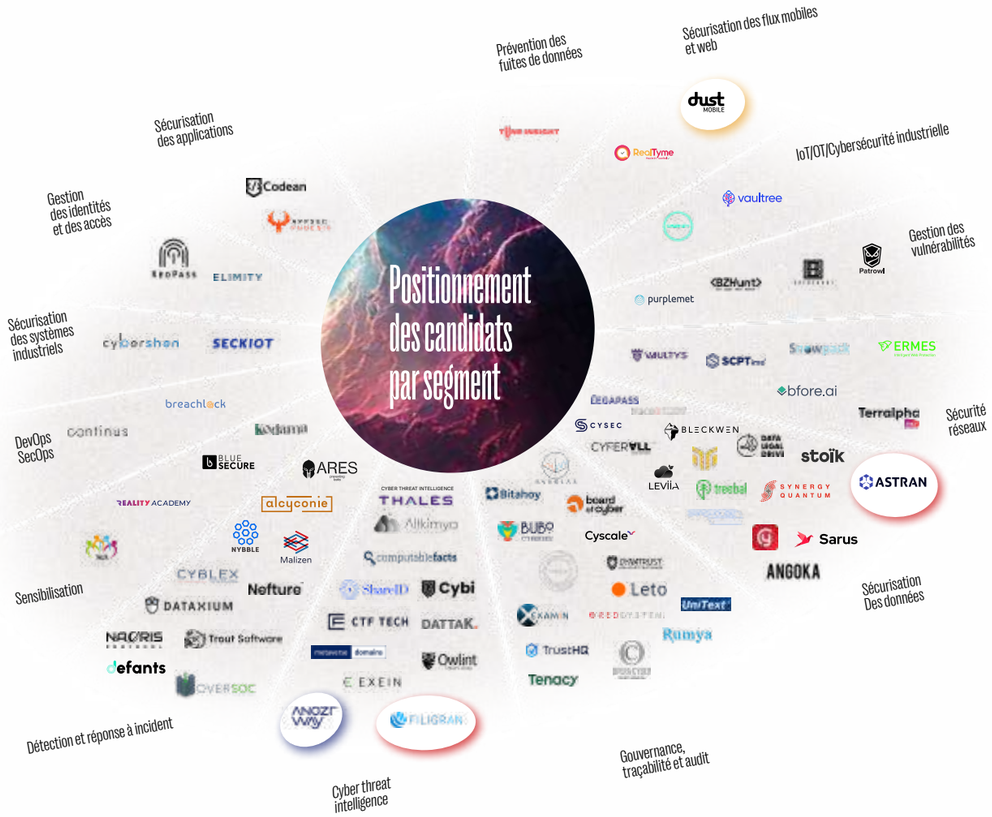
baromètres & panoramas

Panorama de l'innovation cyber

PRIX START-UP Forum InCyber 2023

Les informations présentées dans ce panorama ont été collectées auprès des 81 sociétés candidates à ce prix. Organisé en partenariat avec Atos et avec le soutien d'ECSO, il récompense chaque année les entreprises les plus innovantes dans le domaine de la cybersécurité.

Atos | ECS



Les candidats par segment

Sécurisation des données
16 candidats
↗ +3

Détection et réponse à incident
11 candidats
↗ +7

IOT / OT / Sécurisation des systèmes industriels
4 candidats
↘ -9

Gouvernance traçabilité et audit
15 candidats
↗ +2

Cyber Threat Intelligence
12 candidats
↗ +7

Sécurité réseaux
6 candidats
NOUVEAU SEGMENT

DevOps / SecOps
2 candidats
NOUVEAU SEGMENT

Prévention des fuites de données
1 candidat ↘

Sécurisation des applications
2 candidats
-5

Sécurisation des flux mobile et web
2 candidats
↗ +1

Gestion des vulnérabilités
4 candidats
NOUVEAU SEGMENT

Sensibilisation
4 candidats
NOUVEAU SEGMENT

Gestion des identités et des accès
2 candidats
-1

Les éléments présentés ici regroupent les principaux enseignements de ce panorama. Pour retrouver l'intégralité du document, rendez-vous sur **incyber.org**, le média de la communauté Forum InCyber.

Tendances

65 % de primo-candidats

+ 88 % de participation depuis 2019

3/4 des postulants ont eu une **croissance supérieure à 20 %** en 2022

71 % d'entre elles ont déjà réalisé au moins un tour de table

57 % envisagent de **lever des fonds** dans les six mois

56 % des entreprises ont moins de **dix salariés**

83 % des solutions proposées sont **SaaS/Cloud compatibles**

LE NOMBRE DE VIOLATIONS SE MAINTIENT À UN NIVEAU ÉLEVÉ

ÉVOLUTION DU NOMBRE DE VIOLATIONS

Chiffres-clés

+35 % de DPO
(délégués à la protection des données)

soit **17 432 personnes nommées**
à cette fonction clé

-3,11 %
repli des notifications enregistrées
Cette stabilisation peut être mise au crédit des organisations qui ont gagné en maturité en matière de cybersécurité.

x2
nombre de violations
entre 2019 et 2021

Après une très forte hausse du nombre de violations entre 2019 et 2021, on note un léger repli des notifications enregistrées sur la dernière année.

Focus

Après une très forte hausse du nombre de violations entre 2019 et 2021, on note un léger repli des notifications enregistrées (- 3,11 %) sur la dernière année. Cette stabilisation peut être mise au crédit des organisations qui ont gagné en maturité en matière de cybersécurité.

La médiatisation d'un nombre croissant de cyberattaques au rançongiciel affectant aussi bien des entreprises privées de toute taille que des hôpitaux ou des collectivités locales a accéléré la prise de conscience des dirigeants. Les organisations ont augmenté le budget dédié à la cybersécurité et relevé leurs niveaux de défense.

L'effort de protection ne porte pas seulement sur les investissements en logiciels et matériels. La politique de confidentialité des données personnelles est de plus en plus incarnée. Le nombre de délégués à la protection des données (DPO) a crû de 35 % en une année pour atteindre 17 432 personnes nommées à cette fonction-clé. Pour rappel, le RGPD rend obligatoire la désignation d'un DPO pour les organismes publics et les entreprises privées menant des traitements de données sensibles à grande échelle (Article 37).

En dépit de ces signes encourageants, le nombre de violations reste sur un palier particulièrement élevé. Avec la crise sanitaire, le niveau de menace est monté d'un cran, les cybercriminels profitant des vulnérabilités engendrées par la désorganisation des entreprises et la généralisation du télétravail. Le nombre de violations a plus que doublé entre 2019 et 2021. Cette pression ne semble pas avoir baissé depuis.

Les conséquences potentielles d'une fuite de données sont de nature diverse. Le premier risque porte sur l'utilisation illégitime des informations exfiltrées. Une telle usurpation peut prendre des formes variées et incontrôlées.

Une violation de données peut déstabiliser l'organisation d'une entreprise et entraîner une paralysie partielle ou totale de son activité. Ce qui génère une baisse de productivité et, *de facto*, une perte financière. Une organisation victime d'un rançongiciel n'est pas assurée, par ailleurs, de recouvrir l'intégralité de son système d'information.

Par ailleurs, la révélation d'une fuite de données nuit à la réputation d'une entreprise et peut affecter durablement la confiance placée en elle.

> La CNIL rappelle, en effet, qu'en cas de fuite de données « susceptible d'engendrer un risque élevé pour les droits et les libertés », l'organisme responsable a « l'obligation d'informer individuellement les personnes concernées du fait que leurs données ont été compromises et publiées en ligne. »

Enfin, une organisation s'expose à des poursuites juridiques de la part des personnes morales et physiques concernées par la violation de données et à une sanction, en cas de manquement grave et avéré, par l'autorité de contrôle. En l'occurrence la CNIL pour la France.

BAROMÈTRE
DATA BREACH

Almond BESSÉ CONSEIL EN ASSURANCES

Ce baromètre est animé par la revue stratégique *Cyberleaders* en partenariat avec Bessé et Almond et avec la participation de la CNIL.

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

L'année 2021 n'avait rien d'une exception. Si le nombre de violations de données à caractère personnel notifiées à la CNIL a connu un léger fléchissement (- 3,11 %) l'an dernier, il reste à un niveau particulièrement élevé. Après avoir profité de la désorganisation des entreprises et des acteurs publics durant la crise sanitaire, les cybercriminels continuent à exercer une menace constante, multipliant des campagnes toujours plus sophistiquées.

Pour les organisations victimes, une fuite de données n'a jamais rien d'anodin. Elle entraîne des conséquences plus ou moins lourdes sur les plans financier, opérationnel, réputationnel, judiciaire ou réglementaire. Se fondant sur les données publiées par la CNIL, ce baromètre entend évaluer le phénomène et ses conséquences.

2022, UNE NOUVELLE ANNÉE RECORD

[ANALYSE DES TENDANCES GLOBALES]

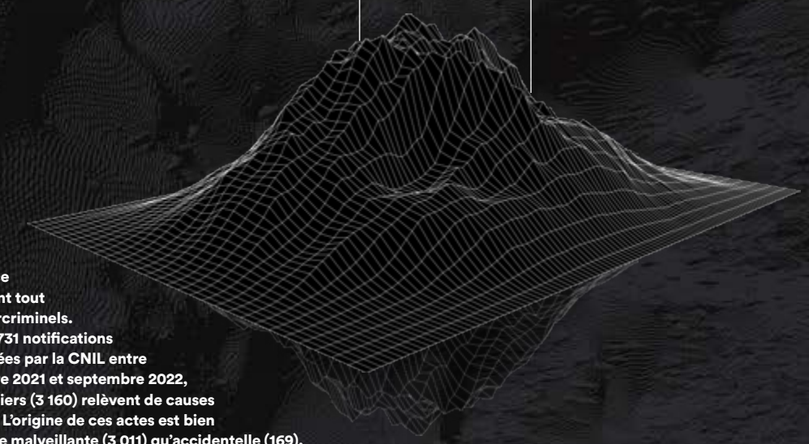
Avec près de 13 fuites de données par jour et 4 731 notifications d'incidents reçues par la CNIL l'an dernier, 2022 fait figure de nouvelle année record. En cumul, ces fuites de données à caractère personnel concernent un très grand nombre d'individus en France. En retenant, par hypothèse, le nombre moyen de personnes concernées par violation, on peut estimer qu'environ cinq millions de Français ont été impactés en 2022. Si la méthode n'a rien de scientifique, elle permet de mettre en évidence l'importance du phénomène.

Rappelons qu'une violation de données à caractère personnel est, selon l'article 4.12 du RGPD, constituée « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises (…) ou l'accès non autorisé à de telles données ».

Le RGDP introduit, par ailleurs, une obligation de notification par les responsables de traitement en cas de *data breach*. Ils doivent alerter la CNIL dans les meilleurs délais, si possible dans les 72 heures après en avoir pris connaissance. Le manquement à cette obligation peut entraîner une amende s'élevant jusqu'à 10 millions d'euros, ou 2 % du chiffre d'affaires annuel mondial de l'entreprise.

4 731
notifications à la CNIL de violations de données à caractère personnel

5 millions
de personnes concernées



La menace vient avant tout des cybercriminels. Sur les 4 731 notifications enregistrées par la CNIL entre septembre 2021 et septembre 2022, les deux tiers (3 160) relèvent de causes externes. L'origine de ces actes est bien davantage malveillante (3 011) qu'accidentelle (169). En revanche, la proportion est inverse concernant les 1 049 fuites dont l'origine est à trouver au sein d'une organisation. Les causes de ces actes internes sont majoritairement d'origine accidentelle (842) et non malveillante (207).

Ces données confirment, en chiffres absolus, que la cybercriminalité est principalement le fait d'individus extérieurs à une organisation. Un phénomène en hausse puisque, en un an, le nombre d'actes malveillants d'origine externe a progressé de 10,6 %. Les actes malveillants d'origine interne augmentent dans une proportion équivalente (+ 11,89 %). Ce qui doit interroger les organisations sur les processus à mettre en œuvre pour contrer ces « ennemis de l'intérieur ».

En ce qui concerne les actes internes d'origine accidentelle, on peut légitimement penser que la généralisation du télétravail, introduit depuis la pandémie de Covid-19, accentue les facteurs de risques. À leur domicile, les appareils des collaborateurs ne disposent pas du même niveau de protection que celui de leur entreprise.

Le télétravail a aussi pour effet d'abaisser le niveau de vigilance. Seuls devant leur écran et sans les conseils avisés de collègues présents sur le même plateau, les employés deviennent une proie plus facile des campagnes de *phishing*.

En revanche, le nombre de fuites « d'origine inconnue » a baissé de 49 % en un an. Alors qu'on fêtera, en mai prochain, les cinq ans de la mise en œuvre du RGPD, les entreprises et administrations ont visiblement gagné en maturité. Au fil des années, elles ont progressivement mis en place les outils permettant de tracer l'origine des incidents.

4 731
notifications

3 160
actes externes

1 049
actes internes

3 011
de nature malveillante

842
de nature accidentelle

LE SECTEUR DES SERVICES PARTICULIÈREMENT TOUCHÉ

ÉVOLUTION DU NOMBRE DE VIOLATIONS

Chiffres-clés

Le secteur des services administratifs et de soutien
concentrent près de

30 %
des violations de données

Viennent ensuite les
activités extraterritoriales
(ambasssades, consulats, institutions internationales)
qui représentent

10 %
des violations de données

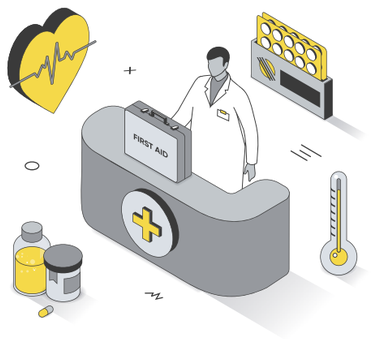
Les rançongiciels touchent particulièrement les
collectivités territoriales

23 %

et les
établissements publics de santé

10 %

Source : ANSSI



Focus

Un secteur d'activité concentre à lui, seul, près de 30 % du total des violations de données à caractère personnel. Il s'agit de celui des services administratifs et de soutien. Derrière ce code NAF de l'INSEE, on retrouve les activités liées à la location, aux voyages, à l'emploi, à la sécurité et plus généralement les sociétés de services aux entreprises.

Viennent ensuite, autour et sous la barre des 10 %, les activités extraterritoriales – à savoir les ambassades, les consulats ou les institutions internationales –, puis les établissements financiers et les compagnies d'assurance, les professionnels de l'immobilier, les cabinets juridiques, comptables ou d'architecture, les activités scientifiques et techniques.

Répartis entre différents secteurs d'activité, les acteurs publics sont particulièrement exposés. Dans son « Panorama de la cybermenace 2022 », l'Agence nationale de la sécurité des systèmes d'information (ANSSI) rappelle que les rançongiciels touchent particulièrement les collectivités territoriales (23 %) et les établissements publics de santé (10 %).

La liste est longue des acteurs publics victimes de cybercriminels. Parmi les cas médiatisés les plus récents, on peut citer les centres hospitaliers de Versailles et de Corbeil-Essonnes, l'Ehpad de Beuzeville, les mairies de Brunoy et de Chaville, les conseils départementaux de Seine-et-Marne et des Alpes-Maritimes.

Ces entreprises privées ou ces organismes publics ont pour point commun d'être en avance de phase dans leur transformation numérique. Revers de la médaille, la dématérialisation généralisée de leurs processus augmente mécaniquement leur exposition aux risques de fuite de données.

A contrario, les activités faiblement digitalisées comme la construction, l'hôtellerie-restauration ou l'industrie manufacturière n'ont à déplorer qu'un faible nombre de violations. Il est à noter qu'entre 2021 et 2022, l'ordre du classement reste inchangé. Le secteur des activités de services administratifs et de soutien conforte même sa première place avec une progression de 34 % en un an.

le Forum InCyber
en chiffres

FORUM INCYBER 2023

20 000	participants dont
+16 000	participants physiques uniques (+ 10,7%)
4 000	participants en ligne
2 700	internationaux
650	partenaires privés & publics
530	intervenants
+1 800	rendez-vous d'affaires via la plateforme de *networking*
82	pays représentés
11	minutes : durée moyenne de visionnage en ligne (+ 22%)
+700 000	vues sur les réseaux sociaux et 50 millions d'impressions sur le sujet

merci
à nos 650 partenaires !

PARTENAIRE PRINCIPAL

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

PARTENAIRES DIAMOND

EVIDEN THALES

PARTENAIRES PLATINIUM

AIRBUS Auvergne-Rhône-Alpes BRETAGNE LA CYBERSÉCURITÉ À SON TERRITOIRE Capgemini CROWDSTRIKE
DARKTRACE DOCAPOSTE EXCLUSIVE NETWORKS Orange Cyberdefense OVHcloud
Netherlands Région Nouvelle-Aquitaine SentinelOne sopra steria TEHTRIS

PARTENAIRES GOLD

abbakan Ovens AGORIA Arrow Five Years Out aws BITSIGHT blancco CAMPUS CYBER
COESING-ET-MARNE cisco cybereason CYBERSECURITY LUXEMBOURG EGERIE EURATECHNOLOGIES FLANDRIN TECHNOLOGIES FORTINET
FORTRA INFINIGATE IN GROUPE ITrust kaspersky LEXFO NeoYAD OneTrust
opentext paloalto pwc ORUM SecurNum GrandEst Région Hauts-de-France Région Occitanie CYBER'OCC SANS
Schneider Electric STORMSHIELD TANIUM TD SYNNEX tenable TREND MICRO txOne networks
XM Cyber YES WE HACK

crédits photos

Adam Jicha
Adrien Vin
Cash Macanaya
Christian Lue
Daniel Lincoln
Efe Kurnaz
FLY:D
Hesam Link
Kristaps AoM3
Maximalfocus
Nathan Watson
Nick Brunner
Romuald Charpentier
Shubham Dhage
Timon Studler

paris

LE FORUM INTERNATIONAL
DE LA CYBERSÉCURITÉ

DEVIENT

FORUM INCYBER EUROPE