LE MAGAZINE DES

PROFESSIONS FINANCIÈRES & DE L'ÉCONOMIE

#26
Mai 2023
ISSN 2431-2460

Cybersécurité : comment assurer la résilience du secteur financier ?

Franck Le Vallois,
Directeur Général de France Assureurs

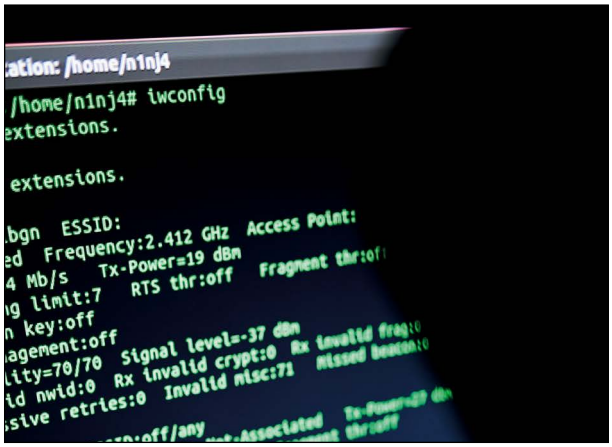
Centre des Professions Financières

Sommaire

Editorial

Dossier : Cybersécurité : comment assurer la résilience du secteur financier ?

Sommaire



Chronique Littéraire

Chronique de la Recherche

Vie du Centre

Édité par le Centre des Professions Financières : 41 boulevard des Capucines - 75002 Paris - Tél. : 01.44.94.02.55 - www.professionsfinancieres.com
Email : contact@professionsfinancieres.com - Présidente du Comité de Rédaction : Marie-Agnès Nicolet -
Rédactrice en Chef de la Publication : Marie-Agnès Nicolet - Secrétariat de rédaction : Catherine Chevassut,
Déléguée Générale du CPF, Noémie HASSON, Chargée de Mission Événementiel -
Conception graphique et mise en page : Studio C infographie Christelle Charlier, christelle@studioc-infographie.fr

MARIE-AGNÈS NICOLET,

Présidente de REGULATION PARTNERS, Présidente du comité magazine et membre du conseil d'administration du centre des professions financières

Cybersécurité : comment assurer la résilience du secteur financier ?

Le **règlement européen « DORA »** sur la résilience opérationnelle numérique du secteur financier vise à harmoniser et renforcer les exigences encadrant les risques opérationnels numériques des entités financières au sein de l'Union européenne. Il s'applique à partir du 17 janvier 2025.

Ce nouveau cadre de gouvernance s'appuie sur six piliers :

Une gouvernance renforcée : L'organe de direction est au cœur de la gestion des risques liés aux Technologies de l'information et de la communication (TIC). Il définit, approuve, supervise et est responsable de la mise en œuvre de toutes les dispositions relatives à la gestion des systèmes d'information.

Un dispositif de gestion des risques informatiques solide, complet et bien documenté intégré au système global de gestion des risques. Il détermine notamment le niveau de tolérance au risque informatique de l'entité financière en fonction de son appétit pour le risque et sa tolérance à l'incidence des perturbations informatiques.

Un processus de **gestion des incidents** permettant de détecter, gérer et notifier les incidents liés aux TIC.

Des **tests de résilience opérationnelle numérique** faisant partie intégrante du cadre de gestion des risques informatiques. Les entités financières soumettent tous les systèmes et applications informatiques essentiels à des tests au moins une fois par an.

Une **gestion des risques liés aux prestataires de services en matière de technologie de l'information et de la communication (TIC)**, encadrée par une stratégie soulignant les dépendances existantes à l'égard des prestataires. Une distinction est opérée entre ceux qui couvrent des services

TIC soutenant des fonctions critiques et ceux qui ne le font pas. Les Autorités européennes de supervision (ESMA, EBA, EIOPA) devront désigner les prestataires des services TIC critiques pour les entités financières, sur la base de critères définis par le règlement et ces prestataires seront directement supervisés par une autorité européenne de supervision.

Le **partage d'information** des entités financières entre elles dans l'objectif d'améliorer la résilience opérationnelle numérique.

Ce cadre est totalement nouveau car si les établissements de crédit, paiement, monnaie électronique et sociétés de financement, entre autres, devaient déjà suivre les orientations de l'Autorité bancaire européenne, ce texte sera à appliquer à l'ensemble des institutions financières européennes de la banque, assurances et asset management (avec des exemptions très réduites)

Et ceci se justifie évidemment par le caractère systémique des cybermenaces

Le centre des professions financières a donc souhaité approfondir le sujet en faisant s'exprimer dans ses colonnes des universitaires et d'autres nombreux experts de ce sujet, pour nous faire mieux comprendre ces nouvelles menaces et les anticiper.

Ce magazine complète donc les réflexions de la conférence organisée en juin 2022, qui avait pour vocation de mettre en exergue les réponses concrètes face aux nouvelles menaces et annonce la nouvelle conférence sur ce thème qui approfondira en 2023 certains aspects de la cyber prévention et résilience.

Nous vous souhaitons une excellente lecture.

Face au risque cyber, donnons-nous les moyens de protéger les Français

FRANCK LE VALLOIS,

Directeur Général
de France Assureurs

« Avec la guerre en Ukraine, les cyberattaques ont bondi l'an dernier de 140 % en Europe » a indiqué mercredi 5 avril 2023 dans le journal Les Echos Thierry Breton, commissaire européen au marché intérieur. Ce chiffre illustre bien l'enjeu que représente le risque cyber pour notre société, d'autant plus perceptible depuis le début du conflit russo-ukrainien. Les assureurs ont depuis plusieurs années identifié les cyberattaques comme une des principales menaces pour la société[1]. Un débat s'est d'ailleurs instauré sur l'assurabilité des cyberattaques. Et ce pour plusieurs raisons.

D'abord, pour une raison technique. Les cyberattaques peuvent-être assurables ?

Le risque cyber se caractérise par une sinistralité de fréquence mais également d'intensité. De plus, ces attaques sont susceptibles d'entraîner un sinistre majeur tels que certains acteurs ont pu en connaître par le passé (Saint Gobain, Altran…). Toutes les strates de la société peuvent être touchées : les grandes entreprises, les TPE et PME, les particuliers ou encore les établissements publics comme les hôpitaux.

Le phénomène est mondial. Par exemple, aux Etats-Unis, la *National Association of Insurance Commissioners* (NAIC), l'association des superviseurs américains, indique que les violations de données en 2021 sont supérieures de 68 % par rapport à 2020[2], tout particulièrement dans le domaine de la santé. Selon le rapport de l'ANSSI[3] « Panorama de la cybermenace en 2022 », la menace se maintient à un niveau élevé en 2022 en France. L'ampleur de ces cyberattaques et leur caractère potentiellement systémique questionnent la capacité des assureurs à pouvoir les couvrir. Or, le marché de l'assurance cyber est encore un marché naissant. En 2022, le marché français du risque cyber représente 327M € de cotisations soit seulement 0,5 % du chiffre d'affaires des assurances de dommages et responsabilité. C'est encore trop peu pour en faire un marché mature. A titre de comparaison, le marché de la cyber assurance aux États-Unis représente environ 6,5 milliards de dollars en primes directes souscrites, selon la NAIC, en augmentation de 61 % par rapport à l'année précédente. Par ailleurs, ce marché est très disparate : le taux de couverture des grandes entreprises en 2021 était de 84 % quand il est de 0,2 % pour les TPE, PME et micro-entreprises[4]. C'est le jour et la nuit.

Ensuite, pour une raison juridique. Les cyberattaques doivent-elles être assurables ?

Le phénomène rançongiciel a représenté près de 80 % des cyberattaques en 2020, selon le Sophos 2022 Threat Report. Le débat portant sur la légalité de la couverture assurantielle des remboursements des demandes de rançons a été vif en 2022. Il était donc urgent d'avoir une position claire. C'est, en substance, ce que pointaient différents

1/ Cartographie prospective des risques, France Assureurs, 2023

2/ *Report on the Cyber Insurance Market*, NAIC, 2022

3/ Agence nationale de la sécurité des systèmes d'information

4/ Enquête Lucy, Lumière sur la cyberassurance, édition 2022, AMRAE,

rapports sur le développement de l'assurance du risque cyber notamment celui du Haut Comité Juridique de la Place Financière de Paris (HCJP) ou encore de la Direction générale du Trésor. Ces rapports ont éclairé les débats sur l'indemnisation par l'assurance du remboursement des rançons payées par l'assuré en évoquant la possibilité de couvrir ce risque sous certaines conditions.
Ce fut utile.

La loi du 24 janvier 2023 d'orientation et de programmation du ministère de l'Intérieur a permis cette clarification très attendue par la profession. Elle a reconnu la licéité de l'assurance du remboursement des pertes liées à une cyberattaque en la conditionnant à une obligation de dépôt de plainte dans un délai de 72 heures.
Ce fut bienvenu.

Les cyberattaques peuvent donc être assurables. Nous pouvons nous en satisfaire. Pourquoi ? Prévoir une interdiction purement nationale de ce type de garantie aurait eu peu d'effet puisque aucun autre État membre de l'Union européenne n'a formellement interdit l'assurabilité du remboursement des rançons en cas de cyberattaque. Cela aurait donc nui au développement de l'assurance et aux mesures de prévention que mettent en place les assureurs, en laissant les cibles privilégiées de ce type d'attaques sans protection.

Car c'est bien là **l'objectif principal que nous devons collectivement atteindre : protéger.** Protéger les entreprises, notamment les TPE, PME et ETI qui sont la cible de 40 % des rançongiciels[5] et qui disposent de moyens largement inférieurs aux grands groupes. Protéger les particuliers, qui peuvent parfois estimer la menace plus lointaine ou incertaine. Enfin, protéger les établissements publics, à commencer par les hôpitaux : 10 % des cyberattaques frappent des établissements publics de santé selon le rapport de l'ANSSI en 2022.

Pour protéger, il faut sensibiliser. La sensibilisation doit être une priorité nationale pour favoriser la prise de conscience des Français. Un chiffre l'illustre : en 2022, 45 % des entreprises ont subi au moins une cyberattaque selon *OpinionWay*[6]. Or, cette étude révèle que le non-respect des fondamentaux dans les pratiques informatiques et les vulnérabilités résiduelles permanentes sont les principales causes des cyberattaques (38 % et 37 %

5/ Panorama de la cybermenace 2022, ANSSI, 2022

6/ Baromètre de la cybersécurité des entreprises, OpinionWay pour Cesin, janvier 2023

respectivement). Plus de la moitié des patrons de PME n'ont pas de référent sécurité informatique. Tout est dit.

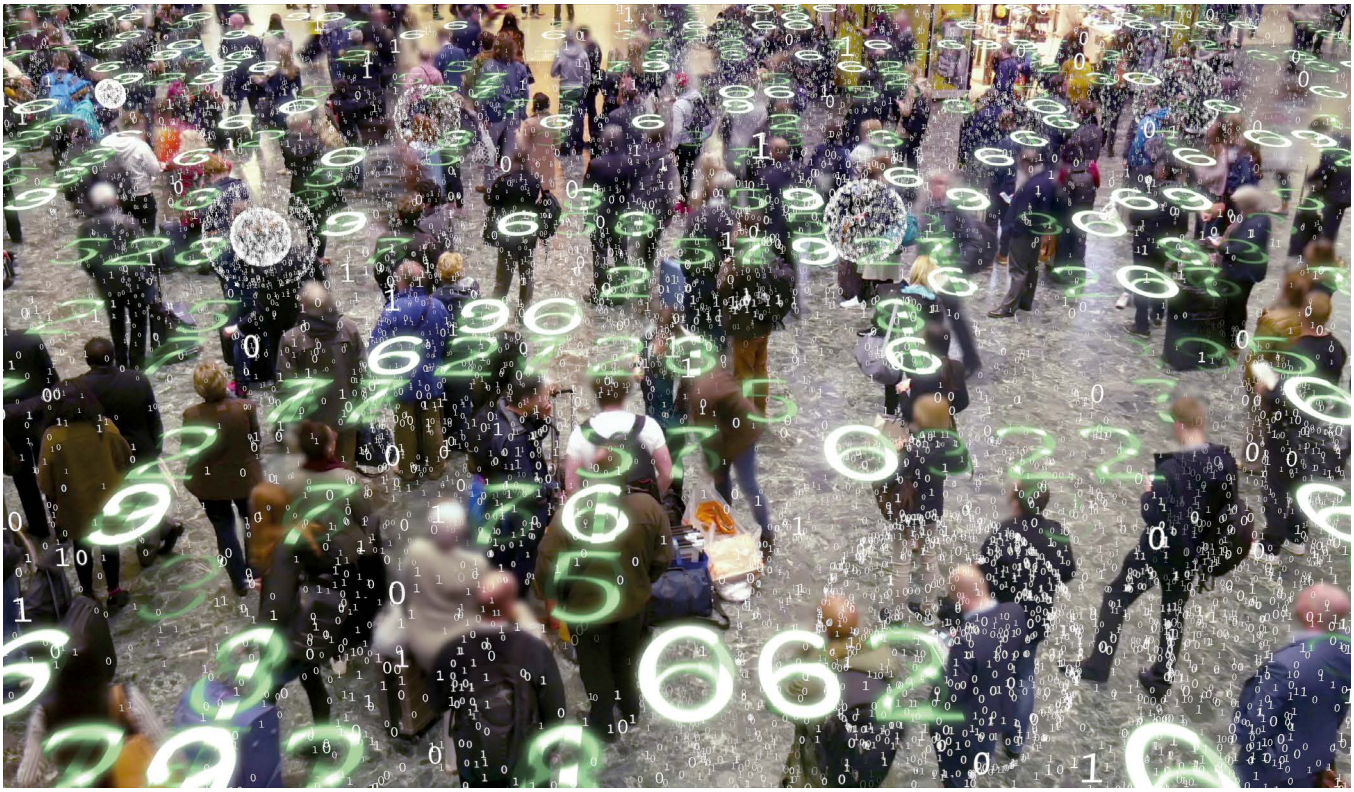
Les assureurs participent activement à cette prise de conscience. C'est en effet par l'assurance que se développent les mesures de prévention car elles sont intégrées aux contrats. L'assurance protège à la fois par la garantie du contrat et par la prévention. Les assureurs ont ainsi développé des mesures d'accompagnement spécifiques au risque cyber afin de prévenir une attaque et d'en réduire les conséquences dommageables.

Et cela commence à porter ses fruits. L'assurance cyber est le segment qui enregistre la plus forte croissance du marché des assurances de biens et responsabilité avec +53 % de progression des cotisations en 2022[7]. France Assureurs accompagne la profession à renforcer cette prise de conscience au niveau de la société française. Ainsi, la Fédération des assureurs a par exemple signé en 2021 un partenariat avec la gendarmerie nationale et agéa, le syndicat des agents d'assurance, afin de sensibiliser les entreprises au risque cyber sur tout le territoire. France Assureurs est également membre fondateur de cybermalveillance.gouv.fr qui a pour missions d'assister les victimes de cybermalveillance, d'informer sur la menace et les moyens de s'en protéger.

Il faut néanmoins aller plus loin. **Il faut une prise de conscience généralisée, incluant toutes les parties prenantes : les citoyens, les entreprises, les assureurs et bien sûr l'Etat.** Il faut développer et diffuser une véritable culture du risque cyber. Les assureurs, dont le métier est de gérer les risques, disposent d'un savoir-faire certain en la matière. C'est la raison pour laquelle France Assureurs propose d'inclure une sensibilisation cyber dans le parcours des jeunes élèves dans les écoles, sur le modèle de ce qui peut se faire en matière de prévention routière. Il faut également amplifier l'effort auprès des entreprises et des collectivités territoriales. En ce sens, la mise en place du Campus Cyber doit être saluée.

Les assureurs sont une partie de la solution. L'Etat, les citoyens et les entreprises ont également dans leurs mains les outils pour mieux se protéger. Travaillons ensemble à mieux protéger les Français. ■

7/ France Assureurs



La cybersécurité dans le secteur financier

Avec un niveau général de cybermenace qui reste élevé en 2022, le secteur financier fait face à une menace cyber permanente, principalement criminelle et hacktiviste. Face à cette menace, le secteur est globalement sécurisé et se prépare aux scénarios de crises majeures, en étroite collaboration avec la Place financière de Paris et l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Le règlement DORA qui entrera en vigueur en janvier 2025, viendra encore renforcer le secteur en imposant des exigences en matière de résilience.

DIDIER COLLET,

Chef de la Division Coordination Sectorielle de l'ANSSI

Une menace principalement criminelle et hacktiviste

La menace cyber impactant le secteur financier diffère en fonction des acteurs : banques, assurance, infrastructures de marché.

Les banques sont sujettes à une diversité de menaces, principalement motivées par le vol d'argent, de données, ou l'extorsion. Un récent rapport[1] indique ainsi qu'en 2022 des banques de pays d'Afrique de l'Ouest, comme le Sénégal ou la Côte d'Ivoire ont été la cible de campagnes d'hameçonnage ciblées. Les cybercriminels auraient cherché à compromettre les systèmes de paiement des banques, et ils auraient eu accès aux passerelles SWIFT dans certains cas, afin de transférer des sommes d'argent vers des comptes sous leur contrôle. En tant qu'entités centrales du système économique d'un pays, les banques sont également sujettes à la menace hacktiviste. Dans le contexte de l'invasion de l'Ukraine par la Russie, de nombreux groupes hacktivistes sont apparus de part et d'autre. Les types d'actions revendiquées par ces groupes sont principalement des attaques par déni de service distribué (DDoS). Le groupe **IT Army of Ukraine**, composé de volontaires défendant les infrastructures ukrainiennes et ciblant des entités russes, a ainsi revendiqué le 13 mars 2023 sur son canal Telegram le ciblage de la banque russe Rosbank, suivi du ciblage des banques russes UBRiR, Bank Bars et de la Banque de Saint-Pétersbourg.

Les assurances, quant à elles, sont des victimes fréquentes de vol de données, du fait de la nature de leur activité. Ces entreprises exploitent un grand nombre d'informations personnelles de leurs clients. La sensibilité de ces données est une motivation potentielle des cybercriminels qui attaquent les assurances à des fins d'extorsion, mais aussi potentiellement de vol d'identité. En 2022, l'assureur médical privé australien MediBank a été victime d'une attaque informatique ayant résulté en une fuite de données. D'après MediBank, les attaquants auraient eu accès au système d'information de l'entreprise en exploitant le couple identifiant et mot de passe d'un prestataire informatique. Les attaquants ont revendiqué la fuite de données personnelles appartenant aux clients de l'entreprise. MediBank a confirmé que les attaquants avaient accès à l'entièreté des données personnelles et de santé de ses 9,7 millions de clients. L'entreprise a déclaré qu'elle refusait de

1/ Rapport conjoint d'Orange Cybersécurité et de l'éditeur de sécurité Group IB

payer une rançon qui ne garantirait pas que ces données ne soient pas publiées. L'exemple de MediBank rappelle que les prestataires des entreprises peuvent constituer un point de vulnérabilité.

Enfin, les infrastructures de marché sont des entités peu ciblées par des attaques informatiques. Toutefois, ces entités sont fortement exposées au risque d'attaque du fait du caractère informatique des échanges, du grand nombre de participants et de la complexité de leurs interactions. Elles sont généralement prises pour cible par des attaques à des fins de déstabilisation. Fin février 2022, une attaque DDoS revendiquée par l'**IT Army of Ukraine** contre la Bourse de Moscou, a eu pour conséquence de rendre le site internet de l'entité indisponible pendant quelques heures. Les attaques sur des entités reliées aux marchés de capitaux peuvent avoir des effets systémiques du fait de l'interconnexion des acteurs. Début 2023, le groupe de rançongiciel **LockBit** a ciblé une filiale de l'entreprise britannique ION Market, qui fournit des logiciels d'opération financière. L'attaque aurait été circonscrite au SI de la filiale de l'entreprise. Toutefois, d'après l'agence américaine CFTC chargée de la régulation des bourses de commerce, l'interruption d'une partie des activités d'ION Market aurait pu avoir des effets sur l'activité du secteur, et illustre ainsi les conséquences potentielles d'une attaque ciblant la chaîne d'approvisionnement (*supply chain*).

Un secteur interconnecté avec une maturité certaine face à la menace cyber

Le secteur financier français est très interconnecté à l'échelle nationale, mais également internationale, avec des filiales pour les établissements de crédit et avec les infrastructures européennes et mondiales pour les infrastructures de marché. Cette caractéristique constitue, de fait, un risque systémique. L'ANSSI accompagne et coopère de longue date avec les acteurs du secteur financier.

La mobilisation du secteur, face à la menace cyber, a conduit à la création de plusieurs enceintes sectorielles (le Groupe de Place Robustesse de la Banque de France, le Forum des Compétences, le groupe de travail interbancaire du Campus Cyber). L'ANSSI collabore efficacement avec ces différents acteurs, notamment dans le cadre de l'anticipation et de la préparation aux crises cyber.

A ce titre, en septembre 2022, la Banque de France et la place financière de Paris (le Groupe de Place Robustesse) ont organisé un exercice de gestion de crise majeure sur la thématique d'une cyberattaque par *supply chain* sur plusieurs acteurs clefs de la Place avec un volet important sur la communication de crise. Cet exercice, accompagné par l'ANSSI, a permis de plonger le secteur financier et certains services de l'Etat dans une crise majeure entrainant des impacts métiers importants et systémiques.

Cet exercice, dont l'objectif était de travailler sur la coordination au sein du secteur, a permis aux dispositifs de gestion de crise de Place composés de cellules thématiques (Fiduciaire, Communication, Liquidité) ainsi qu'aux autres instances de gestion de crise entre acteurs de déclencher leurs mécanismes de mobilisation et de mettre en œuvre leurs mesures de continuité. L'aspect hors norme des évènements a mené à l'identification de solutions de contournement novatrices et de pistes de travail pour faire face à un scénario catastrophe.

Ces axes de travail permettront au Groupe de Place Robustesse de poursuivre le renforcement de la coopération au sein de la Place financière de Paris pour en accroître sa résilience. Pour les autres acteurs du secteur financier, l'ANSSI propose trois guides sur la gestion de crise, disponibles sur le site de l'Agence. Un premier propose une méthodologie pour organiser un exercice de gestion de crise. Un deuxième s'intéresse à la communication de crise et le troisième est consacré à la gestion de crise d'origine cyber pour disposer des meilleurs pratiques pour faire face au niveau opérationnel et stratégique.

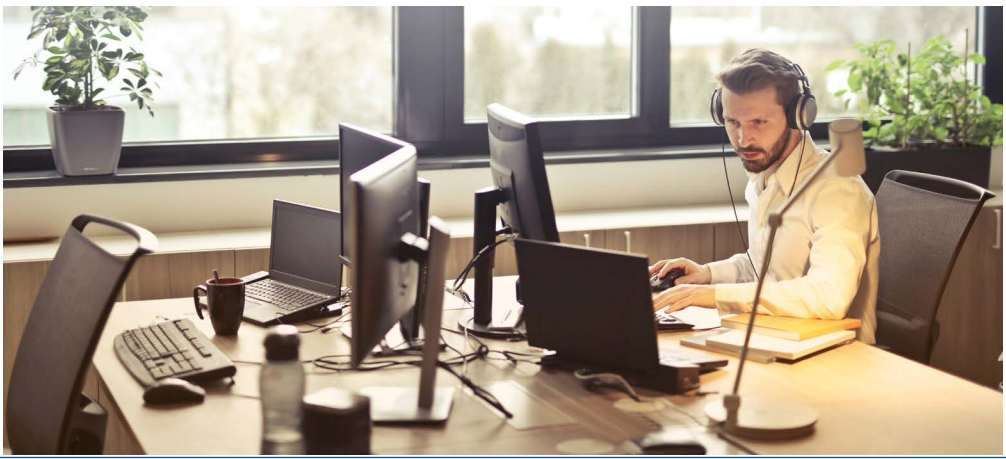
Des exigences de cybersécurité renforcées pour le secteur financier

Au cours des dix dernières années, le contexte réglementaire en matière de cybersécurité s'est étoffé. La France a été l'un des premiers en Europe à se doter d'une doctrine cyber. Ainsi, depuis 2016, l'ANSSI accompagne les opérateurs d'importance vitale pour la Nation, dont ceux du secteur financier, pour le renforcement de la sécurisation de leurs systèmes d'information.

Dans l'intervalle, face à la transformation numérique des sociétés européennes et à l'interconnexion des états-membres, le Parlement européen et le Conseil de l'Union européenne ont adopté, en juillet 2016, la directive « Network and Information Security » (NIS). Transposée au niveau national en 2018, cette directive a eu pour effet d'augmenter le niveau de cybersécurité des acteurs essentiels de dix secteurs d'activité.

La nouvelle directive *Network and Information System Security* (NIS 2) du 14 décembre 2022, qui sera transposée en droit français au deuxième semestre 2024, poursuivra l'effort de sécurisation des entités importantes et essentielles européennes. Ces entités vont de la PME aux entreprises du CAC40, en passant par les administrations publiques et couvrent a minima dix-huit secteurs d'activité.

Concomitamment, à la directive NIS2, le secteur financier s'est doté du règlement européen DORA (*Digital Operational Resilience Act*). Ce règlement, qui entrera en vigueur en janvier 2025 se substituera, pour le secteur financier, à NIS 2, selon le principe *Lex specialis*, et imposera des exigences en matière de résilience. En France, l'ACPR (autorité de contrôle prudentiel) supervisera la bonne application de ce règlement. L'ANSSI continuera sa collaboration avec le secteur financier, tant dans le domaine de la connaissance de la menace, que dans sa sécurisation et la préparation aux situations de crise. ■



Innovations assurantielles au service de la lutte contre le risque cyber

CAROLINE HILLAIRET,

Professeure à l'ENSAE Paris, CREST, et Membre certifié de l'Institut des actuaires

OLIVIER LOPEZ,

directeur de l'ISUP, Sorbonne Université et Membre agrégé de l'Institut des actuaires

Le risque cyber désigne l'ensemble des risques liés à l'usage des technologies numériques. Avec la croissance de l'économie digitale, il est devenu aujourd'hui un risque économique majeur, avec des incidents cyber en forte augmentation, et des coûts, directs et indirects, estimés à environ 1% du PIB mondial c'est-à-dire de l'ordre de mille milliards d'euros par an (cf. (1)).

Le secteur financier est particulièrement concerné par le risque cyber : d'après le président de la Réserve Fédérale américaine Jerome Powell, le risque cyber constitue la principale menace pesant sur le système financier mondial. En effet ce secteur, qui est fortement numérisé et interconnecté, est une cible privilégiée pour les hackers, d'autant plus qu'il présente des gains potentiellement importants pour les cyber-pirates. Il peut ainsi se trouver en situation de victime contaminée par la crise, et doit se préparer à des attaques majeures, et notamment à de potentiels événements d'une ampleur systémique.

Le secteur de la finance et de l'assurance est aussi bien sûr fournisseur de solutions de couverture du risque et a un rôle important à jouer pour contribuer à la résilience de l'économie et de la société face au risque cyber. Ainsi le marché de la cyber-assurance s'est développé, en mettant en avant des offres innovantes qui couplent prévention, réparation financière, et accompagnement en cas de crise. Néanmoins, de nombreuses questions se posent sur leur viabilité, et sur la capacité du secteur à mutualiser les pertes en cas de sinistre majeur, comme l'illustre le récent rapport LUCY de l'AMRAE (2).

Face à ce risque de grande ampleur, la question de son assurabilité est liée à une éventuelle perte de mutualisation. La mutualisation, mécanisme au coeur de l'assurance, repose sur la compensation du coût des sinistres par les bons résultats sur le reste du portefeuille. Plusieurs caractéristiques du risque cyber peuvent la mettre en péril, notamment le caractère à la fois catastrophique et systémique de ce risque. Un événement catastrophique, touchant une seule victime, peut atteindre des montants trop importants avec probabilité trop élevée (on parle de montant de sinistres à queue de distribution lourde). Un événement systémique peut entraîner des sinistres simultanés pour un grand nombre d'assurés et engendrer un risque d'accumulation. Cette perte de mutualisation est d'autant plus accentuée si le nombre d'assurés n'est pas suffisant pour amortir les sinistres.

Face à ces écueils, un des enjeux est tout d'abord de parvenir à un équilibre entre restreindre le périmètre d'indemnisation (notamment en réduisant la capacité maximale de prestation) et la nécessité de concevoir des polices suffisamment attractives pour élargir la base de mutualisation. Dans le cas d'événements extrêmes touchant simultanément de nombreux assurés, et non mutualisables pour un assureur, des solutions de

transfert de risque adaptées au cyber doivent être développées.

Pour certaines couvertures assurantielles présentant des risques d'accumulation, comme les risques de catastrophes naturelles, des régimes spécifiques d'indemnisation, sous forme de partenariat public privé, ont été instaurés et délivrent aux assureurs une couverture de réassurance illimitée, bénéficiant de la garantie de l'Etat. L'extension de ce type de régime au cyber ne va pas de soi. On ne peut donc faire l'économie d'une réflexion autour d'autres stratégies de transfert de risque, qu'elles soient portées par un réassureur traditionnel, ou dans la perspective de constitution de captives par les grandes entreprises. La question est bien sûr d'évaluer la viabilité économique de ces stratégies. Or cette évaluation est complexe, le risque cyber étant difficile à quantifier, à la fois en raison de son périmètre évolutif et de l'absence de données fiables et structurées sur les incidents.

Bien que permettant une mutualisation à plus grande échelle, la réassurance a des limites : un événement majeur se propageant à une grande échelle dans un phénomène de contagion, et ce même au-delà des frontières, peut ainsi faire porter une charge trop importante sur le réassureur. La construction de scénarios stochastiques de crise (cf. (3) et (4)) permettrait de disposer d'un spectre très large de stress tests afin d'étudier l'impact potentiel d'un événement cyber massif et d'estimer la capacité de l'entité (assureur/réassureur/grandes entreprises) à absorber un choc d'ampleur significative.

Parmi les autres stratégies de transfert de risque, l'assurance paramétrique peut apparaitre comme une solution prometteuse pour se couvrir contre certains risques. Le déclenchement du paiement étant lié à la simple constatation de la valeur d'un indice préalablement défini, l'indemnisation se passe d'une démarche d'expertise et d'évaluation des coûts. Outre l'ouverture possible vers une titrisation, la couverture paramétrique est prometteuse car répondant à un impératif de fluidité de la compensation assurantielle. Pour l'assureur, la charge de gestion de sinistre est réduite à la portion congrue : le versement de la prestation est accélérée, favorisant ainsi une reconstruction précoce. Ce changement d'échelle temporelle dans la résolution de l'équation financière est en adéquation avec la réalité du cyber, où la plasticité de la menace impose des réactions toujours plus rapides.

Encore faut-il que le paramètre considéré réponde bien aux attentes de l'assuré. En particulier dans le contexte d'un risque perçu comme immatériel, car la réalité physique du paramètre est rarement évidente, même pour un initié. Sans doute la question ne se pose-t-elle pas de la même manière pour tous les pans du cyber. Car le cyber recouvre des phénomènes variés, avec des conséquences très disparates d'une victime à l'autre. Dans le cas d'une fuite de données, on est prêt à admettre que le volume de données dérobées est un marqueur de la perte financière associée. Le temps d'interruption d'activité d'un site de vente en ligne est également corrélé à la perte financière lors d'une attaque par déni de service. Mais même ici, ces deux propositions de paramètres sont discutables : la nature des données, les conséquences de leur fuite sont variables d'un secteur d'activité à un autre ; si une activité est dépendante de cycles saisonniers, elle peut être ponctuellement plus vulnérable - on pense par exemple à un site de vente en ligne touché rendu indisponible au moment du Black Friday.

Face à la complexité de la discussion autour du paramètre, la confiance est essentielle. Confiance en la fiabilité du paramètre, sa disponibilité et sa traçabilité. Confiance également entre assuré et assureur dans la co-construction de ce modèle d'assurance.

Car c'est bien sur une forte collaboration assureur - assuré que repose le succès : face à un risque émergent, l'information manque, et les deux parties ont besoin d'échanger celle-ci afin d'apprendre et de construire une protection, pas uniquement financière. Il faut ainsi rappeler le rôle historique de l'assurance face à d'autres périls : le risque incendie est souvent cité, où l'éclosion d'une vision collective, via l'assurance, a fortement contribué à développer et à diffuser des normes. De par le caractère évolutif de la menace, éteindre le feu du cyber est sans doute plus complexe. Mais pour aider à sa maîtrise, les innovations assurantielles et financières sont particulièrement prometteuses. ■

(1) McAfee and Center for Strategic and International Studies, *The Hidden Costs of Cybercrime*, (2020)

(2) AMRAE, LUCY : *Lumière sur la CYberassurance*, (2022)

(3) Hillairet C., Lopez O. *Propagation of cyber incidents in an insurance portfolio: counting processes combined with compartmental epidemiological models*, Scandinavian Actuarial Journal, 2021(8), 671-694

(4) Hillairet C., Lopez O., d'Oultremont L., Spoorenberg B. *Cyber-contagion model with network structure applied to insurance*, Insurance: Mathematics and Economics 107 (2022) 88-101

Cyberattaques dans le secteur financier : un état de la menace

« Connaissez l'ennemi et connaissez-vous vous-même ; en cent batailles vous ne courrez jamais aucun danger. » Sun Tzu, l'art de la guerre

MALIKA SMAILI,

Auditrice IHEDN, spécialiste en risques du domaine bancaire

Le sujet se démocratise, il devient accessible partout et pour tout le monde mais seulement lorsqu'il est trop tard, lorsque la menace a été mise à exécution et que le système d'information n'est plus disponible, terrassé par une attaque cyber. Toutes les entreprises, quelque soit leur taille, sont des cibles et les établissements bancaires n'y échappent pas. Rappelons-nous de la banque centrale européenne, victime d'une intrusion sur un service de partage de fichiers en janvier 2021, de la bourse de Nouvelle Zélande paralysée pendant quatre jours en août 2020 après une compromission des données de marché, ou des attaques de rançongiciels (ce petit programme informatique qui chiffre les données) dont ont été victimes la filiale asiatique d'AXA en mai 2021 et TRAVELEX en décembre 2019. Lorsque les données sont ainsi codées, il n'est possible de récupérer la clé de chiffrement qu'en échange de paiement d'une rançon à minima ; car il arrive que la victime soit exposée à une double extorsion, lorsque le pirate met en vente les dites données sur le marché noir même après avoir reçu l'argent de la rançon. Un véritable fléau particulièrement pour les données bancaires de millions de clients. Ces attaques ne sont pourtant pas une fatalité à condition de s'y préparer et d'y répondre à temps.

Boostés par la pandémie et la digitalisation

Comme dans bien d'autres domaines, la crise sanitaire a exacerbé la tendance. Selon un rapport de la Banque des règlements Internationaux (BRI) datant de 2021[1], les institutions financières ont été largement plus exposées à des attaques que la plupart des autres secteurs (en dehors de la santé). Un rapport du FMI sur les pertes que pourraient causer les cyberattaques dans le secteur financier estime le montant à près de 9% du bénéfice net mondial des banques (100 milliards de dollars)[2]. Les attaques à l'encontre d'établissements financiers surfant sur la vague du Covid 19 sont passées de 5000 par semaine en février 2020 à plus de 200 000 en mai de la même année. Beaucoup de clients utilisaient les services bancaires en ligne pour gérer leurs comptes et pour la majorité des paiements. Le télétravail massif a également engendré des situations inédites dans lesquelles des traders travaillaient depuis leur domicile, alors qu'ils sont soumis à des règles règlementaires strictes qui exigent une surveillance et un enregistrement de leurs appels en permanence. Or, partager son réseau avec les autres membres de la famille, pouvait les exposer à des logiciels malveillants ou

1/ https://www.bis.org/publ/bisbull37.pdf
2/ https://www.imf.org/en/Blogs/Articles/2018/06/22/blog-estimating-cyber-risk-for-the-financial-sector

à d'autres opportunités pour le pirate (vol de données, intrusion dans le système, compromission de comptes de traders etc…).

Cyberattaques et biais cognitifs

C'est dans le domaine bancaire qui déploie des trésors d'imagination pour maintenir ses performances que l'on observe le plus d'innovation technologique (utilisation massive de cloud, d'intelligence artificielle, numérisation des services…). Profitant de la forte digitalisation du secteur bancaire et de la crise sanitaire, les pirates, sans scrupules, ont déployé des trésors d'imagination pour amener les utilisateurs là où ils voulaient qu'ils aillent : activer certains biais cognitifs bien connus en sciences sociales et jouer sur leurs désirs et leurs émotions. Pour décider, le cerveau humain a tendance à prendre des raccourcis mentaux, plus faciles d'accès et moins coûteux en temps, en énergie et en concentration. Ainsi, il s'agit d'amener la victime à agir en profitant du biais d'autorité ou d'expertise (la cible accorde de la crédibilité au message du fait de la position dont l'attaquant se réclame) ; l'attaquant peut aussi utiliser une stratégie d'urgence (« transmettez-moi le plus vite possible tel document ») ou actionner la curiosité ou l'appât du gain en proposant de remporter la loterie du siècle.

Etat des lieux de la menace

Qui sont les attaquants

Un rapport publié par l'Autorité des Marchés Financiers[3] en 2021, et relatif à l'état de la menace dans le domaine boursier, indique que les cybercriminels sont organisés en groupes spécialisés dans le secteur financier, parfois encouragés par des états (Russie, Chine, Corée du Nord, etc.) utilisant des outils sophistiqués, disponibles dans un véritable supermarché du cybercrime sur le Dark Web.

Parmi les autres typologies d'acteurs, il peut s'agir d'activistes motivés par le rayonnement que pourrait avoir l'impact de l'attaque sur leur cause idéologique. D'autres acteurs malveillants pourraient aussi être motivés par l'abolition de nos systèmes démocratiques ; et quoi de mieux que d'd'exploiter des vulnérabilités systémiques d'un monde financier interconnecté pour entrainer perte de confiance, agitation et chaos social.

Pourquoi et comment menacent-ils ?

Du braquage d'une agence à l'attaque informatique ciblée, la motivation du pirate reste la même : le gain financier. Seules les méthodes changent. Mais l'appât du gain n'est pas la seule motivation. Le système bancaire repose sur la confiance du consommateur, l'attaquant peut donc être motivé par l'exécution d'un sabotage visant à déstabiliser le système bancaire ou nuire à l'image de marque de l'institution, surtout si l'attaque génère des perturbations du service à la clientèle. Moins dans le monde bancaire que dans l'industrie, mais cependant non négligeable, il peut s'agir d'espionnage parrainé par des États-nations dans un contexte de tensions géopolitiques afin d'obtenir des informations critiques (secrets d'affaires, renseignements exclusifs, etc..). La Banque de France le rappelle bien dans son dernier rapport évaluant les risques du système financier français publié en 2021[4].

Une des techniques d'attaque les plus populaires dans le secteur bancaire est de cibler les clients, et dans une moindre mesure les collaborateurs après une reconnaissance préalable, en utilisant un mail d'hameçonnage (phishing) qui incite le destinataire à cliquer. Ce clic va permettre le téléchargement silencieux d'un programme qui s'exécutera immédiatement ou qui est programmé pour un déclenchement ultérieur. Une fois le ver dans le fruit, les conséquences sont multiples : pertes financières pour les clients, attaque du système d'information de l'établissement visé etc..

L'autre menace principale et redoutée, est une utilisation d'une chaine d'approvisionnement en exploitant une des ses potentielles vulnérabilités. Les établissements financiers sont particulièrement exposés car ils sont interconnectés dans un écosystème complexe et difficilement traçable, dont le moindre grain de sable pourrait entrainer des réactions en chaines d'une ampleur considérable (risque systémique). Utiliser le maillon le plus faible de la chaine reste donc un bon moyen pour l'attaquant bien

3/ https://www.amf-france.org/sites/institutionnel/files/2020-02/study-stock-market-cybercrime-_-definition-cases-and-perspectives.pdf

4/ https://publications.banque-france.fr/sites/default/files/medias/documents/2021_s1_ers_0.pdf

informé. Et quoi de plus simple que de se renseigner sur le fournisseur de telle ou telle solution digitale bancaire, puis d'attaquer les infrastructures de celui-ci ? le site de relations professionnelles LinkedIn est une source précieuse et ouverte de données accessiblesà tous. Pour exemple, l'affaire Solarwinds en 2021, reste aujourd'hui un cas d'école en matière de compromission des systèmes de distribution de logiciels. C'est l'une des opérations de cyberespionnage les plus sophistiquées de ces dernières années. Les pirates ont eu accès au réseau de l'éditeur et ont infecté son logiciel de gestion, permettant ainsi de cibler l'ensemble des clients de l'éditeur.

Le déni de service distribué reste encore en 2023 un scenario redouté. Il s'agit, via des robots, de générer et simuler un trafic internet très important pour épuiser les ressources du serveur et par conséquent bloquer le site web. Les clients ne pouvant plus se connecter à leur espace, c'est un risque d'image avéré.

D'autres techniques peuvent aussi ébranler les marchés boursiers. Il peut s'agir d'une fausse information diffusée via un « deepfake », des contenus élaborés grâce à une intelligence artificielle et diffusant des informations fausses mais totalement crédibles et réalistes pour les personnes mal informées. L'AMF, mais aussi les régulateurs australiens, anglais et américains ont renforcé le cadre juridique pour lutter contre ce type d'attaques. En France, c'est l'article L465-3-213 du Code monétaire et financier qui sanctionne ce comportement frauduleux. Souvenons-nous de l'affaire Vinci en 2016 et du faux communiqué annonçant des erreurs comptables et le licenciement du directeur financier. L'information reprise par Bloomberg a fait immédiatement plonger le cours de l'action Vinci. Huit minutes après la diffusion de l'information par Bloomberg, l'agence publie un démenti. L'action retrouvera presque instantanément son précédent prix, et l'affaire sera portée devant les tribunaux.

Atténuation des impacts

Contrôler, évaluer, couvrir, tester sont les maitres-mots de la lutte contre les cyber-attaques. Les banques sont considérées comme des opérateurs d'importance vitale, et le secteur bancaire est l'un des mieux avancés en termes de protection. Malgré une digitalisation très avancée, on ne dénombre aucun incident de portée systémique dans le secteur financier. Les régulateurs ont bien conscience que la résilience du système financier passe par la mise en œuvre d'exigences très fortes, au travers de règlements très contraignants (CROE, DORA, NIS2 ...).Mais la conformité ne règlera pas tout, et déployer des procédures préventives pour simplement ne pas s'exposer au risque d'amende, est insuffisant. Dans certains domaines, seule la mise en place d'un cadre de gestion des risques et de contrôles associés permettra de limiter l'impact d'une attaque.

Il faut veiller à identifier les rôles critiques de l'organisation et estimer leur potentielle exposition à un risque d'espionnage ou d'usurpation d'identifiants de connexion. Renforcer les contrôles permettra d'identifier des vulnérabilités exploitables par des personnes malveillantes. L'humain, maillon de la chaine dans les processus bancaires, devra être sensibilisé très régulièrement, au moins une fois par an, et des tests de phishing régulièrement exécutés pour maintenir sa vigilance à un niveau acceptable.

Il est aussi important de ne pas négliger les sujets opérationnels : Connaitre son système d'information, cartographier ses dépendances, tracer sa chaine d'approvisionnement, réaliser des tests d'intrusion, sont autant d'actions bénéficiant à la prévention. Une bonne connaissance du système d'information permettra également de mieux gérer l'accès à l'information au travers du principe du « besoin d'en connaitre », l'accès aux applicatifs critiques, le filtrage de contenu, la politique de couverture des vulnérabilités logicielles (patching). Les banques et les assureurs français n'ont pas attendu pour s'organiser, ils occupent une place prépondérante au campus cyber, ce lieu voulu par le président Macron, qui permet de mener des projets communs au profit de la cybersécurité. ■

Malika Smaïli

Ingénieure en électronique, diplômée en intelligence économique et auditrice de la 3e session nationale souveraineté numérique et cybersécurité de l'IHEDN, Malika Smaïli est aujourd'hui experte en risques opérationnels et cybersécurité du monde bancaire.

Faire face à la menace du risque cyber

Tout le monde est concerné par le risque Cyber : particuliers, collectivités locales, établissements de santé, administration, petites et grandes entreprises. Chaque jour, les exemples d'attaques sont nombreux, qu'il s'agisse des médias ou de l'entourage proche.

FLORENCE PICARD,

Actuaire certifié de l'Institut des actuaires Membre du Directoire de la Fondation du Risque

Quelles sont les menaces ?

Les menaces résultent de la conjonction de stratégies malveillantes des attaquants et de failles de protection des victimes (humaines ou techniques).

Elles ont des objectifs variés. Menées par des « entreprises » du crime motivées par l'argent, elles agissent souvent par rançonnage. Elles peuvent aussi servir des intérêts privés, ou agir pour des Etats, notamment par espionnage industriel, ou simplement pour nuire : porter atteinte à l'image ou saboter des outils de production ou de service.

Nous nous limiterons ici au domaine économique, sachant que la défense nationale joue un rôle clé dans la guerre cyber.

Car il s'agit d'une forme de guerre, silencieuse, atypique, qui concerne chaque acteur de l'économie et ne relève que partiellement de la Défense Nationale car il s'agit d'actes qui, pris individuellement, ont une motivation lucrative, mais qui servent au final des opérations de déstabilisation géopolitique.

Contrairement aux risques habituellement assurés (risque automobile, incendie, perte d'exploitation, catastrophes naturelles, etc..), il n'y a rien de naturel dans cette menace qui utilise la technologie au service de stratégies d'attaques criminelles.

Il s'agit d'une véritable économie souterraine composée d'entreprises structurées, employant des ingénieurs compétents (et cupides), « travaillant » en direct mais aussi via des « affiliés » autorisés à utiliser leurs logiciels moyennant une rétrocession sur les gains, et souvent, le respect de certaines règles de comportement (sorte de « code d'honneur »), pour ne pas gâcher le marché en attaquant des cibles populaires. Ils sont d'ailleurs parfois débordés par ces affiliés moins intelligents dans leur cupidité, comme en atteste les attaques contre les hôpitaux, tel que celui de Corbeil Essonne.

Les ingénieurs de cyber sécurité des entreprises déploient des moyens de plus en plus importants pour sécuriser les systèmes informatiques (SI) et faire barrage aux attaquants. L'Intelligence Artificielle commence à les aider dans la détection et la prévention des attaques.

Mais souvent, les intrusions dans les systèmes d'information s'effectuent via des messages piégés (phishing) et ce sont les victimes elles-mêmes qui ouvrent la porte aux hackers (en cliquant sur un lien frauduleux par exemple).

Quels sont les risques pour une entreprise ?

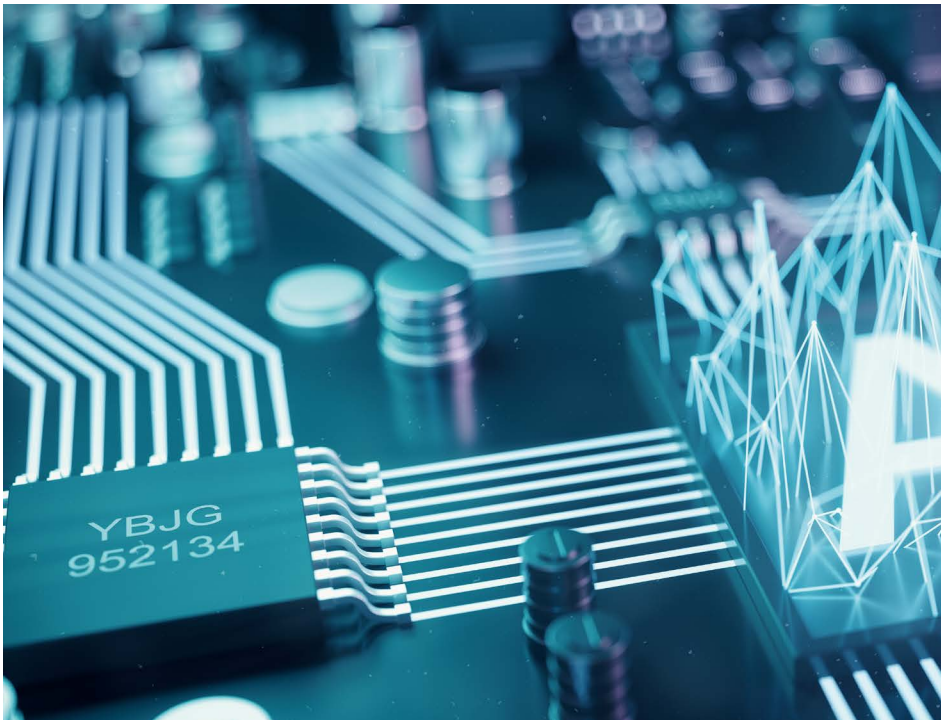
Une entreprise peut être spécifiquement visée par une attaque, mais elle peut aussi être victime du caractère viral de certaines attaques, par exemple via un prestataire lui-même infecté. Ce caractère systémique peut provoquer une diffusion de nombreux sinistres, dans tous les pays à la fois, affectant des entreprises de tous secteurs d'activité et de toutes tailles (exemple des rançongiciels WannaCry et Petya en 2017).

Les types d'attaques sont assez nombreux : parmi les plus fréquentes citons le « deni de service » et le « vol de données » avec demande de rançons pour les restituer.

Une attaque par deni de service rend le service inaccessible par saturation de demandes ; c'est un type d'attaque très efficace quand l'entreprise a pris des engagements de rendre un service dans un délai donné (c'était le cas pour TV5 Monde en 2015).

Le vol de données avec cryptage les rend inutilisables et payer la rançon pour les récupérer n'est pas une solution recommandée car non seulement les hackers ne rendent pas toujours les données non cryptées, mais surtout, cela alimente les industries criminelles du dark web qui ont pris une importance considérable : drogues et armes à feu, payables en Bitcoin, plateforme de financement participatif pour organiser toutes sortes de crimes, notamment les trafics d'armes et de stupéfiants, voire même des assassinats.

Pour l'entreprise, c'est l'arrêt de tout ou partie du SI et de l'activité de l'entreprise qui constituent le risque principal de la menace : perte d'exploitation, de production, de commercialisation, de clientèle, surcoût pour pallier partiellement l'arrêt du SI par l'embauche de temporaires. Le délai de récupération d'un fonctionnement normal est souvent très long : plusieurs mois. C'est aussi le cas pour les villes : Angers en 2021, Atlanta en 2018 en sont des exemples. Plus d'un an après, Angers en subissait encore les conséquences, notamment



pour la réservation de places en crèches encore à l'arrêt, malgré près d'un milliard d'euros dépensés. Selon l'ANSII, Agence nationale de la sécurité des systèmes d'information, il faut environ deux ans à une ville attaquée pour se remettre sur pied.

Pour les petites entreprises, mal protégées, et mal préparées, le risque cyber peut être vital. Malheureusement, faute d'une obligation de déclaration des attaques, il n'existe pas de statistiques fiables.

Comment répondre à ces menaces : cyber sécurité et formation du personnel

Pendant quelques temps, la cyber sécurité a espéré pouvoir assurer à elle seule la protection des systèmes d'information (SI), le SI étant vu comme un château fort qu'il faudrait rendre imprenable.

Il est ensuite apparu évident que, au-delà de l'informatique, c'est l'ensemble du personnel de l'entreprise qui était concerné pour éviter que les collaborateurs contribuent aux attaques par manque de vigilance. Des formations, suivies de training réguliers, sont maintenant une pratique courante dans les grandes entreprises pour le respect des « gestes barrière Cyber ». Elles

ne garantissent pas l'absence d'erreur humaine, mais de gros progrès ont été réalisés. Au-delà de l'entreprise, c'est même chaque citoyen qui est concerné, car les bots (robots), qui lancent des attaques Ddos (deni de service), sont parfois dormants dans des machines appartenant à des particuliers.

Malheureusement la situation est différente pour les petites PME et TPE, qui disposent rarement d'un directeur informatique, encore moins d'un spécialiste de la sécurité et qui n'ont pas toujours connaissance des outils très pratiques et efficace mis à leur disposition par le GIP ACYMA.

Vivre avec la menace

Il faut se rendre à l'évidence : nous devons apprendre à vivre avec cette menace, comme c'est le cas avec la Covid ou avec les nouveaux risques climat ou géopolitique.

L'idée n'est plus seulement de se protéger de la menace, mais d'apprendre à agir de la façon la plus appropriée si elle se réalise, afin de minimiser l'impact d'une attaque réussie : prendre les bonnes décisions dans les premières minutes du sinistre, chacun sachant exactement ce qu'il a à faire, cela se prépare dans un bon plan de crise, alliant technique informatique et organisation des activités. Restaurer au plus vite un SI endommagé, mettre en place les solutions alternatives de fonctionnement prévues dans le cadre du plan de crise, se protéger par des process d'organisation du travail conçus « by design » pour que l'activité soit moins dépendante du SI, il s'agit bien de ne pas s'épuiser en cherchant à tout éviter, mais parallèlement à l'éducation de toute la population et aux mesures de prévention qui sont essentielles, de travailler en amont d'une éventuelle attaque pour accélérer la capacité à restaurer le SI et les données au plus vite, car c'est le temps d'arrêt d'activité qui coûte cher. Pour cela il faut identifier les activités dont la mise à l'arrêt est le plus dommageable, pour prévoir des solutions de contournement avec des fonctionnements en mode dégradé.

Ainsi, le risque cyber confère une importance capitale à la prise en compte des risques opérationnels et à leur analyse fine, activité par activité, et avec leurs interactions.

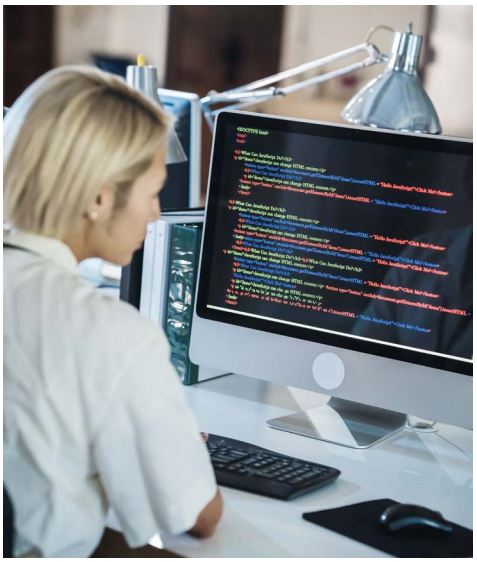
Le législateur a pris des mesures pour garantir que les grandes entreprises du système financier prennent tous les moyens nécessaires et allouent les budgets adéquats. La responsabilité des dirigeants est engagée, notamment au travers de la loi NIS2.

Un plus large ensemble d'entreprises sera bientôt concerné par la loi Dora.

Mais quand l'attaque est là, que le SI a été infecté ou piraté, il est important, pour la valeur économique et la pérennité de l'entreprise, de disposer de l'indemnisation d'un contrat d'assurance et de l'assistance technique souvent proposée avec ces contrats.

A cet égard, après avoir accompagné le marché et essuyé des pertes, en l'absence de données pour évaluer le risque, les assureurs et les réassureurs sont devenus prudents car il y va de leur solvabilité : ils ne peuvent pas supporter les risques systémiques qui relèvent de la solidarité nationale.

Ils sont d'autant plus handicapés pour assurer ce risque que, outre l'absence



de données, la réglementation n'est pas adaptée : à l'inverse des captives que peuvent créer les entreprises, les assureurs n'ont pas le droit de mutualiser le risque dans le temps, ce qui leur permettrait de lisser sur plusieurs années les pics des grands sinistres.

Si l'on veut que les assureurs puissent jouer leur rôle, il est indispensable que la réglementation les autorisent à constituer des provisions pour égalisation.

Bien connaître les impacts économiques de la menace pour protéger efficacement le tissu des entreprises

Tout l'effort actuel des pouvoirs publics (1 milliard affecté au plan de cyber sécurité en 2021) porte sur la prévention et la sécurité informatique, mais pas sur la protection financière ni la connaissance de la dimension économique du risque, pourtant non maîtrisable par la technologie, à court-moyen terme.

Le Campus Cyber initié par le Président de la République, inauguré en février 2022, est le lieu totem de la cybersécurité. De gros moyens financiers y sont consacrés et nul doute que des solutions techniques vont émerger, notamment par un dialogue à établir entre ingénieurs de sécurité et spécialistes de l'Intelligence artificielle.

La dimension technologique est certes essentielle mais l'écosystème cyber doit non seulement bénéficier de la prévention et la remédiation technique, mais aussi de la protection et la remédiation financière, comme pour tous les risques car, malgré les meilleurs efforts de prévention, il n'existe pas de risque zéro.

Le choix a été fait de protéger les grands groupes et de leur permettre de s'organiser pour disposer des provisions nécessaires en cas de sinistre.

Mais c'est tout le tissu industriel qui devrait l'être. Or rien n'est fait à ce niveau. La mort de petites entreprises emportées par une attaque et la perte des emplois concernés n'est pas une sanction méritée. Il faut pouvoir permettre aux petites entreprises de disposer, à un prix abordable, d'une couverture financière à la hauteur des dommages.

Bien connaître ce risque nouveau, très particulier, est une nécessité pour que les assureurs puissent organiser des mutualisations et intervenir massivement sur la partie aléatoire. Le risque systémique et les évènements exceptionnels mériteraient de bénéficier par ailleurs d'un système de solidarité inspiré du régime des catastrophes naturelles.

Connaître le risque nécessite la collecte et le partage des données de façon sécurisée afin d'avoir une observation holistique de la menace et que chaque assureur mène sa politique de souscription en connaissance de cause, comme c'est le cas par exemple s'agissant de la mortalité.

Or pour le moment, rien n'est fait pour l'Observatoire de la menace. Prévu dans les statuts du GIP ACYMA comme l'une de ses 3 missions, il ne fait plus partie du programme de travail de ce Groupement d'intérêt public.

Un effort national pour la création d'un observatoire du risque est pourtant indispensable pour permettre d'évaluer et d'organiser la solidarité financière par la mutualisation.

Car faire face à la menace, c'est observer et mesurer ces dommages et leur contexte de survenance, pour bien connaître le risque et préserver le tissu économique de ses impacts à la fois techniques et financiers. ■

Cybersécurité des professions financières : les régulateurs demandent des comptes

Nicolas ARPAGIAN,

Vice-President Cybersecurity Strategy & Digital Risks du cabinet HeadMind Partners, Enseignant à l'Ecole Nationale Supérieure de la Police (ENSP) et à Sciences Po Saint Germain.

Auteur de « La Cybersécurité » (PUF) et « Frontières.com » (Editions de l'Observatoire)

Twitter : @cyberguerre

3,15 millions d'euros. C'est l'amende infligée en décembre 2022 à la banque espagnole Abanca par la Banque Centrale Européenne (BCE) suite à la cyberattaque dont l'établissement avait été victime en février 2019. Elle avait conduit à la paralysie de ses distributeurs de billets, à l'incapacité à procéder à des virements et à accéder aux comptes via l'application maison. Ce n'est pas en raison du principe d'être piraté que le banquier espagnol a été sanctionné : mais pour avoir attendu quarante six heures pour avertir le gendarme bancaire européen. Or, depuis 2017, les entités placées sous l'autorité de la BCE doivent informer celle-ci dans les deux heures de la détection d'un incident informatique significatif. Cette réactivité est exigée afin de limiter les effets d'une possible propagation à l'ensemble de la communauté financière. Il existe en effet un véritable risque systémique en raison de l'interconnexion des systèmes d'information, et de la capacité de l'attaquant d'exploiter une faille d'un logiciel qui serait présente au sein de différentes sociétés du même domaine d'activité.

Dans le même esprit, le Conseil de Stabilité Financière (CSF), qui rassemble une trentaine d'autorités financières nationales (banques centrales, ministères des finances…), ainsi que différentes instances internationales chargées d'établir des normes en matière précisément de stabilité financière plaide[1] régulièrement pour le déploiement de modèles d'appréciation du risque cyber qui soient harmonisés au sein des organisations du secteur. L'importance stratégique de la disponibilité et de l'intégrité des systèmes de communication dans le bon fonctionnement des échanges financiers et commerciaux explique la prise en compte grandissante des moyens de détection et de remédiation des cybermenaces dans les processus d'évaluation des acteurs économiques[2]. Au point que l'ensemble des auditeurs (juridiques, comptables…) réclament désormais des éléments de mesure de l'exposition au risque cyber. Qui font désormais partie intégrante des démarches de « due diligence » pour connaître la valeur d'une entreprise. Et cela concerne désormais les structures au sens large. Puisque la BCE estime qu'en 2021 les sommes concernant les prestations externalisées (cloud computing, sous-traitants, consultants…) constituaient presque la moitié (47,4%) des dépenses informatiques des banques européennes. Une tendance cadencée par l'adoption grandissante de services dans le nuage. Ce qui pose la question de la maîtrise en continu de l'environnement technique élargi de l'entreprise. Avec des partenaires ou des fournisseurs qui peuvent être l'objet d'agressions qui conduisent en cascade à la détérioration, voire à l'arrêt des services bancaires. Le Trésor des Etats-Unis[3] a indiqué qu'au cours de l'année 2021 les institutions financières du pays avaient été amenées à payer près de 1,2 milliard de dollars pour faire face à des rançongiciels. Soit le double du montant payé en 2020. Sur la même période, le nombre d'attaques sous la forme de rançongiciels a triplé, représentant quelque 1 500 incidents documentés par l'autorité étatsunienne visant la sphère financière. ■

1/ "Towards a framework for assessing systemic cyber risk"- John Fell, Nander de Vette, Sándor Gardó, Benjamin Klaus & Jonas Wendelborn, *Financial Stability Review*, Novembre 2022.

2/ « Entreprises, mettez de la cybersécurité dans vos comptes », Nicolas Arpagian, *Les Echos*, 29 décembre 2021.

3/ *Financial Trend Analysis*, Financial Crimes Enforcement Network, Novembre 2021.

Cyber assurance, prévention et gestion du risque pour assurer la pérennité de nos entreprises

MARIE SOYER,

Directrice Générale d'ALPTIS

ARNAUD GRESSEL,

Président de RESCO Courtage ET expert Cyber Assurances à l'IHEMI+ Master GGRC à la Sorbonne

Longtemps ignorés ou sous-représentés dans les baromètres et cartographies des risques, les risques cyber se sont manifestés avec virulence depuis 2017 lors de deux vagues d'attaques mondiales (Wannacry - mai 2017, NotPetya - juin 2017), sans laisser de répit depuis cette date aux entreprises et collectivités.

On a pu croire que le risque était à son apogée lors du passage au travail à distance nécessité par le confinement lié covid-19 en 2020. Or il n'en n'est rien, la menace n'a cessé de croître depuis. Celle-ci est devenu protéiforme, professionnelle quand elle n'est pas étatique, et dans tous les cas, systémique.

Désormais en tête des baromètres des risque des entreprises depuis 2020 (1), les risques cyber devraient se maintenir à ce niveau encore les 5 prochaines années (2) tel que le prévoit France Assureurs, devant les risques climatiques et les catastrophes naturelles.

Il est désormais convenu d'entendre « ce n'est pas SI mais QUAND cela vous arrivera … ».

Dans ces conditions, il est légitime de s'interroger sur la pérennité de l'assurance cyber (la question fait occasionnellement la une des médias) et sur l'intérêt d'y souscrire.

Voyons plutôt en quoi le recours à l'assurance va concourir à développer la résilience des entreprises et autres organisations, et pourquoi les autorités tentent de clarifier le marché de l'assurance cyber afin de favoriser son recours compte-tenu de son rôle clé dans la protection des entreprises

L'assurance cyber, condition nécessaire à la sécurité économique des PME et ETI

Si les entreprises font face à un risque croissant, les PME et les Entreprises de Taille Intermédiaires sont particulièrement exposées. Leur surface financière les rend attractives pour les attaquants et la plupart d'entre elles n'ont pas encore consenti aux investissements de protection jugés nécessaires par les assureurs. Ces deux facteurs les rendent difficilement assurables : seules 0,2% des PME sont assurées et 9% des ETI (3). Même si l'on peut estimer que ces chiffres ont quelques peu progressé en 2022, cela reste très insuffisant.

La méconnaissance de la plus-value de ces contrats d'assurance associée à une sous-estimation de la gravité du risque n'explique pas à elles seules cette sous-assurance. Ceci était vrai en partie jusqu'à la crise Covid.

Le marché a en effet connu un revirement

très fort depuis 2020, sous l'effet de la très forte dégradation de la sinistralité subie par les assureurs (4), et il s'est inversé : Avant 2020, il était encore « relativement » aisé de pouvoir souscrire des couvertures assurance, toute catégorie d'assurés confondue : TPE, PME, ETI et Grands Comptes. Ces derniers avaient d'ailleurs pour la plupart signé ces garanties, bénéficiant de cartographies des risques plus élaborés et de ressources financières supérieures. Les résultats de ces programmes étaient relativement rentables de l'aveu même des assureurs spécialisés. Ces derniers parvenaient à rendre leurs offres attractives avec des critères d'éligibilités accessibles, et des niveaux de primes et de garantie satisfaisants.

L'explosion des sinistres cyber, ransomware en tête, a eu des conséquences sur les conditions de souscription et de renouvellement dès 2021. Et les niveaux de primes, qui avaient même tendance à baisser jusqu'en 2019 du fait d'une relative concurrence, ont remonté brutalement, accompagnés par des limitations de montants garantis, une hausse des franchises, et désormais plus fréquemment, des sous-limitations pour certains risques (ransomware, carence du prestataire IT, risque systémique).

Aujourd'hui, malgré une meilleure sensibilisation au risque, les PME et les ETI rencontrent des difficultés pour s'assurer du fait des conditions de prix élevées et/ou d'accès à l'assurance (nouveaux critères d'éligibilité). L'assurance cyber peut être perçue comme dissuasive. Les grands-comptes recherchant même des solutions alternatives avec la création de captives telle que MIRIS (5).

Ce constat est jugé insatisfaisant par les pouvoirs publics qui veulent permettre à l'assurance de jouer un rôle essentiel dans la prévention du risque, dans l'aide à la gestion de crise et dans la protection des bilans des entreprises. Car, ne pas s'assurer sur le risque principal en pleine tempête, c'est faire peser un risque majeur sur les organisations, qu'elles soient privées ou publiques. Mais c'est également faire peser un risque sur toute la chaine de valeur clients / fournisseurs.

A titre d'exemples, voici quelques exemples de tarifs relevés sur la fin d'année 2022 (avec des disparités dans les niveaux de couvertures proposés – limitations, franchises – expliquant en partie les écarts)

PME (plasturgie) – CA 10 M€ - Plafond de garantie souhaité : 1 M€
- **Prime annuelle :** proposition variant de 2 à 5 K€

PME (édition de logiciels) – CA 30 M€ - Plafond de garantie souhaité : 2 M€
- **Prime annuelle :** proposition variant de 15 à 35 K€

Institution financière – CA 120 M€ - Plafond de garantie souhaité : 4 M€
- **Prime annuelle :** proposition variant de 80 à 150 K€

C'est pourquoi, sous l'impulsion de la Direction Générale du Trésor, la loi LOPMI a été débattue au parlement fin 2022 afin de permettre le recours à l'assurance, tout en le conditionnant à plusieurs mesures décisives dont l'obligation du dépôt de plainte sous 72 heures pour donner droit à toute indemnisation par l'assurance. Une autre décision majeure qui a fait, et fera encore débat : la licité du remboursement des rançons (à concevoir en ultime recours) par les assureurs, afin de débloquer un marché indispensable à la survie des entreprises.

D'autres mesures, moins spectaculaires mais non moins efficaces ont été reprise par la Direction Générale du Trésor : favoriser le partage des données et les synergies entre les acteurs publics et privés pour développer la connaissance de ces risques évolutifs, et accéder à une meilleure maîtrise du risque.

Une dynamique de promotion et d'organisation de la résilience s'est mise en marche. Il est désormais fréquent que les assureurs soient associés à des réunions de sensibilisation regroupant l'ANSSI, la gendarmerie, les acteurs de la cyber sécurité et des acteurs de l'assurance afin de porter à la connaissance des dirigeants le panel des moyens et ressources à mettre en œuvre.

Le risque cyber, un nouveau risque à maîtriser pour le secteur de l'assurance

Pour les assureurs, le risque cyber a ouvert un nouveau champ d'activité qu'il s'agit de maîtriser. Le principe de

(1) Baromètre des risques d'Allianz AGCS

(2) La cinquième édition de la cartographie des risques de France Assureurs

(3) Rapport AMRAE - Lucy 2022 (p 13)

(4) Rapport AMRAE - Lucy 2022 (p 19/20)

(5) https://www.argusdelassurance.com/assurance-dommages/risques-d-entreprise/cyber-miris-la-mutuelle-des-entreprises-obtient-son-agrement.209426

l'assurance est de déporter le risque de l'assuré vers l'assureur afin que l'assuré ne soit pas mis en danger par une situation critique à laquelle il ne saurait faire face. Pour accepter ce déport de risque et l'assumer de manière pérenne, l'assureur va travailler sur trois facteurs : l'analyse du risque, la prévention (pour éviter la survenance), la prise en charge financière et l'accompagnement à la gestion de crise (en cas de survenance).

L'analyse du risque

L'analyse de risque est réalisée par l'assureur avant l'entrée en garantie pour accepter ou refuser le risque et le tarifer. Cette étape est essentielle pour proposer aux entreprises assurées une pérennité du programme et une maîtrise des tarifs, garanties et conditions de souscription. Les effets de la sélection initiale sont renforcés par les questionnaires et / ou audits de renouvellement réalisés chaque année.

La prévention

La prévention vient compléter l'analyse du risque qui aura identifié les points de vigilance sur lesquels l'entreprise doit porter ses efforts de protection. A l'instar des assurances incendie obligeant le chef d'entreprise à installer sprinklers et extincteurs, l'assurance cyber requiert des mesures de protection qui s'ajustent dans le temps à l'évolution de ce risque. Au titre des précautions à prendre, la sauvegarde des données est systématiquement exigée afin de faciliter les actions de remédiation en cas de CryptoLocker, sans passer par le remboursement de rançon, ce que tout assureur cherche à éviter. Les contrôles d'accès au système d'information via MFA (authentification multi facteurs), la mise en œuvre de cloisonnement du SI (Tier Model) font partie des niveaux de sécurité à mettre en place. L'assureur partage avec l'entreprise assurée le besoin de limiter le risque au maximum.

La prise en charge financière et l'accompagnement en cas de crise

Toujours dans l'objectif de maîtriser le risque, la première action de l'assureur sera d'aider l'entreprise dans ses premiers pas dans la crise, car ils sont déterminants pour en limiter la portée. Cette prestation est assurée pour le compte des assureurs par des sociétés spécialisées, la plupart du temps sans limitation. Elle est particulièrement importante dans le contexte des PME et ETI qui n'ont généralement pas la capacité, en termes de ressources et de compétences nécessaires, de circonscrire la crise et éviter qu'elle ne s'étende. Ce n'est que dans un deuxième temps que les autres éléments de la garantie seront actionnés, selon le choix d'étendue des garanties opéré par l'entreprise : les garanties dommages : perte d'exploitation et frais supplémentaires d'exploitation (ex : mise en place d'une plate-forme tel pour informer les clients) ; les garanties en responsabilité civile (en cas de mise en cause de l'entreprise sur les conséquences d'une cyber attaque), le remboursement de la rançon (désormais encadrée par la loi LOPMI et à n'envisager qu'en dernier recours). La sélection initiale des risques et les démarches de prévention demandées par l'assureur limitent très fortement (et c'est le but) les situations ou le paiement de la rançon est nécessaire.

Les dispositifs d'assurance cyber contribuent à créer un écosystème de protection autour de nos entreprises. Ils représentent une force agissante pour compléter sur le terrain les actions de la gendarmerie, des acteurs de la cyber sécurité et bien sûr de l'ANSSI qui guident l'ensemble des travaux.

L'assurance cyber est en passe de devenir indispensable pour les 146 000 PME (7) et les 5400 ETI françaises (6) lorsqu'elles recherchent un financement auprès de banques ou de fonds d'investissement. Pour les mêmes raisons de garantie de continuité d'activité, elle devient rapidement une norme pour participer à des appels d'offres.

Les réseaux de distribution d'assurance, très agissants sur le terrain auprès des entreprises françaises (40 000 intermédiaires d'assurances) (8) doivent désormais évoluer et se former pour accompagner les entreprises dans la gestion de ce nouveau risque. ■

(6) https://www.economie.gouv.fr/files/2021-12/2022-0105-DP-strategie-nation-ETI.PDF)

(7) https://www.economie.gouv.fr/cedef/chiffres-cles-des-pme

(8) https://www.economie.gouv.fr/facileco/assurance-assureurs-mediation)

PME du cybercrime vs cybersécurité des grandes organisations :

qui est David, qui est Goliath ?

La cybermenace se maintient en 2022. Les attaquants ont du temps, de l'argent, cherchent toujours de nouveaux moyens d'arriver à leurs fins et affichent aujourd'hui plus de capacités à se spécialiser, s'organiser et à monter en expertise. Les gains sont colossaux pour les attaquants et par rebond les conséquences financières des attaques sont toujours plus importantes pour les organisations touchées. Quelles sont les attaques les plus courantes et où en sont les grandes organisations dans leurs investissements en cybersécurité ?

GÉROME BILLOIS,

Directeur de la practice Cybersécurité, société Wavestone

Des attaques majoritairement opportunistes et qui visent des gains financiers

La motivation première des attaquants reste financière. Ainsi, le *ransomware* (attaque visant à voler des données et à bloquer le système d'information en chiffrant les ordinateurs et les serveurs puis à demander une rançon) demeure la menace numéro une des organisations : 51% des incidents gérés par le CERT Wavestone (CERT-W) ont impliqué ce type d'attaque. La nature opportuniste des attaquants signifie que tous les secteurs et toutes les entreprises peuvent être touchées. Ces groupes d'attaquants **se sont largement professionnalisés pour devenir des PME du cybercrime.** Par exemple, lors du démantèlement du groupe de cybercriminels CONTI, les autorités ont pu évaluer leur revenu annuel à 160M$ en 2021 et que la structure comptait au moins 65 membres. Basés sur l'expérience terrain du CERT-W, nos calculs de rentabilité estiment qu'un attaquant peut percevoir un ROI compris entre 200% et 800% ! **Ces entreprises du crime sont aujourd'hui dotées de services de recrutement, RH, finance, expertises techniques, équipes d'intrusion…** Ils font largement de la publicité pour leurs activités afin de recruter de nouveaux cybercriminels, notamment en publiant des offres d'emplois.

Plus ciblés, les autorités relèvent aussi de **nombreux cas d'espionnage et de déstabilisation**, industriels et étatiques, tels que mentionnés dans le Panorama de la Cybermenace 2022 publié par l'Agence nationale de sécurité des systèmes d'informations (ANSSI).

Enfin, certains secteurs médiatiquement exposés sont particulièrement soumis à **des attaques de type « *hacktivismes* »** qui visent à faire passer des messages

idéologiques ou à nuire à une organisation ou à une marque. Ces attaques sont souvent de faible intensité mais peuvent être très visibles dans les médias.

Les attaquants pénètrent dans les systèmes majoritairement à cause d'un mail de *phishing* et/ou à l'utilisation de comptes utilisateurs volés. Il y a donc encore une marge de progression concernant la sensibilisation des collaborateurs et la protection de nos messageries. On note toutefois que ces dernières années des investissements massifs ont été réalisés dans de nombreuses grandes structures pour sécuriser leur SI (accès conditionnel, authentification à facteurs multiples, définition de règles de détection d'incidents cyber…), entraînant concrètement une réduction du temps de détection d'une attaque non-négligeable. A titre indicatif, le temps de détection d'une intrusion est passé en moyenne de 94 jours en 2020 à 35 jours en 2022 d'après le rapport CERT-W.

Quel est le niveau de maturité en cybersécurité des grandes organisations ?

Wavestone mesure régulièrement le niveau de maturité des grandes organisations. Pour ce faire, nous maintenons un benchmark auprès de 100 structures (représentant plus de 3 millions d'utilisateurs) afin d'évaluer leur niveau de maturité autour des 16 thèmes clés de la cybersécurité. Les résultats sont sans appel : **les organisations françaises n'engagent pas encore assez de moyens (humains et techniques) pour se protéger contre des attaques.** En effet, en moyenne et tous secteurs confondus, les organisations de notre échantillon ont obtenu la note de 46/100 en matière de maturité cyber par rapport aux exigences des normes internationales.

Les niveaux sont en revanche très disparates selon les filières. Les acteurs les plus matures sont ceux sur lesquels la pression réglementaire est la plus forte, en particulier le secteur financier et les structures soumises à la directive NIS (texte européen imposant des mesures de sécurité pour les infrastructures critiques) ou à la LPM (Loi de programmation militaire, imposant des niveaux de sécurité minimum aux structures identifiées comme d'importance vitale par l'Etat).

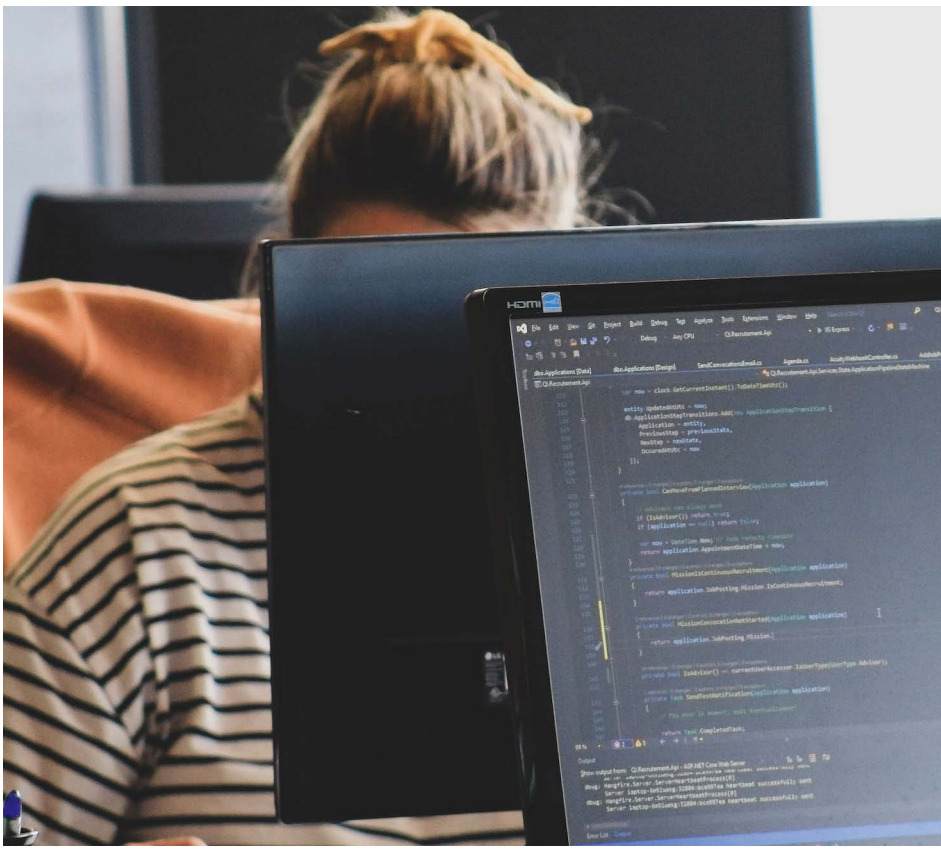
Le budget dédié à la cybersécurité est aussi trop faible : il est mesuré à 6,1% du budget informatique. Là encore les différences sectorielles sont importantes, le financement de grands programmes de cybersécurité varient entre 100 et 800M d'euros dans le secteur de la finance contre 15 à 80M d'euros pour l'industrie par exemple.

Quels sont les priorités d'investissement ?

S'assurer de la mise en œuvre des mesures essentielles

Il existe des défis techniques à relever pour bloquer les attaques les plus fréquentes. Sur les technologies de protection, les deux mesures phares que sont les EDR (outil de protection avancée des ordinateurs et serveurs) et **l'authentification multi-facteurs** (MFA) ont connu des déploiements importants ces dernières années.

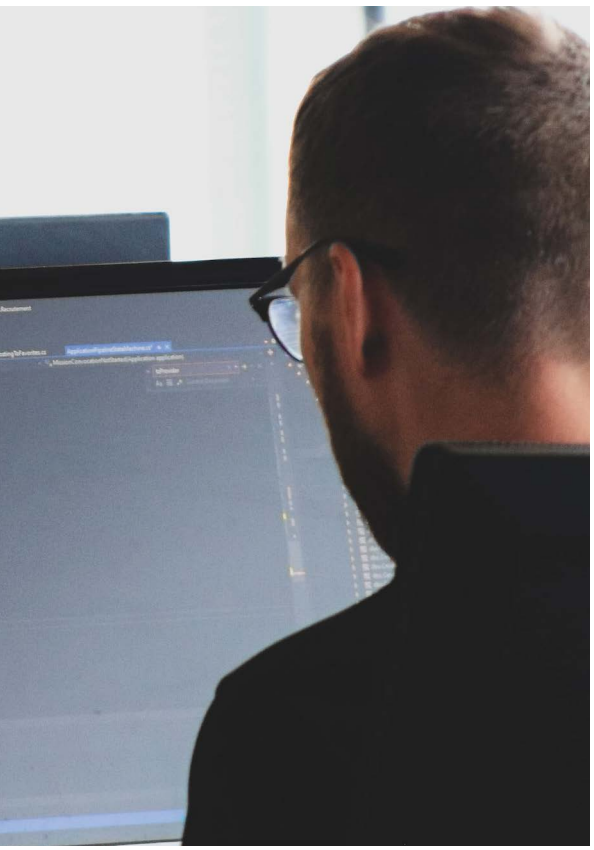
Toutefois beaucoup reste à faire, notamment sur la **sécurité de *l'Active Directory*** (brique technique peu visible



qui gère l'ensemble des droits d'accès aux informations et aux ordinateurs dans la plupart de systèmes d'information), cible numéro un des attaquants puisque ce composant est impliqué dans 90% des crises gérées par le CERT-W l'année dernière. Dans votre plan d'investissement n'oubliez pas non plus d'inclure les **sauvegardes**, et en particulier d'étudier leur externalisation et leur capacité à résister à une attaque *ransomware*. Enfin, les sujets les plus en difficulté aujourd'hui restent la **sécurité des applications et des données**, en particulier du fait du volume d'actifs concernés, et, de manière plus surprenante, **la sécurité cloud.** Sur ce dernier point, de très mauvaises pratiques sont en vigueur, souvent car il y a un faux sentiment de sécurité du fait des discours des fournisseurs. Un exemple concret : plus de 42% des organisations évaluées permettent l'accès d'administration à leur système cloud avec un simple login / mot de passe.

S'entourer d'une équipe compétente

Mais ces boucliers et mesures techniques ne feront pas tout. Vous devez aussi disposer de compétences en cybersécurité… et elles sont rares actuellement : plus de 3 millions d'emplois vacants dans le monde, dont 15 000 en France et 700 000 aux Etats-Unis. Aussi d'après notre benchmark, seulement 1 personne pour 1500 employés en moyenne est dédiée à la cybersécurité, ce qui est loin d'être suffisant pour couvrir tous les nouveaux sujets associés : résilience, gestion du budget cyber, analyse des vulnérabilités, etc. Evidemment **le recrutement est une piste mais il ne faut pas négliger non plus les mobilités internes ou l'usage de sociétés spécialisées pour vous accompagner.** Dans tous les cas, vous devez savoir qui dans votre organisation est en charge de la cybersécurité.



Mettre en place des investissements pluriannuels

Vu l'ampleur des besoins et la durée des projets, il est souvent nécessaire de piloter un programme de remédiation cybersécurité sur plusieurs années. Il pourra s'appuyer sur les piliers du référentiel NIST quia vous aidera à prioriser vos projets en fonction des enjeux *Identify, Protect, Detect, Respond, Recover.*

Cette approche pluriannuelle permet de lisser ses investissements entre lancement de projets (phase de *Build*) et leur maintien (phase de *Run*). La gestion d'un budget cyber est un sujet complexe qui requiert l'adoption d'un cap et de la flexibilité. Pour le piloter efficacement il faut **connaître ses besoins présents et anticiper ses besoins futurs**, qui souvent évoluent rapidement au regard de la menace.

Conclusion

L'impact financier d'une attaque contre les organisations devient de plus en plus critique compte tenu des moyens importants mis en œuvre par les attaquants. Les menaces se multiplient aussi à cause du nombre d'applications utilisées pour produire et fournir leurs activités, dans un contexte d'organisation étendue. La guerre entre attaquants et responsable de la cybersécurité est donc loin d'être terminée. Pour se prémunir et réduire les impacts il faut **engager plus d'efforts dans la sensibilisation des collaborateurs, la protection de son SI et faire de la résilience sa priorité.** ■

Cybersécurité, l'urgence absolue

La cybercriminalité est la « criminalité du XXIème siècle », thème du 1er Forum International de la cybersécurité (FIC), en 2007. A l'époque, peu de décideurs prenaient la question au sérieux. Aujourd'hui, elle est le fléau qui menace non seulement les personnes physiques et morale - avec le risque pour les entreprises de ne pas se relever après une cyberattaque - mais aussi les Etats.

Marc WATIN-AUGOUARD,

Chef de la Majeure « Souveraineté numérique et Cybersecurité à l'IHEDN

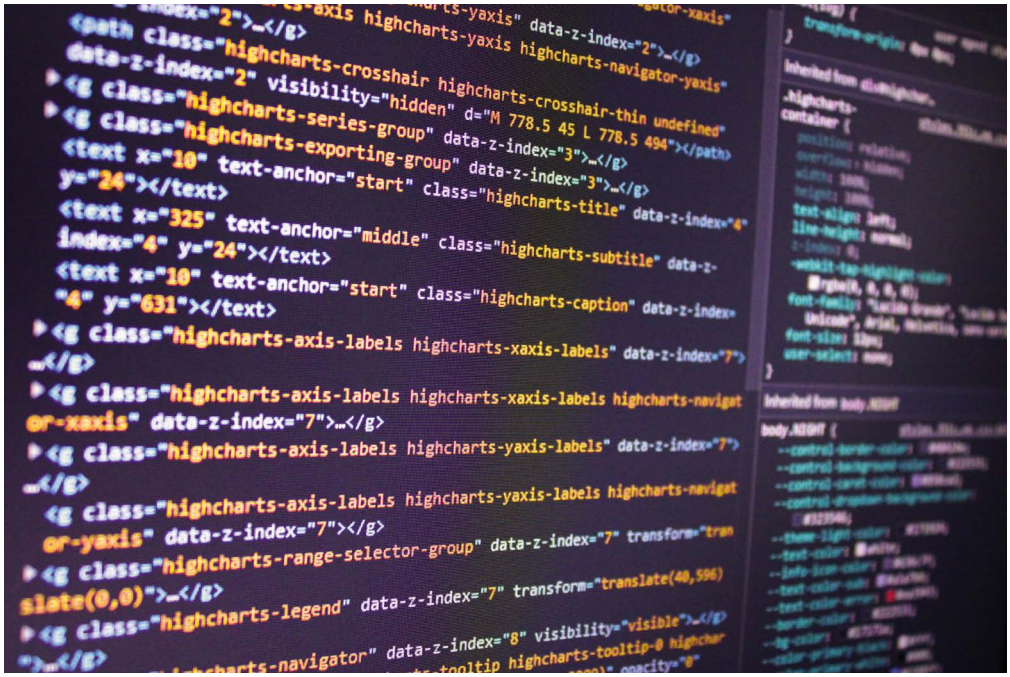
Pour comprendre cette évolution, il faut observer la « tectonique des plaques ». La cybercriminalité est le fruit d'un double mouvement : la migration des délinquants vers le cyberespace s'accompagne d'une migration des Etats et d'organismes paraétatiques qui le pénètrent pour mener des actions « infra-guerre » ou pour accompagner leurs actions de guerre cinétique par des opérations cybernétiques.

Le délinquant est généralement plus intelligent qu'on ne le pense. Agir dans le cyberespace offre pour lui le meilleur rapport avantage/risque pénal. Jamais il n'a été aussi près de sa victime ; jamais il n'a été aussi loin de son juge ou de son gendarme, car il peut agir à distance, depuis un Etat « cybervoyou » qui ne coopère pas ou, pire, encourage les prédateurs.

La deuxième migration vient de certains Etats peu respectueux du droit international ; elle rejoint la première. Jadis, les Etats avaient recours à la force pour s'en prendre à un autre Etat. C'était la politique de la canonnière. Aujourd'hui, sans renoncer à la force, ils trouvent dans l'espace numérique un terrain propice à des actions masquées, en dessous du seuil de l'agression armée, qu'ils confient le plus souvent à des cybercriminels en groupe organisé agissant pour leur compte, afin de mieux brouiller les pistes. S'ils ne sont pas pris, ils reçoivent le salaire de leur turpitude. Dans le cas contraire, l'Etat déclare les ignorer et promet une action vigoureuse venant de lui qui, comme il l'a toujours affirmé, met tout en œuvre pour lutter contre la cybercriminalité. Si les images de certaines arrestations s'arrêtent devant la porte de la prison, il est établi qu'il existe une sortie donnant accès aux services secrets. La règle de la « diligence due » qui impose à un Etat de ne pas tolérer une action hostile depuis son territoire est ici bafouée.

Cette tendance lourde devrait s'accélérer, la cybercriminalité s'inscrivant dans une zone grise, hybride. Si l'Etat n'accentue pas sa stratégie d'action, notamment avec l'augmentation sensible de ses capacités d'investigation et de poursuite des prédateurs, le risque est grand de voir sa légitimité remise en cause, car sa première justification est de protéger les personnes physiques et morales et les biens matériels et immatériels.

Dans le « monde réel », la sécurité relève essentiellement de la puissance publique. Dans l'espace numérique, en revanche, l'Etat doit composer



avec de nombreux acteurs privés qui possèdent une part importante de la réponse, ne serait-ce qu'en raison de leur connaissance de la menace et de leurs offres de cybersécurité. Par les capteurs qu'ils déploient ou les systèmes basés sur l'IA qu'ils mettent en œuvre, ils ont une vision en temps réel des cyberattaques et des comportements dont ne disposent pas les ministères régaliens. Le partenariat public-privé est parfaitement illustré par l'écosystème israélien, à Be'er Sheva, ville ayant poussé dans le désert du Néguev. Y sont rassemblées des universités, des centres de recherche, des startups, des entreprises du numérique, des acteurs étatiques (armée, police). C'est sur ce modèle que se créent, en France, les Campus Cyber, dont le premier vient d'ouvrir ses portes sur l'esplanade de la Défense. 1800 acteurs publics et privés, civils et militaires se croisent, se rencontrent, partagent leur expérience de la cybersécurité. Le partenariat public-privé est aussi l'une de motivations de la création du FIC en 2007. Mais cette manifestation, la plus importante en Europe et qui s'implante au Canada (FIC Nord Amérique), est aussi un lieu où s'exprime la volonté de développer la coopération internationale. Sans elle, point de salut ! Comment, en effet, lutter contre un phénomène transfrontalier en limitant son champ d'action à l'intérieur des frontières ? Europol, agence européenne de coopération, marque des points, chaque fois que plusieurs états mettent en commun leur renseignement et leurs capacités d'investigation.

A supposer que tout l'arsenal public et privé soit en ordre de bataille, cela ne suffirait pas pour permettre de sécuriser une « métamorphose numérique » qui n'en est qu'à ses balbutiements. Avec l'hyperconnexion qu'annoncent la 5G puis la 6G, il faut désormais résonner de manière systémique, en construisant une cybersécurité collective et collaborative. Les territoires (départements, régions) retrouvent une raison d'être, dans un monde numérique apparemment sans frontière. Parce qu'ils rassemblent des acteurs qui se connaissent, ils peuvent être ces espaces d'échange et de solidarité sans lesquels il ne peut y avoir de résilience.

La cybersécurité, c'est d'abord un état d'esprit, une conscience partagée, avant d'être le résultat de technologies. Au sein des institutions, des entreprises, des collectivités territoriales et des services publics qui leur sont rattachés, la cybersécurité ne doit pas être le monopole des spécialistes (DSI, RSSI, directeurs de la sûreté, etc.). Chacun est concerné, en commençant par le COMEX qui doit désormais hisser la question au niveau stratégique. La question n'est pas de savoir si on va être attaqué, mais quand ? Cela signifie qu'il faut anticiper,

planifier l'organisation de la gestion de crise cyber à venir.

Le coût de la cybersécurité est parfois présenté comme un obstacle, eu égard au coût exorbitant d'un RSSI, d'un centre de supervision (SOC), d'un EDR, même si la mutualisation peut souvent apporter une réponse. Est aussi invoqué le coût de l'assurance cyber. Ces arguments ne doivent pas être balayés, car ils constituent un obstacle pour beaucoup d'entités.

En vérité, si l'on considère que 85% des incidents sont d'origine humaine, c'est l'acculturation de tous au risque cyber qui est sans doute la mesure la moins coûteuse et donc la plus accessible. La gendarmerie nationale multiplie les actions de sensibilisation. La DGSI en fait de même au profit d'entreprises sensibles. Il faut aller encore plus loin pour développer une conscience partagée sur le risque cyber qui ne concerne pas seulement les autres. Toute personne, toute entreprise, toute administration connectée est une cible potentille, surtout si elle offre une faible défense. Les collectivités territoriales, les hôpitaux ont cru à une protection absolue du fait de leur mission de service public. On mesure aujourd'hui le résultat !

Dans le monde réel, nous avons la chance de compter sur les pompiers en cas d'incendie, sur des policiers et gendarmes pour arrêter les délinquants. Mais cela n'interdit pas- au contraire – de développer une politique de prévention mise en œuvre à titre individuel et collectif. Il ne viendrait à personne l'idée de jeter un mégot allumé dans sa corbeille, de laisser sa porte ouverte à tous vents. Pourtant, c'est ce qui arrive trop souvent encore dans notre utilisation de l'outil numérique. Comme le souligne l'Agence nationale pour la sécurité ses systèmes d'information (ANSSI), la première démarche est d'adopter une « hygiène informatique » qui évite bien des déconvenues.

Finalement, sans négliger l'apport des technologies, la cybersécurité est d'abord l'agrégation de nos comportements. Il est donc urgent de replacer l'humain au cœur de la cybersécurité. ■

Les entreprises de la finance dans la tourmente du ransomware

PHILIPPE LUC,

CEO & Cofondateur ANOZR WAY, 12 ans chez Malakoff Médéric comme Directeur Commercial France et Directeur Marché

La cybermenace s'intensifie d'année en année, qu'il s'agisse de ransomware[1], de fraude au président, ou d'autres types d'attaques. **En 2022, les attaques par ransomware ont augmenté de 35% par rapport à 2021, soit 1 attaque revendiquée toutes les 3h dans le monde,** selon le Baromètre ANOZR WAY du Ransomware[2]. Les entreprises du secteur de la finance ne font pas exception : le secteur fait partie du top 10 des secteurs les plus visés en France en 2022.

8 attaques cyber sur 10 ciblent les dirigeants et collaborateurs

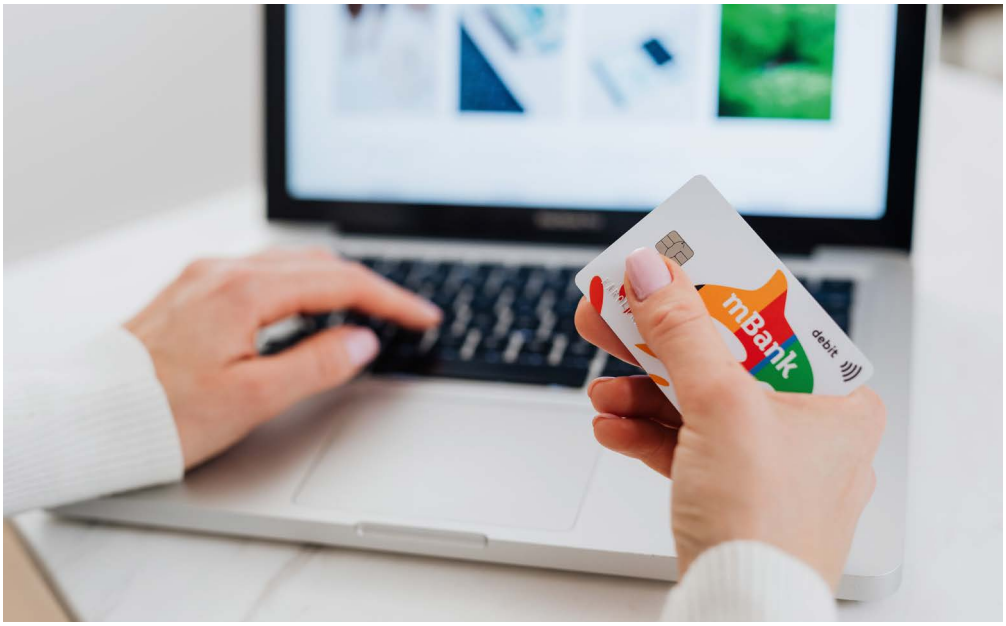
Les efforts sont souvent portés sur la sécurisation du système d'information. A juste titre, mais ce n'est malheureusement pas suffisant… Surtout quand l'on sait que **8 attaques cyber sur 10 ciblent les dirigeants et collaborateurs.** Cela signifie que les cybercriminels pour contourner les systèmes de sécurité techniques visent directement les personnes au sein de l'entreprise.

Les pirates ont bien compris que **l'humain était une porte d'entrée possible sur le système d'information.** Ils privilégient les messages piégés (hameçonnage/ phishing) personnalisés et ciblés. Pour cela, ils se renseignent en amont sur leur cible, en collectant toutes les informations disponibles sur le web, que ce soient les données publiques des profils de réseaux sociaux ou les données fuitées qui se trouvent sur le darkweb. Ils se font aussi passer pour un membre de votre entourage professionnel ou personnel pour maximiser les chances de réussir leurs attaques.

Les dirigeants et managers, cibles privilégiées

Plus d'1 dirigeant sur 3 a été victime d'escroqueries par hameçonnage en 2022, soit **12x plus que les autres collaborateurs**. Les dirigeants, membres du COMEX, CODIR, cadres, sont des cibles privilégiées pour les cybercriminels, de par leur statut et par leur accès à des documents confidentiels ou données sensibles.

A leur insu, **de nombreuses informations d'identité sont en libre accès sur le web et darkweb** à cause de fuites de



données issues d'autres cyberattaques (hôpitaux, collectivités, e-commerces, etc.) : documents d'identité, adresse du domicile, données bancaires, e-mails et mots de passe...

Les conséquences peuvent être multiples : usurpation d'identité, arnaque financière, etc. Une fois les données personnelles recueillies, la personne malveillante peut utiliser l'identité d'un dirigeant dans une "fraude au président", ou d'une personne du service comptabilité pour demander de réaliser un virement en urgence, autrement dit une "fraude au faux virement" (FOVI).

L'impact colossal des cyberattaques

Les attaques par ransomware peuvent être particulièrement destructrices pour les entreprises dans le secteur de la finance, particulièrement prises pour cibles en raison des informations sensibles et confidentielles qu'elles traitent. Cela entraîne ainsi **la perte de données sensibles concernant les clients, un impact sur le chiffre d'affaires, des pertes financières, une chute de la valorisation boursière et une atteinte à la réputation de l'entreprise.**

La perte de chiffre d'affaires annuel par entreprise consécutive à un ransomware est estimée en moyenne à 27%, hors paiement éventuel d'une rançon qui peut s'élever jusqu'à 128 000€ en moyenne par entreprise[3]. **Pour l'année 2022, l'impact économique est de 2,8 milliards d'euros de perte de chiffre d'affaires pour les entreprises françaises victimes de ransomware.**

Comment se prémunir des cyberattaques ?

Au-delà des mesures de sécurité techniques à mettre en place pour se protéger des cyberattaques (sauvegarde régulière, maintien des logiciels à jour...), **il est nécessaire de prendre en compte l'aspect humain.**

Il est important de sensibiliser les utilisateurs aux risques et de leur enseigner les bonnes pratiques de sécurité comme reconnaitre les pièges des e-mails de phishing.

En amont, pour qu'ils deviennent des cibles beaucoup plus difficiles à atteindre, il est nécessaire que chacun soit conscient de toutes les informations le concernant exposées en ligne. En maîtrisant cette empreinte numérique, on complexifie le travail des pirates lorsqu'ils se renseignent sur une entreprise et son personnel. Ils choisiront alors de passer leur chemin et de s'en prendre à une cible beaucoup moins complexe.

En étant informé, vigilant et en mettant en place des actions correctives, chacun contribue à la protection de son entreprise contre les cyberattaques. ■

[1] Ransomware : type de logiciel malveillant qui crypte les fichiers d'une victime. Les attaquants demandent ensuite une rançon à la victime pour rétablir l'accès aux fichiers moyennant paiement.

[2] Baromètre ANOZR WAY du Ransomware - Bilan 2022 & Prévisions 2023 https://anozrway.com/fr/barometre-ransomware/

[3] Hiscox

Dans quelle mesure la sécurité et la régulation des blockchains peuvent-elles générer des coûts financiers ?

VICTOR WARHEM,
Économiste
chez BSI Economics

Depuis quelques années, avec l'explosion du secteur des cryptoactifs, les blockchains se sont imposées comme des solutions populaires pour échanger et stocker des données en ligne. Les blockchains se développent de plus en plus dans le domaine de la finance, mais également dans bien d'autres, comme celui des chaines d'approvisionnement, des services notariaux, de la comptabilité, etc. Le secteur de la blockchain pourrait représenter à ce titre plus de 1 000 milliards USD d'ici 2030, contre moins de 20 aujourd'hui.

Néanmoins, même si elles présentent par nature un degré de sécurité cryptographique élevé, elles peuvent être sujettes à des cyberattaques, engendrant ainsi des coûts de cybersécurité supplémentaires et incitant les régulateurs à définir un cadre réglementaire stricte. Qu'en est-il plus précisément dans leur secteur « historique », le secteur financier ?

Des blockchains publiques bien plus perméables aux cyberattaques que les blockchains privées

La blockchain est un registre numérique distribué et décentralisé auquel il est possible d'accéder selon certaines modalités, qu'il est possible d'utiliser pour émettre ou stocker des informations, des actifs numériques, pour valider des transactions, et qui fonctionne grâce à des protocoles algorithmiques déterminant comment une transaction est validée – ce qu'on appelle communément le mécanisme de consensus.

Il convient de distinguer trois types de blockchains : de manière schématique, les blockchains publiques présentent les registres les plus distribués et décentralisés en matière d'émission, d'accès, d'utilisation, et de participation au mécanisme de consensus, tandis que les blockchains privées se caractérisent par un contrôle d'une autorité ad-hoc des acteurs pouvant émettre les actifs, accéder aux registres, utiliser la blockchain, et/ou participer à la validation des transactions. Enfin les blockchains hybrides, où l'autorité ad-hoc donne accès à tout le monde tout en gardant la main sur le mécanisme de consensus, constitue une catégorie à part tout en présentant des caractéristiques pour la plupart comparables aux blockchains privées.

Les blockchains privées – dont les plus grandes sont produites par Hyperledger Fabric, Quorum ou R3-Corda – sont utilisées pour tout type d'application blockchain, y compris dans le domaine financier. Peu d'informations publiques relatives à leurs coûts de cybersécurité ou de régulation sont disponibles – probablement, justement, en raison

de leur caractère privé. Elles peuvent néanmoins en théorie faire face à des attaques de déni de service, ou à des attaques « des 51 % » - où les pirates prennent le contrôle de plus de 50 % des nœuds utilisés pour la validation des transactions et corrompent le mécanisme de consensus pour extraire des fonds de la blockchain. Néanmoins, les organisations à l'origine des grandes blockchains privées (Linux Foundation pour Hyperledger Fabric, ou JP Morgan puis ConsenSys pour Quorum) sont réputées présenter des niveaux de cybersécurité adéquats tout en étant conformes aux régulations si elles existent. Leurs blockchains sont d'ailleurs généralement sollicitées pour améliorer le niveau de cybersécurité des organisations qui y souscrivent. Les montants qui ont été volés ou perdus sur ces blockchains ont ainsi très nettement inférieures à ceux qui l'ont été sur les blockchains publiques.

En effet, la question de la cybersécurité se pose bien davantage pour les blockchains publiques. Si elles portent en elles une promesse de sécurité – en réalité plutôt de résilience – et de transparence, elles connaissent de nombreux types de défaillance depuis leurs débuts. Tout d'abord, les plus petites, malgré leur décentralisation, peuvent au même titre que les blockchains privées être corrompues par une attaque « des 51 % » (comme l'a subi le Ronin Network en mars 2022 avec une perte de 624 millions USD). Au-delà des attaques touchant au mécanisme de consensus, elles sont surtout vulnérables dans leur « périphérie », à commencer par les « contrats intelligents » – algorithmes de service financier impliquant des cryptoactifs – dont le code n'a pas été suffisamment testé et présentent des failles comme dans le cas du piratage de la blockchain Poly Network en 2021 ayant conduit à une perte de 611 millions USD. Les portefeuilles de dépôts des fonds présentent aussi souvent des failles de sécurité et l'hameçonnage est monnaie courante pour s'emparer des identifiants des portefeuilles d'utilisateur. Par ailleurs, d'autres types de cyberattaques sont possibles : malwares, ransomware, exploitation des « ponts » entre blockchains, etc. Il a ainsi été démontré que, parmi les projets sur blockchains publiques présentant un montant total sous gestion supérieur à 10 millions €, 6,2 % avaient été piratés ces dernières années, selon KPGM. En 2022, les montants volés ou perdus excédaient ainsi les 3 milliards USD, bien que ces vols et pertes aient dans certains cas été le travail de créateurs de blockchain malveillants, et pas de failles de cybersécurité.

Les fournisseurs de service financier : au cœur des enjeux de cybersécurité

Sur qui reposent les coûts de cybersécurité « possibles » dans l'univers des blockchains publiques ? Sur plusieurs types d'acteurs : les fournisseurs de service financier (FSF[1]), les émetteurs de cryptoactifs s'il y en a, les utilisateurs qui stockent leurs fonds, et enfin les « validateurs » (*miners* en anglais) des mécanismes de consensus qui permettent à la blockchain de fonctionner et qui participent aussi généralement à sa gouvernance. Hormis les FSF, ces acteurs sont souvent difficilement identifiables et leurs coûts de cybersécurité sont mal connus.

Les FSF représentent au contraire des acteurs financiers plus « classiques ». Leurs coûts de cybersécurité se concentrent potentiellement sur la sécurisation de leur interface sur Internet, des liquidités dont ils disposent et des services qu'ils vendent. Le mécanisme de consensus des plus grandes blockchains publiques de l'écosystème ne leur sont pas accessibles, mais les plus utilisées, Bitcoin et Ethereum, n'ont jamais été piratées grâce à leur niveau très élevé de décentralisation. Compte tenu des liquidités importantes qu'on y trouve, les fournisseurs les plus susceptibles de connaitre des cyberattaques sont les *exchanges*, plateformes d'échange de cryptoactifs, qu'elles soient centralisées (comme Binance) ou décentralisées. Par exemple, l'*exchange* Coincheck a subi un vol d'environ 500 millions USD de liquidités en 2018.

Comment les fournisseurs de services peuvent-ils concrètement améliorer leur cybersécurité ? En auditant régulièrement par le biais de cabinets externes leurs différents services et/ou en engageant un responsable ou une équipe en charge

1/ Ces fournisseurs n'incluent pas les protocoles – notamment ceux de la finance décentralisée – non gérés par une entité unique. Pour ces contrats intelligents de la finance décentralisée, il est très difficile d'améliorer la cybersécurité même si nombre d'entre eux présentent des failles exploitables. Si une faille est découverte, il faut compter sur un développeur spécialisé pour créer une nouvelle version depuis le protocole de base.

de la cybersécurité. Pour l'heure, il manque cruellement de ressources humaines dans ce domaine, avec un nombre d'expert en cybersécurité de contrats intelligents compris entre 1 000 à 1 500 à l'échelle mondiale, selon KPMG.

Renforcement de la cybersécurité, cap sur 2025 avec la réglementation MiCA

Le règlement MiCA, dont le vote a été repoussé au Parlement européen en avril 2023, et dont l'application est attendue à horizon 2024-2025, devrait néanmoins constituer une manière efficace de stimuler ce secteur en obligeant les FSF utilisant les blockchains publiques dans l'Union européenne (UE) à élever leur niveau de cybersécurité. En France, ils sont une soixantaine disposant d'un enregistrement PSAN – pour Prestataire de Services sur Actifs Numériques –, qui les oblige déjà à mettre en place un dispositif de lutte contre le blanchiment et de financement du terrorisme et donc à identifier les utilisateurs.

En effet, les Fournisseurs de Service de Cryptoactifs (Crypto-Asset Service Providers, CASP) – statut qui va remplacer tous les autres pour les fournisseurs de services dans l'Union – seront bientôt tenus à des exigences en matière de gestion des risques et de sécurisation des fonds, notamment en souscrivant à une assurance, ce qui semble pour l'heure difficile à obtenir dans ce secteur et pourrait finalement s'avérer très coûteux. Ils n'auront par ailleurs d'autres choix que d'allouer des ressources pour sécuriser portefeuilles, interfaces, contrats intelligents, et éventuellement mécanismes de consensus de validation si possible. S'agissant des autres coûts réglementaires des CASP, ils seront liés notamment aux obligations de respecter les exigences prudentielles en matière de fonds propres (allant de 50 000 à 150 000 euros minimum en fonction du type de structure), de réserves (au moins 25 % de leurs frais généraux de l'année précédente), et de liquidité (déterminées dans les textes à venir de l'Autorité européenne des Marchés Financiers).

Les coûts liés à la mise en place du règlement européen MiCA ont été estimés par l'étude d'impact du règlement. Ainsi pour ce qui est des fournisseurs de services devant se mettre au diapason de la régulation européenne d'ici 2024-2025, il faut compter entre 35 000 et 75 000 euros pour la confection obligatoire du « livre blanc » définissant le projet – si cela n'est pas déjà fait. À cela s'ajoute entre 2,8 et 16,5 millions € pour la mise au niveau réglementaire, qu'il s'agisse de la mise au niveau en termes de cybersécurité ou en termes de gouvernance, etc. Il faudrait compter en plus de ces coûts uniques des coûts annuels compris entre 2,2 et 24 millions € pour satisfaire les exigences réglementaires européennes. Pour ce qui est du cas spécifique des *stablecoins*, les exigences réglementaires sont encore plus drastiques compte tenu d'une part de l'interdiction de toucher des intérêts pour les utilisateurs des *stablecoins* mais aussi de l'obligation de maintenir un niveau de réserve prudentiel extrêmement élevé pour pouvoir endurer de grandes fluctuations dans le niveau de la demande.

Coûts de cybersécurité en Europe : forte hausse mais effets incertains

Ainsi, les coûts obligatoires de cybersécurité et de régulation pour les FSF sur blockchain publique vont drastiquement s'élever ces prochaines années dans l'Union européenne. Le pari est fait que cette mise au pas réglementaire pourrait aider les acteurs des blockchains publiques à minimiser les vols et pertes liés à leurs services, générant ainsi une confiance et une demande accrue en Europe.

Néanmoins, puisque ces utilisateurs auront toujours accès aux services fournis par des acteurs extra-européens via Internet – à leurs risques et périls –, le règlement européen pourrait au contraire entraver le développement du secteur en Europe. Les prochains mois seront décisifs pour mieux comprendre la tendance qui l'emportera. Un premier test sera la mise en place d'ici l'automne 2023 d'un enregistrement PSAN renforcé en France.

À long-terme, la menace des ordinateurs quantiques et l'arrivée du règlement « MiCA 2 », destiné en théorie à réguler les autres acteurs des blockchains publiques, devraient constituer une nouvelle source de coûts pour le secteur, qui aura peut-être d'ici là connu un essor suffisant pour que « le jeu en vaille la chandelle ». ■

Article rédigé en janvier 2023

Le risque Cyber dans le domaine bancaire

Nous habitons un monde dans lequel la connexion est devenue reine. Grâce à elle, mais aussi grâce aux terminaux de toutes sortes par lesquels elle s'exprime, nous communiquons à la vitesse de la lumière dans notre univers numérisé. Nos démarches sont simplifiées, notre réactivité est exemplaire. Et nos organisations s'en trouvent grandies, améliorées.

Vincent
MÉRIC de BELLEFON,

Directeur Cybersécurité-Risques IT du Groupe Crédit Agricole et Directeur Général Adjoint CA-GIP (Credit Agricole Group Infradtructure Platform)

Bien qualifier le risque cyber

Pourtant, car il y a un revers à toute médaille, un risque nouveau est apparu en corollaire de cette évolution bénéfique : **le risque cyber.** Et il ne cesse de croître et de menacer ces mêmes organisations, enrichies par les fonctionnalités nouvelles du digital, mais aussi dépendantes de leur transformation digitale. Bien évidemment, cette menace concerne les banques au même titre que toutes les entreprises. Pour bien la comprendre, encore faut-il bien la qualifier. Elle pose, en effet, trois problèmes importants : **la confidentialité, l'intégrité et la disponibilité.**

Les banques disposent de toutes sortes de données extrêmement précieuses. Elles concernent les clients, les collaborateurs, le marché, les paiements, etc…. Les Cybercriminels chercheront à mettre la main dessus pour les exporter de manière illicite en vue de les revendre ou d'exercer un chantage à la publication (risque de confidentialité). Ils essaieront de les manipuler en vue de fraudes ou de destruction (risque d'intégrité). Ou, enfin, ils tenteront de bloquer les systèmes (risque de disponibilité).

Avant les années 2014-2015 le risque portait essentiellement sur la surface exposée sur Internet (les sites web, les serveurs B2B, etc.). Désormais, la multiplicité des portes d'entrée peut mener l'attaquant au cœur même du réseau de l'entreprise. On peut citer pêle-mêle les PC dont la conception et la surveillance sont inadéquates (ports USB non restreints, anti-virus obsolètes…), l'internet des objets (IOT), les réseaux WiFi mal sécurisés.

Les fondamentaux de la réponse des établissements financiers

Les établissements financiers sont exposés aux mêmes menaces que tout autre type d'entreprise. Une différence toutefois, et de taille : lorsqu'un de leur client subit une attaque, en particulier une fraude, celle-ci peut avoir des répercussions sur l'établissement lui-même. Il est donc d'autant plus prégnant pour eux d'établir une ligne de défense efficace.

Très tôt, les établissements ont développé des chaines de défenses basées sur quatre principes clefs : **la prévention, la protection, la détection et la réaction.**

La prévention rassemble les actions autour de l'analyse de la menace, de la formation des parties prenantes de

la sécurité du système informatique, de la sensibilisation de l'ensemble du personnel, de la gestion adéquate des droits d'accès aux applications et aux systèmes et de la mise en place d'équipes spécialisées comme le CSIRT ou la Red Team.

La protection est plus une question de matériel. Elle concerne par exemple les équipements de filtrage des flux, dispositifs de blocage des logiciels malveillants, durcissement des configurations logicielles, chiffrement, signature électronique des transactions, etc…

La détection résulte d'un état d'alerte permanent qui permet par exemple, le repérage du déclenchement d'un logiciel suspect dans un poste de travail ou l'activité anormalement élevée d'un serveur , etc…. Elle amène également au repérage des échanges, internes aux réseaux, typiques d'une attaque en cours.

Enfin, la réaction représente le dernier stade, celui de l'urgence. C'est la mise en place d'un dispositif de gestion de crise ou d'équipes fonctionnant, selon l'urgence en mode commando ou au fil de l'eau.

Les fondamentaux de la réponse du Crédit Agricole

Pour un groupe comme le Crédit Agricole, composé de systèmes d'informations complexes, multiples, eux-mêmes répartis dans les nombreuses structures juridiques constituant un Groupe, il est fondamental d'assurer une homogénéité des pratiques. Cela passe par des corpus de règles et de normes, définies pour chaque domaine de l'informatique (développements, gestion des identités, conception des réseaux, protection des données, etc.).

Par ailleurs, une attention particulière a été portée, et depuis longtemps, à la constitution d'une communauté de professionnels de la cyber sécurité répartie sur tous les aspects : sécurité des applications, sécurité des infrastructures, détection, anticipation, cryptographie. Elle travaille de concert avec les maîtrises d'ouvrage, les products owners et d'autres spécialités telles que la protection des données à caractère personnel et la conformité.

En complément, au niveau de chaque entité, des collaborateurs spécialisés sont dédiés à cette surveillance numérique. De même, à l'échelle du Groupe, une équipe traite le sujet cyber mais aussi celui des risques IT, et coordonne cet effort en lui donnant force et cohérence.

Autre rouage essentiel de cette démarche de sécurité, la sensibilisation et la formation des collaborateurs aux activités hostiles dont ils peuvent être la cible. Une information permanente est organisée

autour de cette thématique dans les newsletters du Groupe. Des actions spécifiques et récurrentes sont mises en place : tests de sensibilité au phishing, campagnes de communication, formation obligatoire annuelle, parcours ludiques et digitaux à l'occasion du cyber mois. Il faut présenter les messages de façon originale, souvent décalée et éviter le côté anxiogène inhérent au propos. Trouver le juste ton est un exercice complexe.

Enfin, des unités dédiées au contrôle évaluent continuellement les systèmes et les pratiques et émettent des recommandations. Ainsi, le CSIRT centralise les demandes d'assistance, traite les alertes, effectue la veille, échange les informations avec d'autres unités équivalentes,..... La Red Team, quant à elle, détecte, prévient et élimine les vulnérabilités en imitant le rôle d'un attaquant et en trouvant les chemins d'intrusion, étape par étape, vers une cible en exploitant les vulnérabilités des ordinateurs et autres composants informatique mais aussi des processus et de l'environnement physique.

S'ajoute à ce travail permanent les travaux de la Direction Risques Groupe et de l'Inspection Générale ainsi que les audits des superviseurs (ACPR, BCE notamment).

Et les clients dans tout ça ?

Il est inconcevable de laisser le client sur le bord du chemin. Les établissements financiers représentent une véritable chaîne dont le client fait intimement partie. C'est pourquoi les banques sensibilisent en continu leurs clients particuliers et entreprises : sites web de banque en ligne, courriers, fascicules distribués en agence, newsletters, événements spécifiques... Dans le Groupe Crédit Agricole, les rencontres pluriannuelles des Caisses Régionales avec leurs sociétaires, représentent autant occasions de passer les messages de cybersécurité.

D'un point de vue plus technique, les moyens mis à disposition des clients apportent des fonctions de sécurité avancées (validation des ordres, authentification multi-facteurs, plafonnement des transactions ainsi que d'autres moyens internes et confidentiels).

De même, les ordres de paiement sont analysés et les transactions suspectes sont bloquées ou sur-contrôlées.

La menace cyber prend souvent une tournure dramatique pour les entreprises. Les ransomwares peuvent remettre en cause une santé financière considérée comme saine. C'est pourquoi certains établissements financiers proposent des services d'accompagnement à la mise en place de mesures de cyber-protection, ainsi que des offres d'assurances.

Notre monde s'est digitalisé. Le réel et le virtuel se côtoient désormais naturellement. De même, les menaces se sont développées dans ces deux univers. Aujourd'hui, le risque cyber n'est plus nouveau. Nous avons appris à y faire face. L'efficacité de nos réponses respectives dépend de notre organisation collective, mais aussi de notre capacité d'étonnement individuelle.

Nous devons toujours avoir à l'esprit, que **lorsqu'il y a un doute... c'est qu'il n'y a pas de doute.** ■

La cyber sécurité : une opportunité de développement et de business pour le secteur financier

Nicolas FERREIRA,

Directeur Général Adjoint chez Finance Innovation.

Organisateur de l'événement Cyber Day – Cybersécurité et Métiers de la Finance : une opportunité de transformation pour la banque et l'assurance

La sécurité est un des piliers fondateurs de toute relation avec ses clients, et c'est un des atouts majeurs de l'écosystème financier qui, étant responsable de masses financières conséquentes, est sensibilisé depuis longtemps au sujet. S'il est toujours possible de faire mieux, et toujours nécessaire de rester à la pointe de la lutte contre des risques cyber évoluant très rapidement, les acteurs de la finance ont un niveau de maturité certain. Ils sont un tiers de confiance reconnu, et c'est d'ailleurs un de leurs avantages concurrentiels majeurs face aux fintechs et autres acteurs technologiques.

Dans ce contexte changeant, la question est de savoir comment, dans le cadre d'une digitalisation toujours plus poussée, la protection contre les risques cyber et la lutte contre la fraude peuvent être une opportunité pour développer de nouveaux business models et de nouvelles relations avec ses clients. Comment la sécurité, socle de confiance, peut faciliter et fluidifier les relations avec le client, tout en établissant le bon niveau de sécurité, qui doit être rassurant sans entraver les parcours.

La cybersécurité, au-delà de l'informatique

Afin d'intégrer la cybersécurité au sein d'une démarche réellement tournée vers le business, elle doit être approchée sous un angle élargi, au-delà de la vision IT traditionnelle : les failles informatiques qui pourraient être exploitées, permettant à des intrus d'infiltrer les systèmes, afin soit de voler des données, soit de bloquer des systèmes et demander des rançons (rançongiciels). Les RSSI et CISO sont les gardiens du temple, mais ils peuvent parfois être cornérisés, coupés des métiers, en ayant une approche purement informatique. Ils peuvent être perçus comme des freins à l'innovation, au lieu d'être un atout dans la relation avec le client.

Pour autant, qu'il s'agisse de l'entrée en relation avec le client, l'analyse crédit, la gestion de patrimoine ou la gestion backoffice et la conformité, la fraude documentaire, l'usurpation d'identité ou la fraude informatique se mélangent de plus en plus : y a-t-il finalement une réelle sécurité lorsqu'un client envoie un scan d'une pièce justificative par mail ? Comment vérifier son authenticité, et même l'identité de celui qui a envoyé le mail ? Les outils technologiques pour sécuriser l'identification d'un client ou une transaction relèvent-ils de la cybersécurité ou du KYC ? Le règlement DORA sur la résilience opérationnelle numérique invite justement à avoir une approche élargie des risques.

L'innovation fintech au service de la sécurité

Un grand nombre de solutions proposées par des fintechs et startups permettent d'intégrer de la sécurité de manière agile et le moins douloureuse possible pour le client : Netheos mets

en place par exemple des solutions de souscription à distance et de signature électronique, alors que Share ID, grâce à des technologies de reconnaissance faciale, permet l'authentification d'une personne grâce à son sourire, et ce sans stockage de données personnelles biométriques. Enfin, il existe également des approches combinant sécurité et conformité comme celles proposées par exemple par Vialink, afin d'adresser largement la sécurisation du parcours client et le KYC.

Le paiement est un terrain de jeu particulièrement fertile pour la fraude, mais aussi pour l'innovation : MoneyTrack utilisera ainsi la technologie blockchain pour sécuriser les versements par les mutuelles, collectivités et institutions financières à des particuliers. Stream Mind utilise l'intelligence artificielle afin de croiser les coordonnées bancaires et personnelles pour sécuriser les virements, alors que la carte Handsome s'attaque à la fraude lors du paiement en caisse par les malvoyants, qui sont très souvent victimes de fraude lors du passage en caisse. Sans parler bien sûr du Buy Now Pay Later, dont une grande partie du métier des fintechs est la gestion du risque lié à la fraude comme ce que propose Algoan.

Au-delà des solutions de sécurisation internes et techniques du secteur financier, les institutions financières doivent-elles être des acteurs plus proactifs dans la protection de l'économie ?

Le banquier, l'assureur, sont des tiers de confiance des entreprises. Ils sécurisent leur quotidien de plusieurs manières, que ce soit financièrement ou dans leur business (par exemple en fournissant ou prescrivant des solutions de paiement sécurisées pour les commerçants et e-commerçants). Dans ce cadre, ces institutions ont à la fois la légitimité et un réel intérêt à contribuer également à la sécurisation face aux risques cyber et à la fraude de leurs clients.

Un client bien protégé face aux menaces cyber est tout d'abord un client moins risqué financièrement, mais c'est aussi un client plus serein et mieux fidélisé. Il existe désormais des initiatives de la part du secteur bancaire afin de sécuriser leurs clients : LCL s'est associé par exemple à Almond et Board of Cyber, afin d'encourager ses clients à faire un diagnostic de vulnérabilité et engager une démarche de protection.

Le Crédit Agricole Alpes Provence, partant du constat que la sécurité devien,t de plus en plus un enjeu fort pour ses clients, a créé sa filiale Cyber Way, alliant diagnostic et accompagnement à la mise en place de bonnes pratiques face au risque cyber.

Et l'assurance dans tout ça ?

Le secteur de l'assurance n'est pas en reste et poursuit son travail de couverture des risques, en clarifiant son offre et en l'adaptant aux divers types d'acteurs :

- Les TPE/PME sont peu attaquées, mais leurs systèmes informatiques sont plus vulnérables et leur pronostic vital est souvent engagé quand cela arrive : selon une étude de la CCI, 60% des entreprises subissant une attaque mettent la clé sous la porte dans les six mois après une cyberattaque
- Les ETI sont de plus en plus des cibles de choix : elles présentent des retours financiers intéressants pour les attaquants tout en étant moins bien protégées que les grands groupes
- Les grands groupes sont globalement bien couverts, mais face à la difficulté de prévoir les risques et couvrir des masses financières importantes, ils pourraient de plus en plus avoir recours aux captives en internalisant la gestion de ces risques

Afin de répondre à ces problématiques de nouvelles offres d'assurance cyber émergent, notamment avec des insurtechs comme Stoïk ou DattaK, dont l'objectif est double : 1/ faciliter la montée en compétence des TPE/PME en matière de risques cyber et 2/ leur permettre de bénéficier d'une couverture assurancielle simple et adaptée à leur taille.

Notre économie est depuis plusieurs années face à un stress permanent en termes de sécurité numérique, avec la digitalisation forcée suite à la crise Covid et la généralisation du télétravail, la guerre en Ukraine, mais aussi un mouvement de fond de digitalisation depuis les années 2000. La mise en lumière des risques cyber doit être une opportunité pour les institutions financières de renouer avec leurs clients, en affirmant leur rôle de tiers de confiance grâce à l'innovation. ■

Pourquoi le risque cyber est aussi l'affaire des Directions Financières

MAXIME CARTAN,
Co-fondateur et CEO

ALFREDO GARCIA,
CFO, Citalid

Les entreprises de toutes tailles et de tous secteurs s'appuient chaque jour un peu plus sur la technologie pour piloter l'ensemble de leurs opérations. En parallèle, les menaces cyber évoluent au rythme de ces avancées technologiques et du contexte géopolitique.

Directions financières et RSSI : unis face au risque cyber

Si les RSSI sont en première ligne face au risque informatique, la cybersécurité n'est pas seulement un problème technologique ; c'est un sujet qui concerne toutes les fonctions de l'entreprise. Pour qu'une entreprise valorise son image de marque, préserve la confiance de ses clients et sa stabilité financière, des mesures de cybersécurité appropriées doivent être mises en place pour protéger les actifs et les données.

Pour réduire la pression de la menace, il faut la comprendre et évaluer les risques qui en découlent. Cette évaluation précise du risque permet ainsi aux directeurs financiers de projeter une véritable stratégie d'investissement au sein de leur organisation.

Les dépenses de sécurité passent parfois au second plan par rapport à des priorités informatiques ou commerciales. Par conséquent on constate que les entreprises sont parfois mal préparées pour faire face aux menaces, notamment cyber. Il est essentiel de consulter le RSSI pour déterminer comment le financement pourrait contribuer au développement d'une culture de sécurité et de confidentialité. En valorisant la cybersécurité, la protection de la vie privée et la protection du partage de la donnée, les organisations améliorent leur profil de sécurité.

La difficulté à laquelle sont aujourd'hui confrontées les directions financières est la faible lisibilité, à la fois des réelles menaces qui pèsent sur leurs organisations et sur les réponses apportées par les fournisseurs de solutions technologiques. Nombreux sont les rapports et études qui mettent en lumière l'ampleur du risque cyber, sa technicité, sa force de frappe, etc. Pourtant, il est important pour chacun – au sein de sa propre organisation – de comprendre le risque qui lui est propre, en fonction de son industrie, de son périmètre géographique, de sa taille, etc.

Déployer les solutions de cybersécurité pertinentes, c'est-à-dire adaptées au risque spécifique de l'organisation, tout en faisant face aux contraintes financières associées est une problématique majeure pour les entreprises. Pour garantir que leurs activités sont suffisamment protégées contre les cyber-risques, les directeurs financiers doivent pouvoir s'appuyer sur des outils d'aide à la décision et ainsi accompagner les RSSI dans l'arbitrage des investissements réalisés.

Mesurer le risque cyber avec précision pour optimiser son pilotage

Les assureurs ont tout intérêt à collaborer étroitement avec les entreprises assurées pour comprendre la menace, les mesures de cybersécurité implémentées et les potentiels dommages. Cette collaboration, rendue possible par un modèle unifié de quantification du risque cyber, permettrait aux assureurs d'offrir une protection appropriée et de définir des polices qui représentent équitablement le degré de risque.

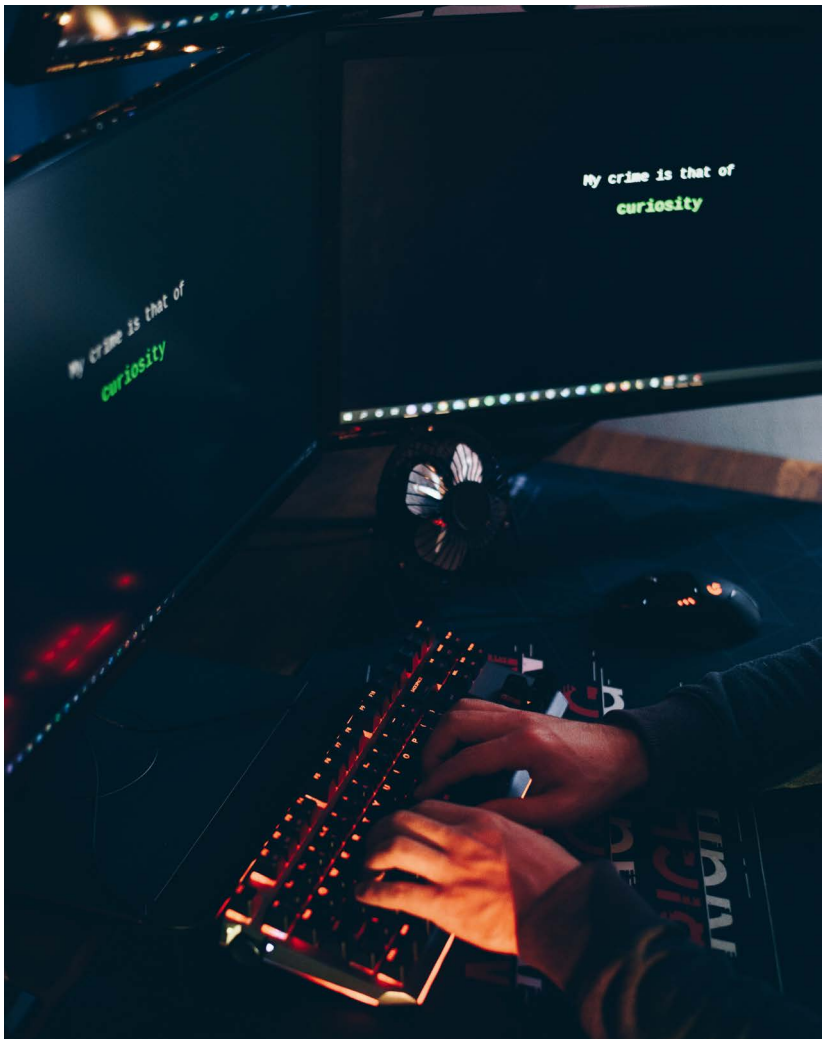
Les directions financières et les RSSI peuvent, ensemble, traduire le jargon de la cybersécurité en termes business et coordonner les risques et les objectifs de cybersécurité en objectifs organisationnels et stratégiques. C'est le cœur de l'exercice de quantification : traduire le risque cyber en risque financier. Ensemble, ils peuvent également définir le niveau de risque en fonction d'un secteur ou d'un environnement spécifique, en mettant en perspective les scenarios applicables à des entreprises similaires.

De la même manière, les directeurs financiers et les assureurs doivent également suivre les dernières positions légales et obligations de régulation en matière de cybersécurité. Accompagnés de la direction des risques, ils peuvent ainsi assurer une couverture et une maîtrise suffisantes et fixer des provisions qui reflètent fidèlement l'exposition. Pour cela il est essentiel que les assureurs et les sociétés quantifient en bonne intelligence les différents risques cyber de la structure.

Directions financières : un rôle-clé dans le pilotage de la stratégie cyber

Si la finance est l'un des secteurs les plus sensibles aux attaques cyber, il faut plus largement que toutes les directions financières participent activement au pilotage du risque cyber. Ce n'est qu'ainsi que la cybersécurité ne sera plus un coût pour l'entreprise, mais un investissement. Le directeur financier doit être bien informé sur les questions de sécurité informatique et le contexte juridique associé pour pouvoir ajuster l'allocation des ressources au regard de la nécessité de protection des actifs et données. Il doit hiérarchiser les objectifs de l'entreprise et tenir compte du retour sur investissement potentiel des solutions de sécurité et d'assurance pour offrir une couverture suffisante et fixer des provisions qui reflètent de manière appropriée le degré de risque.

Ainsi, il est important pour les parties prenantes de comprendre les tendances cyber pour pouvoir mieux les appréhender. Équipées d'un produit qui les accompagne dans cette compréhension des risques propres à leur organisation et des solutions qui pourraient les aider à le réduire, les directions financières joueront aux côtés des RSSI un rôle actif dans les prises de décisions et la définition d'une stratégie de pilotage du risque. Les fonctions traditionnellement dites « support » doivent devenir la clé de voûte de la résilience de l'entreprise, de sa réputation et de sa stabilité financière. ■



La cybersécurité des documents numériques :

un cas d'usage concret de la blockchain

THIERRY ARNALY,

Président de
Autenthic Blockchain.

La cybersécurité est un sujet de plus en plus prégnant, non seulement à cause des tensions internationales et de l'action des mafias, mais surtout parce que notre vie, professionnelle et privée, est de plus en plus digitalisée.

Le confinement de 2020 a été un formidable accélérateur de cette virtualisation. Il était soudain devenu impossible de sortir de chez soi, de rencontrer d'autres personnes. Instantanément les échanges se sont fait par mail, visioconférence, appels téléphoniques, … Et tout de suite les ennuis ont commencé car une grande partie de la population n'était pas prête.

Cette accélération brutale de la digitalisation a été l'origine d'une hausse exponentielle de la fraude des documents échangés avec les professionnels du Droit et du Chiffre, au premier rang desquels on a trouvé les responsables juridiques et financiers des entreprises. La fraude la plus connue est celle des RIB, qui consiste à remplacer lors d'échanges par mail un RIB original par celui des pirates.

Un risque de préjudices élevés et multiples

Les professionnels sont de plus en plus nombreux à subir des préjudices à cause de ces falsifications. Il s'agit bien sûr immédiatement de pertes financières. Elles peuvent s'élever à plusieurs centaines de milliers d'euros et au-delà. Pour le moment, les assurances professionnelles semblent encore couvrir le risque, mais nul doute qu'elles modifieront leurs conditions pour ne pas se mettre en danger face à un risque répété.

Au-delà de l'aspect financier, les entreprises sont soumises à un risque sur leur image. En effet, se faire piéger en impliquant involontairement des clients ou des fournisseurs va laisser des traces et ternir l'image professionnelle de la société. Des brèches apparaîtront concernant sa capacité de gérer son système d'informations.

Pour terminer, à plus long terme, on peut se demander si des clients ou des fournisseurs victimes de l'incapacité de l'entreprise à se protéger de la falsification de ses documents numériques ne pourront pas se retourner contre elle et engager une action en justice en soulignant sa responsabilité et en demandant des dommages et intérêts.

La blockchain, une technologie de rupture facteur de confiance

Comment empêcher définitivement ces falsifications ? Il faut créer une référence pour chaque document créé ou transféré pour pouvoir s'assurer que le document qu'on a entre les mains est bien conforme à cette référence, à l'original.

On pourrait imaginer un organisme

central qui réaliserait cette tâche. Il devrait être interprofessionnel et international. De plus, il doit être complètement indépendant et transparent pour que personne ne puisse douter des références créées.

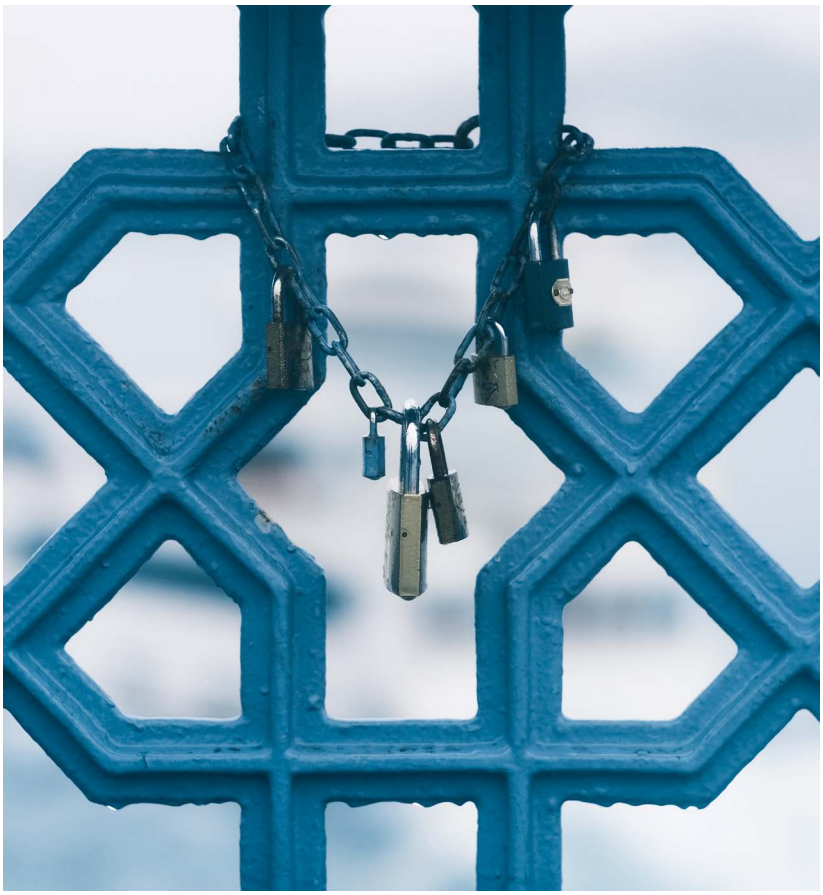
Aujourd'hui cet organisme n'existe pas, mais une technologie informatique révolutionnaire fournit ce service : la blockchain.

Cette technologie existe depuis une quinzaine d'années et son usage se diffuse lentement, mais surement, dans nos sociétés. Elle est connue en particulier pour servir de fondement au Bitcoin et autres cryptomonnaies. Elle est de plus en plus utilisée dans différents secteurs, de l'agriculture jusqu'au spatial, pour la confiance qu'elle confère aux informations qu'on y inscrit. En effet, elle n'autorise ni leur modification, ni leur suppression et elle leur attribue un horodatage certain, véritable preuve d'antériorité.

La blockchain fonctionne comme un registre qui serait dupliqué en temps réel sur des milliers de serveurs dans le monde et dont chaque page contient une référence infalsifiable, grâce à des algorithmes cryptographiques, qui synthétise le contenu des pages précédentes. De sorte que la moindre modification sur une page du registre sur un des serveurs est immédiatement détectée et corrigée.

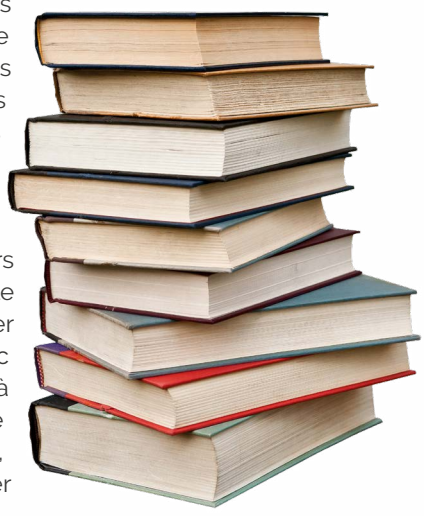
Authentic BlockChain utilise cette technologie pour garantir aux professionnels du Droit et du Chiffre que les documents numériques qu'ils sont amenés à traiter n'ont pas été falsifiés. La difficulté, outre le maniement de la blockchain elle-même, consiste à rendre la technologie invisible et à ne conserver que ses avantages.

Concrètement la sécurisation se passe de deux manières. Premier cas, lorsque le professionnel veut « figer » un document qu'il a créé, une première étape va consister à calculer l'empreinte numérique de ce fichier (Hash) avec une fonction comme SHA256 (qui se trouve sur tous les ordinateurs depuis des décennies). Cette empreinte (une suite de 32 caractères) est unique et ne permet pas de reconstituer



le fichier correspondant. C'est elle que l'on va écrire dans la blockchain. Authentic BlockChain utilise pour cela Polygon (MATIC), une blockchain publique de la famille Ethereum, ce qui permettra à terme de proposer de nouvelles fonctionnalités autour des smart contrats, qui sont des programmes informatiques exécutables inscrits dans la blockchain.

Conformément au RGPD, aucune information personnelle n'est inscrite dans la blockchain, puisqu'on ne pourrait plus les modifier ou les supprimer, même si la personne concernée le demandait. Toutes les informations personnelles sont donc remplacées par des codes dont on conserve les correspondances par ailleurs.



Le professionnel peut alors envoyer son fichier par mail. Le destinataire n'aura qu'à calculer son empreinte numérique avec la même fonction de hash et à la comparer avec celle stockée en blockchain. Si c'est la même, tout va bien ; sinon le fichier

a été modifié, par erreur ou pour une falsification.

Deuxième cas de sécurisation nécessaire, le professionnel veut récupérer un document en étant sûr qu'il n'a subi aucune modification. Il renseigne les coordonnées de son interlocuteur, celui-ci reçoit alors un mail lui indiquant la demande et lui permettant d'enclencher le processus, il arrive sur une page sécurisée où il saisit un code reçu par SMS pour s'identifier plus fortement, il sélectionne sur son ordinateur le fichier à transférer, celui-ci transite via une connexion sécurisée, son empreinte numérique est calculée et déposée dans la blockchain. Lorsque le professionnel veut le récupérer, avant de lui restituer revêtu d'un filigrane indiquant comment s'assurer de sa conformité avec l'original, le service contrôle que son empreinte numérique correspond toujours à celle déposée dans la blockchain. De cette manière, le document reçu est garanti à 100% conforme au document envoyé.

Un besoin de soutien en attendant l'adoption générale

La blockchain est encore considérée comme une technologie émergente et son adoption généralisée n'est pas prévue avant 2025. Pour le moment seuls quelques précurseurs utilisent cette technologie pour se mettre à l'abri de la fraude. Une « évangélisation » des entreprises et personnes concernées doit être réalisée (d'où cet article). La conduite du changement est fondamentale pour assurer une transition réussie. Un événement inattendu comme la pandémie pourrait accélérer ce processus, mais il vaut mieux ne pas le souhaiter.

L'usage de la technologie blockchain pour la cybersécurité des fichiers se différencie des coffres forts numériques et des signatures électroniques. Par rapport aux premiers, elle assure la sécurité même si le document n'est plus dans le coffre et elle permet de s'assurer de la conformité avec un fichier sans avoir à le divulguer. Par rapport aux secondes, elle ne nécessite pas de faire confiance à un acteur centralisé, elle conserve des informations opposables aux tribunaux (tel que l'horodatage) et elle fonctionne plus rapidement et à moindre coût.

Au final, ce qui est important, c'est de savoir que l'outil pour faire face à la falsification des documents numériques existe et qu'il faut se préparer à l'utiliser. La falsification des RIB n'est qu'une première étape et le risque de perte totale de confiance dans les informations échangées de façon numérique pourrait complètement bloquer les échanges et obliger à revenir à des remise de documents papier par des personnes formellement identifiées.

Le sens de l'histoire est bien sûr plutôt d'utiliser les bons outils, comme il y a une trentaine d'années lorsque tout le monde a commencé à se doter d'antivirus. Nul doute que, dans quelques années, la blockchain sera devenue une brique de cybersécurité évidente pour toutes les entreprises. ■

Confidential Computing : réinventer les modèles de sécurité avec AWS Nitro System

Le monde financier est confronté à des défis de sécurité croissants, avec des cyberattaques toujours plus sophistiquées. Le confidential computing, ou informatique confidentielle, est une des réponses à ces défis en renforçant la sécurité des données.

STEPHAN HADINGER,

Directeur de la Technologie AWS France

1. Pourquoi le Confidential Computing permet-il de renforcer la sécurité ?

Le confidential computing est une approche qui protège les données sensibles lorsqu'elles sont en cours de traitement. **Cette approche est complémentaire au chiffrement des données au repos (stockées) et en transit (pendant le transfert), car elle sécurise les données en mémoire, là où elles sont aussi vulnérables aux attaques.** Le confidential computing est apparu sur le devant de la scène au début des années 2010 et, depuis lors, il a suscité un vif intérêt dans le domaine de la recherche et développement (R&D). Les investissements massifs consacrés à cette technologie témoignent de son potentiel et de sa capacité à transformer la manière dont les entreprises gèrent et sécurisent les données. Dans le secteur financier, où la confidentialité et l'intégrité des informations sont cruciales, le confidential computing joue un rôle essentiel pour préserver la sécurité des données et la confiance des clients.

2. Comment AWS réinvente les modèles de sécurité en proposant AWS Nitro System par défaut sur ses services?

Amazon Web Services (AWS), leader dans le domaine du cloud, a développé une solution innovante appelée **AWS Nitro System.** Il s'agit d'un ensemble de technologies qui permet d'améliorer les performances et la sécurité des services cloud d'AWS. **C'est une exclusivité AWS,** notamment disponible dans la Région Paris d'AWS depuis 2017. Concrètement, ce sont des cartes accélératrices que nous mettons dans chaque serveur. Ces cartes améliorent les performances, réalisent du chiffrement à la volée de toutes les données entrantes et sortantes. Mais surtout ces cartes créent une barrière physique de sécurité.

AWS Nitro System empêche même les opérateurs d'AWS d'accéder aux données des clients. **On peut comparer le système Nitro à un coffre-fort sans serrure** : même si quelqu'un voulait accéder aux données à l'intérieur, il ne pourrait pas le faire, faute d'outils. En utilisant le système AWS Nitro, la sécurité des données est renforcée car il élimine la possibilité d'accès non autorisé par les clients et restreint techniquement l'accès à tout opérateur, y compris les employés d'AWS. AWS Nitro System crée ainsi une barrière physique qui empêche tout accès à vos données pendant les courts moments où ces données sont en clair dans les unités de traitement des serveurs. Le développement du système Nitro a permis de repenser radicalement

l'architecture de virtualisation pour offrir une sécurité optimale aux clients. AWS a réussi à créer une solution de sécurité puissante et flexible adaptée aux besoins des entreprises du secteur financier.

3. Donner aux clients le contrôle de leurs données.

Grâce au confidential computing, AWS Nitro System met en place un environnement où AWS ne peut techniquement pas accéder aux données de ses clients, sans leur autorisation explicite. Cette approche est cruciale pour protéger les données des entreprises financières contre les demandes d'accès de la part d'autorités étrangères. Elle s'inscrit dans une approche plus globale d'AWS concernant la sécurité : **donner aux clients le contrôle de leurs données.**

Aujourd'hui, le contrôle des ressources numériques, ou souveraineté numérique, est plus important que jamais. C'est pourquoi nous avons récemment lancé l'***AWS Digital Sovereignty Pledge*** – notre engagement à offrir à tous les clients AWS l'ensemble le plus avancé d'outils et de fonctionnalités de contrôle disponibles dans le cloud au service de la souveraineté.

Contrôle de l'emplacement de vos données
AWS a toujours permis à ses clients de contrôler l'emplacement de leurs données. Aujourd'hui en Europe, par exemple, les clients ont le choix de déployer leurs données dans l'une des huit Régions existantes. Nous nous engageons à fournir encore plus de services et de capacités pour protéger les données de nos clients. Nous nous engageons également à développer nos capacités existantes pour fournir des contrôles de localisation des données encore plus précis et transparents. Nous allons également étendre les contrôles de localisation des données pour les données opérationnelles, telles que les informations relatives à l'identité et à la facturation.

Contrôle fiable de l'accès aux données
Le système AWS Nitro, qui constitue la base des services informatiques d'AWS, utilise du matériel et des logiciels

spécialisés pour protéger les données contre tout accès extérieur pendant leur traitement sur les serveurs EC2. Nous nous engageons à continuer à développer des restrictions d'accès supplémentaires qui limitent tout accès aux données de nos clients, sauf indication contraire de la part du client ou de l'un de ses prestataires de confiance.

La possibilité de tout chiffrer, partout
Aujourd'hui, nous offrons à nos clients des fonctionnalités et des outils de contrôle pour chiffrer les données, qu'elles soient en transit, au repos ou en mémoire. Tous les services AWS prennent déjà en charge le chiffrement, la plupart permettant également le chiffrement sur des clés gérées par le client et inaccessibles à AWS. Nous nous engageons à continuer d'innover et d'investir dans des outils de contrôle au service de la souveraineté et des fonctionnalités de chiffrement supplémentaires afin que nos clients puissent chiffrer l'ensemble de leurs données partout, avec des clés de chiffrement gérées à l'intérieur ou à l'extérieur du cloud AWS.

Depuis décembre 2022, AWS permet à ses clients, directement ou via un tier de confiance, de gérer et sécuriser les clés de chiffrements à l'extérieur du Cloud AWS. En France, ATOS et THALES proposent notamment de tels services.

La résilience du cloud
La souveraineté numérique est impossible sans résilience et sans

capacités de continuité d'activité lors de crise majeure. Le contrôle des charges de travail et la haute disponibilité de réseau sont essentiels en cas d'événements comme une rupture de la chaîne d'approvisionnement, une interruption du réseau ou encore une catastrophe naturelle. Actuellement, AWS offre la plus haute disponibilité de réseau de tous les fournisseurs de cloud. Chaque Région AWS est composée de plusieurs zones de disponibilité (AZ), qui sont des portions d'infrastructure totalement isolées. Pour mieux isoler les difficultés et obtenir une haute disponibilité de réseau, les clients peuvent répartir les applications sur plusieurs zones dans la même Région AWS. Pour les clients qui exécutent des charges de travail sur place ou dans des cas d'utilisation à distance ou connectés par intermittence, nous proposons des services qui offrent des capacités spécifiques pour les données hors ligne, le calcul et le stockage à distance. Nous nous engageons à continuer d'améliorer notre gamme d'options souveraines et résilientes, permettant aux clients de maintenir leurs activités en cas de perturbation ou de déconnexion.

Conclusion

Le confidential computing, et plus particulièrement AWS Nitro System, redéfinissent la manière dont les entreprises financières peuvent protéger leurs données sensibles. **AWS Nitro System est une technologie de pointe qui renforce la sécurité des données pour les entreprises dans le domaine financier.** En combinant le chiffrement en mémoire avec le chiffrement au repos et en transit, le Confidential Computing s'impose comme une protection essentielle pour les entreprises qui manipulent des informations financières sensibles. ■

L'assurance du risque Cyber

Réflexions sur l'article 5 de la loi LOPMI

La loi N°2023-22 d'orientation et de programmation du ministère de l'intérieur du 24 janvier 2023 qui contient quelques dispositions sur le risque cyber a introduit un nouvel article dans le code des assurances au N°L.12-10-1[1] qui est entré en vigueur le 24 avril 2023.

PIERRE MINOR,
Avocat associé,
Coat Haut de Sigy de Roux Minor,
membre du HCJP

La suppression du mot rançon

Les rédacteurs de cette nouvelle disposition se sont sensiblement éloignés de la rédaction initialement proposée dans le projet de loi[2]. Cette nouvelle disposition qui peut surprendre à plus d'un titre prévoit en effet que le versement de toute somme au titre d'un contrat d'assurance visant à indemniser les personnes morales et les personnes physiques dans le cadre de leurs activités professionnelles des pertes et dommages causés par une cyber attaque, et plus largement par une atteinte à un système de traitement automatisé de données, est subordonné au dépôt d'une plainte de la victime auprès des autorités compétentes au plus tard 72 heures après la connaissance de l'atteinte par la victime.

L'article 5[3] du projet de loi avait initialement pour objectif d'encadrer les clauses de remboursement des rançongiciels par les assurances, en conditionnant ce remboursement au dépôt rapide d'une plainte par la victime, au plus tard 48h après le paiement de la rançon, afin, pour reprendre l'exposé des motifs du projet, d'améliorer l'information des forces de sécurité et de l'autorité judiciaire et de « casser » le modèle de rentabilité des cyber attaquants.

Cette rédaction initiale présentait d'un point de vue juridique plusieurs avantages. Elle confirmait tout d'abord expressément la licéité des clauses des contrats d'assurance qui prévoient l'indemnisation des rançons payées par les victimes de cyber attaques. Elle qualifiait ensuite justement ces demandes de rançons, d'extorsion, telle que prévue par l'article L312-1 du code pénal permettant de rappeler que celui qui paye la rançon est avant tout une victime. Elle subordonnait enfin le versement de l'indemnisation du paiement d'une rançon par les assureurs au dépôt de plainte par la victime auprès des autorités compétentes au plus tard 48 heures après le paiement de la rançon et non pas 72 heures après la connaissance de l'atteinte à un système de traitement automatisé de données comme c'est le cas désormais.

Pour les parlementaires le mot « rançon » devait être supprimé du texte de loi car d'aucun aurait pu y voir un encouragement à ces pratiques criminelles. En procédant de la sorte le législateur enlevait à cet article sa portée initiale qui était de créer un cadre juridique pour l'indemnisation des rançons pourtant nécessaire au développement d'un marché de l'assurance du risque cyber.

Un champ d'application large

Désormais le champ d'application de l'article L12-10-1 du code des assurances est extrêmement large puisqu'il conditionne le paiement de toute somme au titre d'un contrat d'assurance couvrant les dommages résultant d'une atteinte à un système de traitement automatisé de

données[4] à un dépôt de plainte auprès des autorités compétentes. La nouvelle rédaction inclut incontestablement les contrats d'assurance couvrant les conséquences des risques cyber et l'indemnisation des rançons mais cette indemnisation n'est plus visée expressément et l'on pourrait s'interroger sur le lien entre le dépôt de plainte et l'indemnisation des autres pertes et dommages causées par une atteinte à un système automatisé de données comme les pertes d'exploitation ou celles liées au coût de la restauration d'un système informatique.

L'interrogation se justifie également dans la mesure où l'indemnisation des rançons n'est pas systématiquement prévue dans tous les contrats d'assurance couvrant les conséquences des risques cyber. Le lien entre le dépôt de plainte et le contrat d'assurance qui ne contient pas une telle disposition interroge alors d'autant plus.

Le dépôt de plainte en cas d'attaque cyber se justifie pleinement pour l'information des forces de sécurité et de l'autorité judiciaire comme indiqué ci-dessus. Il faisait d'ailleurs partie des recommandations formulées par le Haut Comité Juridique de la Place Financière de Paris (HCJP) dans son rapport sur l'assurabilité des risques cyber du 28 janvier 2022[5]. Mais cette recommandation était formulée en lien avec l'assurance des rançons, l'information des forces de sécurité et des autorités judiciaires paraissant impérative en cas de demande et de paiement de rançons et d'indemnisation par l'assurance de ce paiement.

On peut penser que l'approche large désormais retenue par le législateur a notamment pour objectif de permettre aux autorités publiques de disposer de plus de données sur le nombre d'attaques cyber.

Cet objectif aurait alors pu être atteint d'une autre manière en rendant obligatoire de façon générale le dépôt de plainte dans le cadre de toute attaque cyber sans lien avec la mise en œuvre d'une police d'assurance. L'obligation aurait alors concerné toutes les victimes.

Il n'est pas certain que l'objectif d'encourager les dépôts de plainte soit ainsi atteint puisque l'obligation ne vise que certaines victimes qui bénéficient d'un contrat d'assurance et n'a pour conséquence que de permettre l'indemnisation au titre d'un tel contrat . Aucune autre sanction n'est prévue en cas d'absence de dépôt de plainte que la seule paralysie du contrat d'assurance.

On notera enfin que si le champ d'application de la nouvelle loi est très large, il ne concerne pas toutes les situations car les demandes de paiement des rançons ne résultent pas toujours d'une attaque par ransomware. Elles peuvent également être faites sous la menace d'une divulgation de données confidentielles ou de données préjudiciables à l'entreprise

La volonté de masquer le mot « rançon » a finalement bouleversé l'économie du texte d'origine en le privant de ses qualités intrinsèques.

Des points de vigilance pour les entreprises

Les entreprises devront désormais être particulièrement vigilantes car le champ d'application du nouveau texte est très large. Sont visées par le nouveau texte toutes les pertes et dommages causés par une atteinte à un système de traitement automatisé de données mentionnées aux articles 323-1 à 323-3-1 du code pénal, ce qui recouvre des situations extrêmement différentes n'incluant pas systématiquement une demande de rançon ou une perte ou une altération de données.

Sont ainsi concernées le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un système de traitement automatisé de données, le fait d'entraver ou de fausser le fonctionnement d'un tel système, d'y introduire frauduleusement des données ou d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient. Ceci peut concerner des situations très diverses, comme celle par exemple d'une cyber attaque entrainant le cryptage des données ou leur vol, accompagnée ou

1/ « Art. L. 12-10-1.-Le versement d'une somme en application de la clause d'un contrat d'assurance visant à indemniser un assuré des pertes et dommages causés par une atteinte à un système de traitement automatisé de données mentionnée aux articles 323-1 à 323-3-1 du code pénal est subordonné au dépôt d'une plainte de la victime auprès des autorités compétentes au plus tard soixante-douze heures après la connaissance de l'atteinte par la victime.

« Le présent article s'applique uniquement aux personnes morales et aux personnes physiques dans le cadre de leur activité professionnelle. »

2/ Projet de loi n°5185 d'orientation et de programmation du ministère de l'intérieur

3/ Art. L. 12 10 1. – Le versement d'une somme en application d'une clause assurantielle visant à couvrir le paiement d'une rançon par l'assuré dans le cadre d'une extorsion prévue à l'article 312-1 du code pénal, lorsqu'elle est commise au moyen d'une atteinte à un système de traitement automatisé de données prévue aux articles 323-1 à 323-3-1 du même code, est subordonné à la justification du dépôt d'une plainte de la victime auprès des autorités compétentes au plus tard 48 heures après le paiement de cette rançon. »

4/ Tel que visé par les articles 323-1 à 323-3-1 du Code pénal

5/ Voir pages 36 à 38

non d'une demande de rançon, mais également l'hypothèse de la reproduction ou du transfert (parfois à soi-même) sans autorisation, de données de l'entreprise par un salarié ou un tiers.

Toutes ces situations devront désormais entrainer le dépôt d'une plainte par la victime auprès des autorités compétentes dans le délai de 72h après la connaissance de l'atteinte par la victime sauf à perdre tout droit à indemnisation au titre de la police d'assurance souscrite.

Ce délai de 72h devra donc être un point d'attention particulièrement important pour les entreprises qui devront l'inclure dans leurs procédures internes de gestion de crises cyber de façon à ne pas l'oublier dans un contexte où le premier réflexe n'est peut-être pas de penser à l'assurance surtout si les pertes ou les dommages ne sont pas immédiatement apparents.

Le point de départ de ce délai de 72H sera inévitablement source de contentieux. Le texte initial envisageait un délai de 48h commençant à courir à partir de la date de paiement de la rançon, point de départ aisément vérifiable. A ce critère objectif le législateur a préféré s'appuyer sur la connaissance par la victime de l'atteinte à un système de traitement automatisé de données. La question de la détermination de la date se posera avec acuité en particulier pour les personnes morales et les grands groupes. Que devra-ton retenir ? La date où les services informatiques ont connaissance avec certitude de l'atteinte au système de traitement automatisé de données ou celle où la direction générale dispose de cette information ? Quelle date retenir pour l'incident informatique qui se révèle après enquête être ultérieurement une atteinte ?

Les entreprises seront donc bien avisées de documenter le déroulement des incidents informatiques et la prise de connaissance de l'atteinte au système et de sa date. C'est à partir de cette date que le délai commencera à courir que des pertes ou dommages aient été identifiés ou non.

La nécessité de documenter la prise de connaissance de l'atteinte par l'entreprise

s'impose en particulier à l'égard de la compagnie d'assurance qui se fera dans un premier temps juge du respect du délai de 72h. La fourniture d'éléments objectifs aisément vérifiables devrait ainsi limiter les risques de contentieux sur le point de départ du délai.

Il appartiendra aux entreprises de faire preuve également de dextérité pour articuler correctement dans le temps la saisine de leur compagnie d'assurance au titre de la police souscrite et le dépôt de plainte. La police d'assurance pourra peut-être faire l'objet d'une mise en œuvre pour des incidents informatiques qui se révèleront ultérieurement être des atteintes visées par les articles 323-1 et suivants du Code pénal. Le dépôt de plainte ne devra donc pas être oublié et s'inscrire dans le délai de 72H après la connaissance de l'atteinte par l'entreprise victime.

Cette disposition pourrait toutefois être considérée comme protectrice des entreprises car leur permettant de diligenter les enquêtes nécessaires pour s'assurer de la réalité de l'atteinte visée par les dispositions du code pénal précité. C'est à partir du moment où la connaissance de la victime est certaine que le délai commence à courir. Devraient ainsi être évités les multiples dépôts de plainte effectués par prudence mais pour des incidents qui se révèlent être mineurs et qui ne rentrent pas finalement dans les

hypothèses visées par les dispositions des articles 323-1 et suivants du code pénal. Mais la détermination du point de départ du délai fera sans aucun doute l'objet de nombreuses contestations et il apparait vraisemblable que certaines entreprises préfèreront déposer plainte dès qu'une suspicion d'une atteinte existe pour ne pas prendre le risque de perdre leur droit à indemnisation au titre de leur police d'assurance.

On rappellera pour mémoire qu'un autre délai de 72h devra être géré par l'entreprise dans le contexte d'une atteinte à l'un de ses systèmes de traitement automatisé de données C'est celui contenu dans l'article 33[6] du RGPD[7] qui impose la notification à l'autorité de contrôle compétente de la violation de données à caractère personnel dans un délai de 72H. Le point de départ de ce délai est la date à laquelle l'entreprise a connaissance de cette violation de données personnelles date qui ne correspondra pas toujours avec la date prévue au nouvel article L.12-10-1 du code des assurances qui est la date de prise de connaissance par l'entreprise d'une atteinte à un système de traitement automatisé de données.

L'assurabilité du cyber rançonnage

La loi n'a donc pas atteint l'objectif, souhaité par beaucoup et notamment par les compagnies d'assurance, de voir affirmer expressément la possibilité au plan juridique de couvrir par l'assurance le risque de cyber rançonnage des entreprises. Cependant les débats parlementaires attestent de la volonté du législateur de traiter cette question sans écarter l'assurabilité et il ne semble pas contestable que le « versement d'une somme en application de la clause d'un contrat d'assurance visant à indemniser un assuré des pertes et dommages causés par une atteinte à un système de traitement automatisé de données »[8] puisse inclure le remboursement des cyber-rançons qu'aucune disposition n'interdit par ailleurs.

La couverture de ce risque par les assurances apparait donc aujourd'hui possible en raison non seulement de la nouvelle loi mais également dans la mesure où elle ne contrevient pas à une règle de droit comme l'a démontré le rapport précité du HCJP.

On rappellera qu'au regard du droit pénal[9] et s'agissant de la situation de l'entreprise victime, le paiement de la rançon n'est pas en soi une infraction pénale car le paiement est effectué sous la contrainte. « Il s'analyse en une extorsion puisqu'elle vise à obtenir une remise de fonds sous la contrainte ce qui correspond au délit prévu par l'article 312-1 du Code Pénal. Il n'apparait donc pas possible de reprocher pénalement un paiement fait sous une contrainte constitutive d'une infraction pénale, la société payeuse étant la victime de cette infraction »[10].

Il convient également de rappeler l'article 122-7 du Code pénal qui exclut la responsabilité pénale de la personne qui, face à un danger actuel ou imminent qui menace elle-même, autrui ou un bien, accomplit un acte nécessaire à la sauvegarde de la personne ou du bien, sauf s'il y a disproportion entre les moyens employés et la gravité de la menace.

S'agissant de l'entreprise d'assurance, prévoir le remboursement d'une cyber-rançon au profit de l'entreprise victime d'un cyber chantage devrait être également considéré comme licite, le paiement de la rançon ne constituant pas une infraction. La couverture d'assurance n'a en effet ni un objet ni une cause illicite. Elle est comparable comme le précise le rapport du HCJP « à une assurance couvrant le risque de vol ou de destruction »[11].

Une limite à ce principe pourrait toutefois se trouver dans l'infraction de financement du terrorisme prévue par l'article 421-2-2 du Code pénal dans l'hypothèse où la cyber-rançon serait demandée par un groupe terroriste. L'infraction étant caractérisée par la connaissance que les fonds remis sont « destinés à être utilisés, en tout ou en partie, en vue de commettre (un acte de terrorisme) »[12] l'entreprise victime qui paye une cyber-rançon pourrait être poursuivie de ce chef si elle avait connaissance du fait que la demande de cyber-rançon émanait d'un groupe terroriste. Il convient de noter que la contrainte exonératoire de responsabilité pénale prévue à l'article

6/ En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

7/ RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

8/ Article 5 de la loi

9/ Rapport du HCJP pages 23 et suivantes

10/ Rapport du HCJP page 23

11/ Rapport du HCJP page 24

12/ Article 421-2-2 du Code pénal

122-2 du Code Pénal pourrait néanmoins trouver à s'appliquer dans certains cas[13] à condition que l'entreprise victime ait agi sous l'empire « d'une force ou d'une contrainte à laquelle elle n'a pu résister ».

La question se pose également pour l'assureur qui pourrait être considéré comme complice et accusé de financement indirect du terrorisme dans l'hypothèse notamment où il a connaissance, en amont du règlement de la rançon, que celle-ci va alimenter un réseau terroriste. La fongibilité entre le paiement de l'indemnité par l'assureur et le paiement de la rançon par l'entreprise[14] est alors susceptible d'exposer l'assureur dans ce cas à une accusation de complicité.

Cependant si l'information que la demande de rançon émane d'un groupe terroriste parvient à l'assureur après le paiement de la rançon, la qualification de financement du terrorisme au titre de l'article 421-2-2 du code pénal ne devrait pas pouvoir être retenue, le paiement de l'indemnisation effectué par l'assureur va demeurer entre les mains de l'assuré et intervient après le paiement de la rançon. Dans cette hypothèse il n'y a aucune fongibilité entre les deux paiements.

Il convient de rappeler également que le respect des régimes de sanctions prononcées par les autorités internationales, européennes et nationales et des mesures de gel des avoirs destinées notamment à lutter contre le terrorisme s'impose également aux assureurs.

Sous réserve du respect de ces règles destinées à lutter contre le terrorisme et son financement, l'assurance des rançons ne se heurte à aucune interdiction en droit français, le paiement de la rançon par l'assuré ne constituant pas en lui-même une activité illicite ou pénalement condamnable[15].

La contrariété à l'ordre public du code civil semble aussi exclue même s'il pouvait être tentant de considérer, par un raccourci, que les assureurs en remboursant les rançons aux victimes contreviennent à l'ordre public ou aux bonnes mœurs car ces remboursements encourageraient indirectement les cybercriminels à poursuivre leurs attaques et donc à commettre de nouvelles infractions.

Enfin on mentionnera qu'au regard du droit des assurances le principe que l'assureur ne répond pas des pertes et dommages provenant d'une faute intentionnelle ou dolosive de l'assuré[16] n'a pas vocation à s'appliquer dans le cas de l'indemnisation d'une rançon, l'assuré est dans ce cas une victime et les pertes et dommages qu'il subit ne relève ni d'une faute intentionnelle ou dolosive de sa part.

L'occasion de confirmer expressément la licéité de l'assurance des rançons a donc été manquée et d'aucuns le regretteront car comme le rapport du HCJP le précisait[17] « ce n'est pas l'existence des garanties « remboursement des rançons » qui est à l'origine de l'existence des attaques par « ransomware » ou autres demandes de cyber-rançons. »

D'autres opportunités de clarification se présenteront peut-être dans l'avenir car toutes les recommandations du HCJP figurant dans le rapport sur l'assurabilité des risques cyber n'ont pas été mises en œuvre à ce jour. Parmi celles-ci figurait une demande de clarification des textes nationaux et européens applicables aux obligations LCB-FT des assureurs en matière de remboursement de cyber rançon afin de fixer le cadre dans lequel les assureurs pourraient s'inscrire pour s'assurer que les mesures qu'ils prennent sont suffisantes au regard de la loi. On pourrait également citer la demande de clarification de l'article L121-8 du Code des assurances pour voir intégrer dans le concept de guerre les attaques cyber perpétrées par les États[18]. ■

13/ Article 122-2 du Code pénal.

14/ Rapport du HCJP page 24

15/ « l'assurance d'un risque pénal est illicite en tant que telle et celle des autres risques est illicite à deux conditions alternatives : qu'un texte spécial le prévoie ou que la garantie ait directement pour objet une activité elle-même illicite » L. Mayaux « Assurance et ordre public : à la recherche d'un critère » RGDA 2008, N°3 cité dans le rapport précité du HCJP page 21.

16/ Article L113-1 du Code des assurances

17/ Rapport du HCJP page 32

18/ Rapport du HCJP pages 48 et suivantes.

Face à la cybermenace, ensemble nous sommes plus forts !

Inauguré il y a un peu plus d'un an, le Campus Cyber est la vitrine de l'excellence française en matière de cybersécurité. Son président, Michel Van Den Berghe nous présente ce lieu totem de la cybersécurité, son périmètre d'action et ses priorités pour 2023.

Michel VAN DEN BERGHE,

Président du Campus Cyber

Qu'est-ce que le Campus Cyber ?

Le Campus Cyber est né de la volonté du Président de la République, Emmanuel Macron, de doter la France d'un lieu totem de la cybersécurité pour, d'une part, fédérer l'ensemble des acteurs de cet écosystème, et, d'autre part, faire rayonner l'expertise et l'excellence françaises dans ce domaine.

Pour ce faire, l'action du Campus Cyber s'articule autour de quatre grands piliers :

- Une approche opérationnelle de la cybersécurité qui s'appuie sur le partage des données pour renforcer la capacité de chacun à maîtrise le risque numérique ; le rassemblement d'experts de l'analyse cyber afin de renforcer les capacités de veille, de détection et de réponse à la menace… ;

- Le développement de la formation et de l'attractivité des métiers de la cybersécurité : aujourd'hui, nous avons un fort enjeu de visibilité afin de casser les stéréotypes et idées reçues sur ce secteur, de susciter des vocations et d'attirer plus de femmes et de jeunes. En parallèle, nous participons à la formation initiale et continue ainsi qu'à la montée en compétences des différents publics (agents de l'État, salariés, étudiant, personnels en reconversion…) au travers du déploiement de programmes communs d'entraînement et de formation, le partage de ressources… D'ailleurs, une quinzaine d'écoles a adhéré au Campus Cyber et cinq y dispensent des cours ;

- L'accélération de l'innovation et de la recherche en matière de cybersécurité pour faciliter le transfert technologique vers les industriels et les entreprises. Pour ce faire, nous travaillons notamment avec l'INRIA, le CEA, l'IMT et le CNRS afin que les chercheurs inventent, développent et créent les solutions et les technologies qui nous permettront de contrer les cybermenaces. À partir de là, il s'agit aussi de les transférer vers la sphère privée mais aussi de faciliter la création de start-up innovantes voire des licornes ;

- L'animation de cet écosystème : le Campus Cyber a été pensé pour être un lieu vivant et ouvert. Il propose ainsi une programmation très riche avec des événements innovants propices aux échanges, aux partages de bonnes pratiques, à la veille technologique et à la découverte des évolutions de la société

numérique de confiance (conférences, webinaires, podcasts, tables rondes, pitchs, job dating, création des communs de la cyber, expérimentations, learning expeditions, événements internationaux, speed dating investisseurs…).

Aujourd'hui, pourquoi est-ce essentiel de disposer d'un acteur comme le Campus Cyber en France et en Europe ?

Le Campus Cyber a été inauguré le 15 février 2022. C'est une société privée avec une participation publique à hauteur de 39 %. Elle a un capital de près de 9 millions d'euros et 167 actionnaires, qui sont essentiellement des grandes entreprises, des écoles, des associations… Ce lieu totem s'étend sur plus de 26 000 m², dont 17 000 m² d'espaces de travail partagés ou privés, 6 000 m² de plateau projets et innovation, et 3 000 m² dédiés à la formation. Il accueille plus de 1 800 experts et 134 sociétés y sont implantées.

Face à la professionnalisation des pirates et cyberattaquants, mais aussi la sophistication et la recrudescence des cyberattaques, qui sont de plus en plus organisées et structurées, il était essentiel et stratégique de pouvoir se doter d'une structure comme le Campus Cyber afin de pouvoir inverser ce rapport de force. Nous sommes, en effet, convaincus qu'ensemble nous sommes plus forts pour lutter contre cette menace. L'idée est de réfléchir et de travailler ensemble pour créer et développer les solutions qui permettront aux grands groupes, PME, TPE, administrations et organisations gouvernementales de contrer ces menaces.

Au-delà, le Campus Cyber est aussi une vitrine de l'excellence française en matière de lutte contre la cybercriminalité et de cybersécurité. Nous avons reçu plus de 50 visites de délégation internationales dans nos locaux depuis l'ouverture. Enfin, c'est aussi un lieu que nous avons aussi voulu attractif afin de susciter des vocations et de contribuer à promouvoir une certaine diversité et mixité dans cette filière. En effet, contrairement aux idées reçues, dans le monde de la cybersécurité, on ne retrouve pas seulement des ingénieurs ou des hackers éthiques. On retrouve également les métiers de la communication, de la formation et relatifs aux relations géopolitiques.

Un peu plus d'un an après l'ouverture du Campus Cyber, quel bilan tirez-vous ?

Il est extrêmement positif ! Quand le Président de la République m'a confié cette mission, de nombreuses personnes de mon entourage étaient sceptiques sur le fait d'arriver à réunir et à faire travailler ensemble et au sein d'un même endroit des entreprises et des centres de recherche dans un contexte marqué par une véritable guerre des talents. Nous avons relevé haut la main ce défi ! Tous les postes de travail sont actuellement occupés. Plus de 500 participants issus d'entreprises différentes collaborent et échangent au sein d'une douzaine de groupes de travail pour produire des livrables concrets sur les enjeux de la cybersécurité à destination de tout l'écosystème. Nous avons ainsi publié le rapport « Horizon Cyber 2030 Perspectives et Défis » sur l'anticipation du risque et de la menace cyber. Aux

côtés de l'ANSSI, nous avons contribué à l'organisation de REMPAR22, un exercice de mise en situation et de gestion de crise auquel plus de 120 sociétés ont pris part. Pour accélérer l'innovation et le transfert des solutions et des technologies vers le monde des entreprises et de l'industrie, avec le Secrétariat Général pour l'Innovation, nous collaborons avec deux entités : Cyber Booster, qui aide les jeunes porteurs d'idée à structurer leur projet, et un incubateur, pour accompagner les projets les plus prometteurs et les mettre en relation avec des investisseurs.

Aujourd'hui, la réussite du Campus Cyber est jalousée dans le monde entier. En effet, s'il existe des structures équivalentes dans différents pays, notre principal vecteur de différenciation est qu'aux côtés des écoles et des centres de recherche, nous avons des entreprises qui, de manière volontaire, se sont installées au sein de ce lieu totem : TotalEnergies, Asltom, Bouygues, SNCF, Siemens, BNP Paribas, la Société Générale, la Banque Postale, PwC, Deloitte…

Quelles sont vos priorités pour 2023 ?

Nous en avons identifié deux. La première concerne les talents. Pour pallier le manque d'attractivité de notre filière, nous collaborons, par exemple, avec les Ministères de l'Éducation Nationale dans le cadre de la réforme des collèges et des lycées pour lancer une grande campagne de promotion des métiers de la cybersécurité. Nous souhaitons aussi former plus de 1000 professeurs et éducateurs aux métiers ou aux enjeux de la filière cybersécurité. Ces derniers sont en contact direct avec les lycées et peuvent les informer et leur présenter nos métiers qui sont passionnants, à la pointe de l'innovation technologique, mais qui ont aussi une véritable dimension sociale. En parallèle, nous travaillons sur la création d'une série télévisée qui s'inspire du succès de la série « Le Bureau des Légendes » et qui avait, par ailleurs, contribué à augmenter l'attractivité et la visibilité de la DGSE. Nous prévoyons aussi de prendre part à des événements qui attirent les jeunes et leurs parents, comme le Festival du Jeu Vidéo et du Numérique des Hauts-De-Seine.

La seconde priorité est plus opérationnelle et concerne la sécurisation de nos PME face à la menace cyber. Si le nombre de cyberattaques est en constante hausse, le nombre d'attaques réussies contre des grandes entreprises françaises a diminué. Selon les chiffres de l'ANSSI, 1 082 incidents ont été répertoriés en 2021 contre 831 en 2022. Cela montre que ces grands groupes et entreprises mettent en place les moyens et solutions pour se protéger et se défendre et surtout qu'ils y arrivent. Toutefois, cela n'est pas le cas des PME et des TPE qui sont démunies face à la cybermenace. On estime, d'ailleurs, qu'une entreprise sur deux victimes d'un ransomware qui refuse de payer dépose le bilan dans les 18 mois qui suivent l'incident. Pour les accompagner, nous allons notamment mettre en place un plan de recommandations afin de les aider à sécuriser leurs systèmes et à développer leur résilience pour être en capacité de poursuivre leur activité même après une attaque. En parallèle, nous développons avec BpiFrance une offre dédiée, le Bouclier Cyber, destinée aux entreprises accompagnées par cet organisme. ■

Cyberattaques : la recette AFNOR pour prévenir et guérir

Pas une semaine sans qu'une entreprise ou une institution ne soit victime d'une cyberattaque. Le guide AFNOR Spec 2208 détaille la conduite à tenir pour assurer une continuité d'activité et reconstruire le système d'information. Il est gratuit !

Julie LATAWIEC,

Responsable Développement et Innovation Secteur des Technologies Numériques, AFNOR

Les chiffres sont effrayants : d'après le baromètre CESIN 2022[1], plus d'une entreprise française sur deux a vécu au moins une cyberattaque au cours de l'année 2021. Et chacune de ces attaques occasionne un manque-à-gagner de 27 % sur le chiffre d'affaires ! Aucun acteur économique, grand ou petit, public ou privé, n'est à l'abri, ni ne doit fermer les yeux sur ce qu'il faut mettre en place pour prévenir les attaques. A l'heure où nous écrivons cet article, l'hôpital de Versailles est durement touché !

Pour savoir comment s'organiser, AFNOR publie le guide « Cyber-résilience, reconstruction du SI et continuité d'activité métiers en cas de cyberattaque paralysante ». Disponible gratuitement chez AFNOR Editions sous le libellé AFNOR Spec 2208[2], il centralise les recommandations et bonnes pratiques d'une quarantaine d'acteurs dont beaucoup ont vécu des cyberattaques : PME, ETI, start-up, grands groupe, hôpitaux, etc. AFNOR en a elle-même subi une, qui l'a privée de son système d'information pendant plusieurs semaines au printemps 2021. « *Les organisations représentées autour de la table avaient besoin d'un condensé de bonnes pratiques pour savoir comment s'organiser avant et pendant : évaluer le risque, les critères à sélectionner pour prendre des décisions, que prioriser pour maintenir une continuité de service* », apprécie Julie Latawiec, qui a supervisé les travaux chez AFNOR. L'Association française de normalisation est ici dans sa mission de conception de réponses standardisées, sur la base d'un partage de bonnes pratiques, à un questionnement commun à plusieurs acteurs économiques. Le guide n'est pas une norme stricto sensu, mais il constitue un outil complémentaire aux normes volontaires existant sur le sujet, comme l'ISO/IEC 27001, qui vient d'ailleurs de sortir dans une nouvelle version[3].

Continuer l'activité et reconstruire le système d'information

Aux responsables des systèmes d'information en entreprise, le guide donne des lignes directrices et des recommandations opérationnelles pour anticiper le traitement d'une cyberattaque, ou y faire face en fonction de la nature de l'activité, de la maturité (3 niveaux sont définis) et des moyens de l'organisme. « *Les cyberattaques peuvent mettre des organisations au tapis pendant des durées longues : plusieurs semaines, plusieurs mois. Nous sommes donc partis*

sur le concept de cyberattaque paralysante. Cela pose certes la question de comment reconstruire le système d'information, après coup, mais surtout celle d'assurer une continuité d'activité, sur un temps long, en l'absence d'outils informatiques ou en présence d'outils fonctionnant en mode dégradé, décrit Xavier Hartout, consultant chez Adenium BRG, qui a coanimé le groupe de rédacteurs du guide AFNOR.

Le guide est assorti de plusieurs annexes : synthèse des bonnes pratiques, fiche souscription cyber-assurance, guide synthétique pour les petites structures, fiche de déclenchement d'un plan de continuité informatique. ■

1/ https://www.cesin.fr/actu-7eme-edition-du-barometre-annuel-du-cesin-enquete-exclusive-sur-la-cybersecurite-des-entreprises-francaises.html

2/ https://www.boutique.afnor.org/fr-fr/norme/afnor-spec-2208/cyberresilience-reconstruction-du-si-et-continuite-dactivite-metiers-en-cas/fa204225/338577

3/ https://www.boutique.afnor.org/fr-fr/norme/nf-en-iso-iec-27001/technologies-de-linformation-techniques-de-securite-systemes-de-management-/fa187277/59084

Intelligence Artificielle et Cybersécurité : solution ou menace ?

Besma ZEDDINI,

Enseignante-chercheur en intelligence artificielle et cybersécurité, CY Tech, CY Cergy Paris Université,
Responsable de la filière Cybersécurité et du Mastère Spécialisé® Cybersécurité & Smart Systems,
Chargée de mission à l'innovation et transfert des sciences expérimentales

L'intelligence artificielle vise à construire des programmes informatiques qui s'adonnent à des tâches demandant des processus mentaux de haut niveau tels que l'apprentissage perceptuel, l'organisation de la mémoire et le raisonnement critique [Minsky, 1956]. En d'autres termes, il s'agit de l'ensemble des moyens théoriques et techniques pour faire simuler à des machines des comportements généralement associés à l'intelligence humaine. De nos jours, les travaux sur l'intelligence artificielle visent plutôt à résoudre des problèmes d'une manière plus satisfaisante que l'intelligence humaine. Les travaux et applications se concentrent sur l'intelligence artificielle faible[1], focalisée sur une tâche précise (la recommandation de contenus, la reconnaissance d'images pour l'authentification ou la détection de pathologies, la traduction automatique, etc.).

Divers domaines de recherche s'inscrivent dans la démarche générale de création d'une intelligence artificielle, tels que la représentation de connaissances, le traitement automatique des langues, la robotique, la planification, la modélisation cognitive, etc. Ces domaines de recherche sont actifs depuis des décennies, mais le regain réel d'intérêt pour l'intelligence artificielle, tant académique qu'industriel, a eu lieu au début des années 2010 avec le développement vertigineux du Big data, des sciences de données en général et de l'apprentissage automatique en particulier (supervisé ou non supervisé) et surtout de l'apprentissage profond.

Les deux faces de l'Intelligence artificielle

En décembre 2018, le cabinet d'études McKinsey a recensé les usages réels de l'intelligence artificielle, et plus particulièrement l'apprentissage profond, pour le bien social [McKinsey, 2018]. Diverses actions, telles que la fondation et la plateforme ONU « AI for good » ou le projet « AI for Social Good » de Google[2] mettent en avant les projets en intelligence artificielle au service du bien commun et du progrès de tous les humains. Les avancées en IA sont d'ailleurs généralement accueillies avec enthousiasme, et les usages duaux des nouvelles technologies, leur usage détourné ou leur sensibilité aux attaques sont généralement passés sous silence.

Pourtant, l'intelligence artificielle peut avoir des applications néfastes voire criminelles, en utilisant les mêmes théories, les mêmes technologies et les mêmes avancées. Le système de lecture labiale de Google et Oxford [Chung *et al.*, 2017], permettant de lire sur les lèvres d'une manière souvent plus pertinente que des professionnels humains, peut aider les personnes ayant un trouble de la parole, sourde ou malentendante ; mais il permet également de développer un système de surveillance ou d'« écoute » plus performant par des entités malintentionnées. Un système

de génération automatique de vidéos [Greenmier, 2018] peut optimiser la production cinématographique et documentaire, mais il peut également participer à la diffusion massive de fake news et à la désinformation. Un drone autonome peut prendre des vidéos d'endroits inaccessibles, mais il peut également faciliter le lancement de projectiles sur ces mêmes cibles inaccessibles. Il est donc d'une grande importance de protéger l'intelligence artificielle contre les usages frauduleux et de dispenser des efforts comparables sur la cyber-protection de l'IA que sur l'IA elle-même.

Intelligence artificielle comme cible privilégiée des cyberattaques

Plusieurs failles de sécurité dans les intelligences artificielles commerciales sont régulièrement mises en évidences (e.g. [Zhang *et al.*, 2018]). Le chemin semble balisé pour des attaques de plus grande gravité, comme le déverrouillage d'accès et le transfert d'argent. Suivant des techniques similaires, des cybercriminels peuvent cibler l'intelligence artificielle commandant l'authentification d'une institution financière ou une entreprise peu scrupuleuse peut cibler l'IA définissant la stratégie de détermination du prix de son concurrent. En décembre 2017, la société de sécurité Webroot a effectué une enquête concluant que plus de 90% des professionnels de la cybersécurité aux Etats-Unis et au Japon s'attendent à ce que les attaques utilisent l'intelligence artificielle contre les entreprises pour lesquelles elle est supposée travailler [Webroot, 2017].

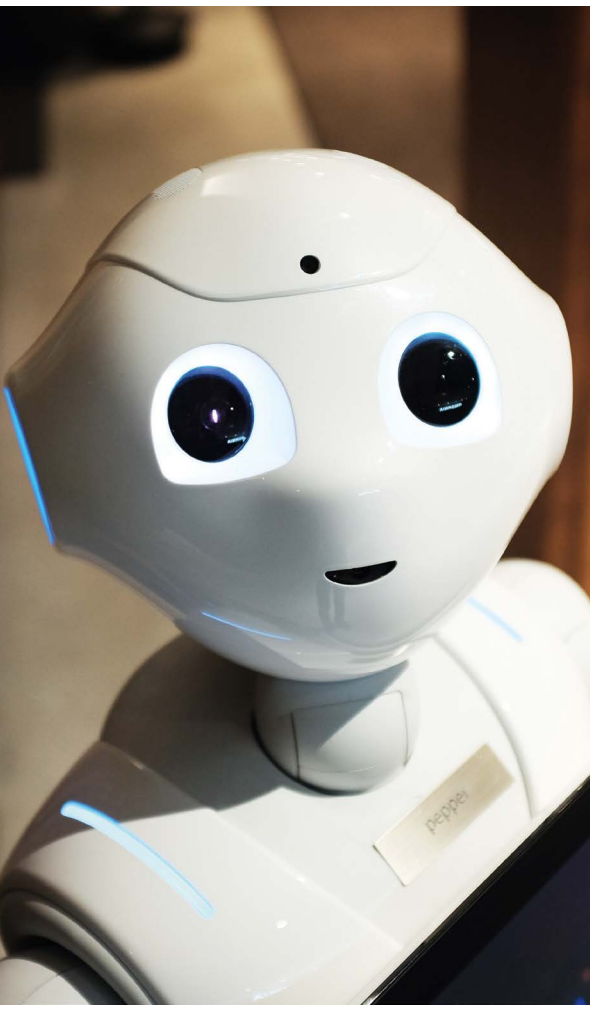
Ces menaces pèsent sur toutes les étapes de mise en place d'une intelligence artificielle. La méthodologie de l'apprentissage automatique est en effet fondée sur trois étapes : l'acquisition de données (e.g. images, vidéos, voix, transactions, etc.), l'apprentissage sur cette base de données (e.g. raisonnement par analogie, apprentissage de compétences comme la conduite, ou la prévision d'états futurs, etc.) et enfin l'action fondée sur de nouvelles données (génération d'images, de textes ou de vidéos, la conduite ou la navigation, etc.). Le système résultat est amélioré et corrigé par un processus itératif durant l'exécution. Chacune de ces étapes présente un risque de compromission.

1. Lors de l'étape d'acquisition des données d'apprentissage, ces données peuvent être corrompues ou manipulées.

2. Lors de l'étape d'apprentissage elle-même, les algorithmes d'apprentissage peuvent être détournés ou corrompus.

1/ Par opposition à l'intelligence artificielle forte, capable de construire des programmes ayant conscience d'eux-mêmes

2/ https://ai.google/social-good



3. Lors de l'étape de mise en place du système, la configuration des composants du système peut être changée et détournée de l'objectif principal.

Cette méthodologie à trois-étapes présente également deux principaux risques en termes de sécurité. Le premier est que les systèmes sont généralement conçus pour s'exécuter en boucle fermée, sans intervention humaine, dans leur travail quotidien. Les attaques vers ces systèmes peuvent ainsi rester longtemps sans être détectées. Le second risque est relatif à la grande masse de données manipulée par les algorithmes d'IA qui font que les raisons guidant une telle décision sont souvent difficilement interprétables. Cela signifie que, quand bien même une attaque serait détectée, ces motivations peuvent demeurer opaques.

Intelligence artificielle comme solution aux cyberattaques

La méthodologie, la technologie et les outils d'intelligence artificielle peuvent également être mis à contribution pour protéger les systèmes des cyberattaques. Une analyse des cyberattaques passées peut permettre de différencier les situations réellement dangereuses de celles qui le sont bien moins (une faute de frappe sur un mot de passe comparée à un usage frauduleux de carte bancaire, par exemple). Plus généralement, l'IA peut aider à renforcer la sécurité des systèmes fondés sur l'IA durant les trois principales étapes de cybersécurité : la prévention, la détection et la réponse aux attaques.

1. **La prévention** : l'apprentissage automatique peut servir à apprendre des attaques précédentes et de pouvoir mettre en place les systèmes pertinents pour chaque menace de sécurité identifiée. Ce système de prévision pourra rapidement s'adapter aux menaces précédemment inconnues.

2. La détection : les méthodes de détection fondée sur la signature des attaques (des règles statiques identifiant les attaques) sont bouleversées avec l'IA. Les algorithmes fondés sur l'IA peuvent maintenant détecter tout changement comparé à une situation définie comme normale du système. Cela offre davantage de potentiel de détection des menaces inconnues jusqu'alors. Par ailleurs, l'apprentissage par renforcement et l'apprentissage profond permettent maintenant de se dispenser des grandes bases de données d'entrainement, et peuvent être bien plus rapidement opérationnels dans ce contexte de détection d'attaques.

3. **La réponse** : l'IA peut participer grandement aux cyberattaques en priorisant le travail des analystes et en l'orientant vers les activités à haute valeur ajoutée. Elle peut également permettre la mise en quarantaine automatique de parties du système ou de ses utilisateurs pendant une attaque.

En guise de conclusion et perspectives, Les questions principales qui se posent : Faut-il se fier à l'IA ? Quid de l'explicabilité et de l'éthique de l'IA ? ■

Références

[Minsky, 1956] M. Minsky, "Heuristic Aspects of the Artificial Intelligence Problem", Lincoln Laboratory, M.I.T., Lexington, Mass. Group Report No. 34–55, 1956

[McKinsey, 2018], McKinsey, "Notes from the AI frontier, applying AI for social good", discussion paper, december 2018, 48 pages, 2018

[Chung et al. 2017] J. S. Chung, A. Senior, O. Vinyals and A. Zisserman, "Lip Reading Sentences in the Wild", IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Honolulu, HI, 2017, pp. 3444-3453, 2017

[Greenmeier, 2018] L. Greenemeier, "Don't Believe Your Eyes", Scientific American 318(4):12-14, 2018

[Webroot, 2017] Webroot, "Game Changers: AI and Machine Learning in Cybersecurity," 9 pages, 2017

[Zhang et al., 2018] R. Zhang, X. Chen, J. Lu, S. Wen, S. Nepal, Y. Xiang, "Using AI to Hack IA: A *New Stealthy Spyware Against Voice Assistance Functions in Smart Phones*", CoRR abs/1805.06187, 11 pages, 2018

Conseil National de la Refondation

Pour une nouvelle approche de la politique industrielle

Forums Mac Mahon. 21 mars 2023

JACQUES-ANDRÉ TROESCH,

Conseiller maître honoraire, Régulateur du marché français et européen de l'énergie (2000-2008).

Les Forums Mac Mahon ont inscrit à leur agenda la politique industrielle dans le cadre de leurs travaux sur la Refondation.

Plutôt que réindustrialisation, qui évoque un retour au passé, les Forums Mac Mahon ont préféré parler de nouvelle approche de la politique industrielle. Ces travaux n'ont pas pour ambition d'être exhaustifs, mais plutôt de partager quelques convictions. Parmi celles qui ont été exprimées, mentionnons cinq d'entre elles :

1- **Les problèmes auxquels la France doit faire face (croissance, indépendance, transition énergétique, emploi et niveau de vie, déficits budgétaires et sociaux, déficits extérieurs...) ne se résoudront pas sans que la priorité soit reconnue et accordée à l'industrie.** Elle est en particulier un facteur clé des gains de productivité.
Une politique de développement industriel ne se résume pas à un simple appui aux entreprises. Elle est tributaire de l'ensemble de la politique gouvernementale.

2- **Un point de départ : le changement des structures gouvernementales.** Afficher la priorité conférée à l'industrie commence par créer un ministère emblématique, avec comme en Allemagne une direction de l'industrie et une direction de l'énergie, des télécom et du numérique. Lui serait attribué le monopole des règlementations concernant l'industrie, qu'il s'agisse des règles techniques, environnementales ou sociales, afin de simplifier et réduire le nombre des multiples règlementations applicables. Cela permettrait aussi l'allègement des structures administratives qui en ont la charge.
La recherche, quant à elle ne devrait plus être liée à l'université, trop théorique, trop éloignée de l'industrie et qui n'en a plus depuis longtemps le monopole. Elle pourrait être dévolue à une agence type DARPA qui couvrirait le militaire et le civil.

3- **Une priorité de la formation et de l'emploi : les emplois industriels.**
Ces emplois sont la base de la réussite d'une nouvelle industrialisation. Leur incidence est fondamentale pour améliorer la productivité générale de l'économie et contribuer à la croissance. La France a besoin de 60 000 ingénieurs par an alors qu'elle n'en forme que 40 000. Aussi, les écoles d'ingénieurs et les écoles ou instituts techniques doivent être prioritaires dans les crédits publics et

la taxe d'apprentissage, en contrepartie d'un engagement d'augmenter leurs effectifs, à commencer par les Ecoles les plus emblématiques dont les effectifs pourraient augmenter de 50%.
Plus largement, une transformation profonde de la mentalité des établissements d'enseignement supérieur, en particulier des universités, est indis pensable. L'enseignement supérieur doit mettre ses chercheurs et ses doctorants au service des entreprises en échange de la rémunération des services rendus, à l'image par exemple du pôle qui s'est constitué autour du campus de Cambridge (25 000 étudiants répartis dans 31 collèges) avec 5 000 entreprises employant 70 000 personnes et un chiffre d'affaires de 22,4 milliards d'euros. Reste néanmoins à trouver les leviers d'une telle mutation.
Au niveau scolaire, un levier important est celui des aides et des bourses, à rendre supérieures pour les élèves de l'enseignement technique et scientifique à celles offertes pour d'autres formations.
Plus généralement et en amont, les enseignements au collège et au lycée devraient consacrer un nombre d'heures suffisant à la découverte des sciences et des techniques.
En aval, le compte formation devrait être recentré sur les formations directement utiles à notre économie, avec un ciblage spécifique sur l'industrie accompagné de bonifications ciblées.
Plus largement encore, c'est une évolution culturelle en faveur des sciences et de la technique qui sera nécessaire. Pour redonner tout leur lustre à la science, à l'industrie et à la technique, et sensibiliser la jeunesse et la population, de nombreuses actions peuvent être proposées : prix scientifiques, olympiades de maths et de physique, rencontres et dialogues entre scientifiques et ingénieurs avec les élèves, émissions de télévision…

4- **Une priorité budgétaire nouvelle : le développement industriel et la recherche.**
Une telle approche passe par la fin de la politique de saupoudrage. Nos moyens n'étant pas illimités, les crédits et les avantages fiscaux pour la création d'entreprises et la recherche développement doivent faire l'objet d'une concentration sur les secteurs industriels les plus prometteurs,

qu'il s'agisse d'industries d'avenir ou traditionnelles, en sacrifiant les politiques jugées moins prioritaires.
Face aux efforts des GAFA, des USA, de la Chine et de l'Allemagne, il est indispensable de prévoir au minimum 100 milliards€ de crédits, bien au-delà des 34 milliards€ sur 5 ans du plan France 2030, et d'atteindre un objectif de 3% du PIB consacré à la recherche.
Pour ce qui concerne les secteurs d'intervention :

a. **La robotisation de l'industrie française et le numérique, qui ne figurent pas au plan 2030, devraient être des priorités majeures de la politique industrielle française,** eu égard notamment au vieillissement de la société et à la pénurie de main d'œuvre que l'on constate dès à présent.

b. **Il faut ensuite tenir compte des nouvelles réalités politiques qui impliquent un effort majeur dans le domaine de la défense,** non mentionné dans le plan 2030. L'objectif pour 2030 devrait être d'atteindre 3% du PIB si nous voulons être crédibles.

c. **Il faudra accorder la priorité des priorités à l'industrie énergétique** qui figure dans le plan de façon mineure. Les Forums Mac Mahon y consacrent des travaux spécifiques.

d. **Autre priorité pour l'avenir de l'industrie française non évoquée dans le Plan France 2030 : la disposition des matières premières.** La France comme de nombreux pays européens dispose de certains des gisements de minerais du futur, à savoir lithium, tungstène, uranium, antimoine, qu'elle devrait envisager de mettre en exploitation.

5- **Une remise en cause des postulats économiques de l'union européenne est nécessaire.**
Il convient de noter qu'aux USA les États sont libres d'aider leurs entreprises sans aucune intervention du gouvernement fédéral. La question mériterait même d'être posée de l'indépendance de la Dgcomp et de son rattachement au commissaire chargé de l'industrie.
L'ère de la mondialisation heureuse est terminée. Les relations commerciales sont dominées par la loi du plus fort : les USA, la Chine et même la Russie en montrent l'exemple. Le temps de la naïveté européenne est révolu. La politique commerciale doit non seulement servir à protéger notre économie mais à assurer sa sécurité. La politique agricole comme la politique industrielle ou énergétique doivent permettre à l'Europe d'asseoir sa place mondiale en cherchant son indépendance et son influence sur le reste du monde.
Dans cette perspective l'agriculture doit redevenir un secteur d'exportation. Les industries d'équipements agricoles et agroalimentaires ont la même importance stratégique que le nucléaire ou la biologie. Plus largement, un Buy European Act est indispensable. Un tel changement de paradigmes ne manquera pas de heurter nombre de nos partenaires. Mais l'enjeu pour la survie de notre économie est tel qu'il ne faudra pas hésiter à les menacer de faire cavalier seul ou avec d'autres, voire de se mettre temporairement en marge de l'Europe. ■

Retour sur la conférence du 13 février 2023

Les défis énergétiques de demain et leur financement seront au cœur du thème du prochain magazine des professions financières.

En anticipation de ce prochain magazine, la conférence du 13 février a permis de débattre notamment de la part des énergies renouvelables dans la transition énergétique, et du rôle de l'énergie nucléaire.

Marie Agnès Nicolet,

Présidente de Regulation Partners et du club des marchés financiers

Vous retrouverez ci-après la synthèse de l'intervention de Jérôme GUILLET, Managing Director, SNOW

« La France a pu ignorer la transition énergétique pendant longtemps car elle bénéficiait du programme nucléaire, qui lui a offert une électricité bon marché et quasiment totalement décarbonée pendant plusieurs décennies. Mais aujourd'hui, alors que le parc nucléaire se fait vieillissant et que le débat porter presque exclusivement sur la construction renouvelles centrales nucléaires, il importe de ne pas ignorer les leçons de la transition vers les énergies renouvelables chez nos voisins, car cette transition est souvent mal comprise, en particulier celle entreprise par l'Allemagne.

L'arrêt des centrales nucléaires - facilement contestable alors que les centrales à lignite continuent de produire - sert d'épouvantail et permet d'ignorer que la part des énergies fossiles dans la production d'électricité est passée de 80% à moins de 50% en 20 ans, avec une tendance qui s'accélère. La réalité est que les énergies renouvelables, qui étaient plus chères il y 10-15 ans, sont aujourd'hui les sources de MWh les moins chères, et que les réseaux s'adaptent pour les intégrer. Leur part dans le système va aller croissant, c'est inévitable, et cette tendance est assez peu compatible avec le maintien de capacités de base comme le nucléaire. Ce qui est remarquable en Allemagne, c'est que les capacités flexibles (centrales au gaz et à la houille) sont moins sollicitées en production nette aujourd'hui, avec 40% d'éolien et de solaire dans le mix, qu'elles ne l'étaient il y a 20 ans quand ces 40% étaient produits par les centrales de base (nucléaire et lignite) - le sujet du stockage d'électricité et du backup éventuel par des centrales à combustible est un problème surestimé.

Aujourd'hui, dans le contexte de l'arrêt des livraisons de gaz russe après l'invasion de l'Ukraine, on peut reprocher à l'Allemagne d'avoir manqué de réflexion stratégique en ne diversifiant pas assez ses fournisseurs (une erreur que la France n'a pas faite), mais pas d'avoir engagé la démarche, et déjà fait près de la moitié du chemin, pour remplacer une système électrique carbone-intensif par des énergies renouvelables. La France va devoir aujourd'hui s'engager plus résolument dans la même voie, sans encore y croire. » ■

Le prochain numéro

du Magazine des Professions Financières et de l'Économie

sera dédié à la

Transition énergétique et préservation du climat : quels financements ?

Prochaine parution en novembre 2023

Centre des Professions Financières

#Mag27