INTERVIEW. « *Il est nécessaire de mettre en place une véritable politique de gouvernance du risque cyber pour les entreprises* »

Tandis que 20 % des entreprises françaises ont déjà été victimes d'une cyberattaque, selon un récent baromètre Cyblex/Docaposte, Pierre-Marie Gauthier, secrétaire général de l'association Eurolaw France Cyber, plaide pour une sensibilisation accrue des dirigeants, qui peuvent être tenus juridiquement responsables en cas d'attaque.

JSS : Quels sont les différents visages du risque cyber ?

Pierre-Marie Gauthier : Sur le plan mondial, le risque cyber peut être distingué de trois façons. Premièrement, il y a les erreurs humaines au sein des entreprises, qui peuvent entraîner la perte ou la destruction de données, ou encore le dysfonctionnement des systèmes informatiques, rendant ces derniers indisponibles. Bien que ce type de risque soit relativement rare, il

reste pertinent. Prenons l'exemple récent de CrowdStrike, que vous avez peut-être suivi. Dans ce cas précis, il s'agit d'une erreur humaine, et non d'une cyberattaque. Une mise à jour de leur logiciel intégré à Windows n'avait pas été suffisamment testée, ce qui a conduit à des dysfonctionnements majeurs pour les utilisateurs. Certains se sont retrouvés avec un écran bleu, et pour corriger ce problème, il a fallu intervenir poste par poste, ce qui est évidemment gérable pour une petite entreprise, mais devient un véritable casse-tête pour des organisations comptant des milliers de postes.

Le deuxième type de risque est la malveillance, que je diviserais en deux catégories. La première, la malveillance politique, concerne des États suspects tels que la Chine, la Russie ou la Corée du Nord, qui utilisent leurs services secrets pour mandater des entreprises tierces afin de mener des attaques ou des actions de malveillance. Ces attaques peuvent prendre la forme de blocages, de désinformation, ou d'autres types d'agressions numériques visant à déstabiliser un adversaire.

Ensuite, il y a la malveillance financière, dont l'objectif est de voler des données, de bloquer des systèmes, ou même de nuire à un concurrent par le biais de ce que l'on pourrait appeler des « tueurs à gages cyber ».

JSS : En quoi consiste la mission d’Eurolaw France Cyber auprès des entreprises susceptibles de connaître des cyberattaques ?

P-M.G : Il est essentiel de se demander ce qui existait auparavant sur le marché pour accompagner les entreprises face aux risques cyber. On y trouvait principalement des avocats, des experts informatiques, et de grandes sociétés d'audit. En plus de ces acteurs, il y avait des entreprises spécialisées dans la gestion de crise, des fabricants de logiciels, et bien sûr, des assureurs. L'idée derrière la fondation de notre association a été de rassembler cette

diversité de services sous un même toit, offrant ainsi une approche globale pilotée en fonction des besoins spécifiques de chaque client.

Notre mission va au-delà de la simple formation ou information sur les cyber-risques. Nous proposons une gestion complète des risques, incluant la cartographie et la hiérarchisation des risques, ainsi que l'élaboration de plans d'action pour les atténuer. Cette approche englobe la détection et le traitement des vulnérabilités, et s'étend jusqu'à la création de plans de résilience. Pour ce faire, notre panel de services inclut non seulement des avocats et des experts informatiques, mais aussi des éditeurs de logiciels, assurant une couverture complète des besoins des entreprises.

À chaque étape, nous proposons un chef de projet dédié qui veille à définir les besoins du client de manière précise, et à adapter notre offre en conséquence. Cela inclut également la mise en place de contrats d'assurance, car nous avons constaté que de nombreuses entités, qu'elles soient publiques ou privées, n'avaient pas un accès adéquat au marché de l'assurance pour faire face aux cyberattaques, que ce soit d'un point de vue financier ou technique.

Le manque d'information et de maturité intellectuelle sur ces sujets empêchait ces entreprises de définir un plan d'action efficace. C'est pourquoi notre association s'est particulièrement focalisée sur la sensibilisation des dirigeants. En effet, c'est à travers eux, qu'ils soient à la tête d'entreprises publiques ou privées, que la décision de déployer une politique de gestion des risques cyber peut être prise et mise en œuvre de manière efficace. Il est crucial de commencer par le commencement, et c'est en sensibilisant les dirigeants que nous pourrons véritablement les accompagner dans la mise en place d'un plan d'action complet et d'un traitement durable des risques.

JSS : Entre autres risques liés à une cyberattaque, on l'oublie souvent, la responsabilité des dirigeants d'entreprise et des exécutifs publics peut être engagée. Comment cela se fait-il ? Quels risques encourent-ils ?

P-M.G : La première source de droit en matière de cybersécurité repose sur le droit civil général, qui établit que toute personne causant un préjudice à un tiers peut être tenue responsable et, en conséquence, être contrainte de verser des dommages et intérêts, conformément aux principes établis dans le Code civil français. Ce concept de responsabilité est universel, présent dans les systèmes juridiques français, allemand, américain, et bien d'autres.

Cependant, face à la spécificité des risques liés au cyberespace, le législateur a jugé nécessaire d'introduire des cadres juridiques additionnels. Parmi ces cadres, la réglementation sur la protection des données personnelles, établie au niveau européen, joue un rôle crucial. Cette réglementation encadre la gestion des données personnelles, c'est-à-dire toutes les informations permettant d'identifier un individu, telles que le nom, le prénom, l'adresse, le numéro de sécurité sociale, les données bancaires, ainsi que les préférences religieuses, sexuelles, politiques, etc. En raison de la capacité des technologies informatiques à stocker, regrouper, et traiter ces données, les entités, qu'elles soient des personnes morales ou physiques, de droit privé ou public, qui traitent ces informations se voient imposer une responsabilité spécifique.

À lire aussi : Cybersécurité et entreprises : quelle marche à suivre pour assurer (autant que possible) ses arrières ?

En cas de non-respect de ces obligations, les sanctions peuvent être sévères. Pour les personnes morales, les amendes peuvent atteindre jusqu'à 20

millions d'euros, ou 4 % du chiffre d'affaires mondial, ce qui constitue une pénalité extrêmement dissuasive. Les personnes physiques, quant à elles, risquent jusqu'à 300 000 euros d'amende et cinq ans d'emprisonnement.

C'est la CNIL (Commission nationale de l'informatique et des libertés) en France, ou son équivalent dans d'autres pays européens, qui est l'organisme chargé de veiller au respect de ces réglementations. En cas de fuite de données personnelles, la loi LOPMI impose désormais une obligation de déclaration à la CNIL dans un délai de 72 heures. Les responsables doivent alors mettre en œuvre des mesures correctives et notifier les tiers concernés, les informant que leurs données pourraient avoir été compromises et détaillant les actions prises pour en limiter les effets, dans la mesure du possible.

JSS : Quelles mesures ont été mises en place pour réduire l'écart de sécurité entre les PME, les entreprises de taille intermédiaire (ETI) et les grandes entreprises face aux cyberattaques ?

P-M.G : Le deuxième point crucial est la directive NIS 2, qui représente une avancée majeure dans la régulation des cyber-risques. Cette directive européenne, qui entrera en vigueur en octobre 2024, impose un ensemble d'obligations spécifiques aux entreprises face aux menaces cybernétiques. Contrairement au RGPD qui s'adresse plus largement à toute entité traitant des données personnelles, la directive NIS 2 cible spécifiquement les entreprises, en particulier celles opérant dans des secteurs critiques.

Les grandes entreprises, à l'échelle mondiale, ont déjà intégré ces problématiques dans leur gouvernance. Elles disposent généralement de services dédiés à la gestion des risques, et ont conscience de leur vulnérabilité, ce qui fait du cyber-risque un sujet de gouvernance prioritaire.

En revanche, les PME et les ETI, qui n'ont pas la même structure ou les mêmes ressources, sont souvent plus concentrées sur leurs opérations courantes, comme gérer leur business plutôt que sur la gestion des risques cyber. Cela les rend particulièrement vulnérables, surtout si elles n'ont pas encore été confrontées directement à des incidents de cybersécurité. Surtout qu'elles représentent une cible privilégiée pour les hackers, qui les exploitent comme une porte d'entrée vers des entreprises plus importantes. En attaquant ces PME et ETI, souvent moins bien protégées, les cybercriminels peuvent accéder aux informations cruciales des grandes entreprises qu'elles sous-traitent, permettant ainsi de récupérer des données stratégiques sans affronter directement les défenses robustes des grandes corporations.

Du coup, cette directive NIS 2 est conçue pour combler le fossé en matière de cybersécurité au sein des entreprises. En France, elle va concerner environ 10 000 entreprises réparties sur 18 secteurs d'activité considérés comme hautement critiques. Ces entreprises, selon leur importance et l'impact potentiel d'une cyberattaque sur la fourniture de services essentiels aux États membres, seront tenues de mettre en place des mesures de protection rigoureuses contre les risques cyber. L'objectif de cette directive est d'améliorer la résilience des entreprises face aux menaces numériques, un enjeu crucial dans un monde où la digitalisation rapide expose les organisations à des risques de plus en plus importants. Pour s'assurer de la conformité, l'ANSSI sera chargée de contrôler que ces entreprises respectent bien les exigences de la directive.

Les dirigeants devront prouver qu'ils ont suivi des formations spécifiques et démontrer qu'ils ont instauré une véritable politique de gestion des risques, avec des plans d'action détaillés et des mesures d'évaluation. Si ces exigences ne sont pas respectées, des sanctions pourront être imposées, pouvant aller jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel de l'entreprise.

Pour les PME et les ETI, la mise en conformité avec NIS 2 représente un défi important. Elles devront soit s'équiper de solutions de protection appropriées, soit faire appel à des sous-traitants spécialisés pour gérer la protection de leurs données. Il est probable qu'une période de transition soit accordée pour permettre à ces entreprises de se préparer avant que les sanctions ne soient appliquées.

JSS : En 2021, une task force opérationnelle a été lancée au sein de votre Réseau, en cas de mise en cause de leur responsabilité civile ou pénale. Quelle expertise, quel service apportez-vous ?

P-M.G : Alors, justement, tout cet accompagnement autour des obligations juridiques telles que le RGPD ou la directive NIS 2 englobe en réalité un ensemble d'exigences complexes. L'objectif est d'aider les entreprises à répondre à leurs impératifs de conformité. Concrètement, cela commence par l'intervention des avocats, qui se chargent de structurer la partie juridique de ces obligations. Leur rôle ne se limite pas à conseiller sur les politiques à mettre en place, mais aussi à rédiger des procédures claires et adaptées au fonctionnement interne de l'entreprise, afin de s'assurer que rien n'a été négligé et que tout est conforme.

Sur le plan technique, l'accompagnement prend une dimension tout aussi cruciale. Il s'agit d'assister les entreprises sur le plan informatique pour qu'elles puissent établir et piloter une véritable politique de gestion des risques. À cet égard, une société du groupe Eurolaw, nommée Égérie, joue un rôle clé. Égérie propose un logiciel déjà largement utilisé par de grandes entreprises, qui permet de centraliser toutes les informations relatives à la gestion des risques en fonction des normes internationales en vigueur.

« Il y a tout un travail d'éducation à mener au sein des entreprises pour instaurer une véritable culture de la sécurité numérique »

Pierre-Marie Gauthier, secrétaire général d'Eurolaw France Cyber

Les experts d'Eurolaw sont ainsi capables de guider les entreprises dans la mise en place et le déploiement de leurs politiques de gestion des risques sur cette plateforme. Celle-ci offre un pilotage extrêmement fin des vulnérabilités cyber et permet également de développer un plan d'action pour quantifier les risques. À partir de cette quantification, les entreprises peuvent planifier leurs investissements financiers de manière progressive et ciblée afin de renforcer leur sécurité et de réduire leurs vulnérabilités.

En outre, Égérie a développé un module spécifique pour l'assurance, qui permet de renseigner toutes les données nécessaires aux assureurs pour évaluer si le risque est assurable. Ce logiciel peut extraire les informations pertinentes pour chaque compagnie d'assurance, ce qui facilite grandement le travail des courtiers. Car ces derniers, en fonction des politiques de sécurité mises en place par l'entreprise, peuvent ainsi identifier les assureurs les plus adaptés à son profil de risque, en s'appuyant sur une évaluation précise et objective des risques.

JSS : Comment les dirigeants peuvent-ils se prémunir d'une cyberattaque, et ainsi, éviter que leur responsabilité ne soit engagée ?

P-M.G : Le sujet central ici, c'est de mettre en place une véritable politique de gouvernance du risque cyber pour les entreprises. Pour cela, il est nécessaire de s'entourer d'experts afin de bien cerner et comprendre la nature de son

risque cyber. Pour un dirigeant de PME ou d'ETI, il s'agit de se poser les bonnes questions : quelles sont les données personnelles que je traite, en quelle quantité, et dans quel contexte ? Comment mon système informatique est-il armé pour résister à des attaques potentielles ? Tout cela commence par un audit approfondi.

Cet audit initial est indispensable pour dresser un état des lieux clair de ce qui est fait, de ce qui ne l'est pas, et de ce qui doit être amélioré. C’est exactement ce que nous faisons actuellement pour un gros syndicat de l’eau, où tout a commencé par un audit détaillé. À partir de cet audit, nous avons pu recommander un ensemble de mesures prioritaires à mettre en place, mais ce n'est que le début du processus de mise en place d'une véritable politique de gestion du cyber-risque.

Cela signifie aussi nommer un DPO (délégué à la protection des données) si l'entreprise n'en a pas, surtout lorsqu’il s’agit d’une entité essentielle. Il faut également s’assurer que l’on dispose d’un RSSI (responsable de la sécurité des systèmes d'information) et qu’un plan soit mis en place pour protéger les vulnérabilités détectées, avec un suivi régulier des mesures mises en œuvre.

Par ailleurs, acheter un logiciel de protection ne suffit pas. Il s’agit d’instaurer une politique d’audit rigoureuse, avec une révision régulière de ce plan pour ajuster les investissements humains et financiers nécessaires. La formation joue aussi un rôle clé, car une bonne politique de cybersécurité repose avant tout sur les bons réflexes. On le constate chez les particuliers, où les erreurs d’hygiène numérique, comme le partage de données bancaires à des arnaqueurs via des phishing, sont fréquentes. Il y a donc tout un travail d'éducation à mener au sein des entreprises pour instaurer une véritable culture de la sécurité numérique.

JSS : Dernièrement, quelles méthodes de piratages des entreprises ont le plus la cote ?

P-M.G : En entreprise, le phishing reste la méthode la plus redoutable et la plus courante, visant à escroquer, voler ou crypter des données, souvent en préparation d'une attaque par ransomware. Cette technique est largement répandue car elle est financièrement efficace, surtout dans le secteur privé où, malgré les recommandations contraires et l'obligation de déclarer les sinistres dans les 72 heures, certaines entreprises privées peuvent encore céder à la tentation de payer la rançon demandée. Dans le secteur public, le paiement de rançons est moins fréquent, en grande partie à cause des restrictions légales et des contraintes budgétaires.

La nature des attaques varie également en fonction du type de cybercriminel en question. Par exemple, lorsqu'il s'agit d'acteurs motivés par des objectifs politiques, les attaques de type DDoS, qui consistent à saturer les serveurs d'une entreprise jusqu'à les rendre inopérants, sont courantes. Ces attaques sont purement malveillantes, et visent à paralyser l'entreprise sans chercher à en tirer un gain financier direct. Il en va de même pour les attaques virales qui ont pour seul but de perturber le fonctionnement de l'entreprise, voire de l'anéantir.

Il existe bien sûr d'autres types d'attaques, souvent moins sophistiquées, mais toujours dans le but de voler des données ou de bloquer des services critiques. Ainsi, il n'est pas surprenant que le phishing et les attaques DDoS soient en pleine expansion, car ce sont les moyens les plus directs et les plus efficaces pour les cybercriminels d'atteindre leurs objectifs. Quant aux virus informatiques traditionnels, souvent créés par de jeunes génies cherchant à se faire un nom, ils existent toujours, mais ils ne représentent pas la menace principale pour les entreprises aujourd'hui.

JSS : Les Jeux Olympiques de Paris 2024 ont-ils contribué à l'augmentation du nombre d'entreprises touchées par les attaques ? Peut-on le craindre également avec les Jeux Paralympiques ?

P-M.G : Je pense qu'il sera pertinent de faire le point dans un certain temps, car il est encore trop tôt pour se prononcer de manière définitive. Cependant, il est évident que les risques sont nombreux, car la France est particulièrement exposée à diverses menaces. Prenons par exemple la situation avec la Russie : l'exclusion des athlètes russes des JO pourrait bien susciter des réactions, et il n'est pas exclu que certains espèrent voir la France rencontrer des difficultés cet été, notamment en matière de sécurité.

Mais on assiste souvent lors de tels événements à une recrudescence des attaques cybernétiques, comme cela a été le cas lors des précédents Jeux Olympiques. Les grands événements internationaux attirent toujours une attention accrue, non seulement des spectateurs et des médias, mais aussi des cybercriminels et autres acteurs malveillants, qui voient là également une opportunité de perturber, d'exercer des pressions ou de démontrer leurs capacités.

JSS : Comment jugez-vous l'efficacité de notre arsenal législatif français et européen pour faire face à la menace cyber qui plane sur les entreprises ?

P-M.G : Je pense que nous avançons progressivement dans la bonne direction, notamment avec le déploiement de la directive NIS 2, même si cela ajoute une certaine complexité pour les entreprises. En parallèle, le Règlement général sur la protection des données (RGPD) est en vigueur dans toute l'Europe, mais il y avait une faille majeure qui est enfin en train d'être corrigée : la vulnérabilité des données européennes lorsqu'elles sont stockées

sur des clouds souverains américains. Ce problème est lié au Cloud Act, la législation américaine qui permet aux autorités américaines de récupérer, en toute légalité mais de manière discutable, des données appartenant à des entités étrangères.

Cette situation pose un problème crucial de souveraineté et d'extraterritorialité, car elle permet aux États-Unis d'exercer une forme d'impérialisme numérique. C'est particulièrement dangereux compte tenu de l'avance technologique significative des États-Unis dans ce domaine. Il ne faut pas oublier que la majorité des grandes entreprises technologiques mondiales sont américaines, et que près de 80 % du savoir-faire technologique est concentré là-bas. En conséquence, si les États-Unis peuvent accéder aux données du monde entier, cela donne un sens très réel au concept de « Big Brother is Watching You ».

Cependant, il est encourageant de voir que la Cour européenne de justice a apporté un nouveau cadre important pour renforcer la protection des données (dit cadre de protection des données : CPD, ou DPF en anglais : « Data privacy framework »). L'Union européenne commence enfin à prendre fermement position contre ce type de lois extraterritoriales. Cela montre que l'arsenal juridique et réglementaire européen se renforce progressivement, même si, comme pour toute chose, cela prendra du temps à se mettre pleinement en place.

Propos recueillis par Romain Tardino