CYBER CERCLE
collection

SÉCURITÉ NUMÉRIQUE en SANTÉ

Regards croisés

Cédric CARTAU
Ingrid DUMONT
Loïc GUÉZO
Philippe LOUDENOT
Fabien MALBRANQUE
Garance MATHIAS
Marina PISANO
Myriam QUÉMÉNER

Préface de Bénédicte PILLIET

2023

SÉCURITÉ NUMÉRIQUE en SANTÉ

Regards croisés

Ce livre est édité sous la direction de
Bénédicte PILLIET, Présidente du CyberCercle

Préface

BÉNÉDICTE PILLIET
Présidente
CyberCercle

Secteur de la santé et sécurité numérique : une thématique que le CyberCercle traite régulièrement depuis plusieurs années déjà, que ce soit dans ses événements ou ses publications.

Si, aujourd'hui, la nécessité de prendre en compte la sécurité numérique pour le secteur de la santé ne fait plus aucun doute - les affaires médiatisées nous le rappellent régulièrement avec un nombre important d'établissements de santé victimes - , ce ne fut pas toujours le cas, même dans un passé somme toute récent. L'enjeu majeur que représente le secteur de la santé pour le bon fonctionnement de la société, la richesse qu'il génère par les données qu'il produit intrinsèquement, ressources indispensables pour la recherche et, aujourd'hui, pour alimenter les intelligences artificielles qui, notamment, aideront à mieux soigner, en fait un secteur d'autant plus intéressant pour les cybercriminels.

Mais une prise de conscience, parfois forcée par ces évènements, ne suffit pas toujours à engager une démarche de sécurité numérique efficace dans un secteur aussi vaste et hétérogène que celui de la santé. Des laboratoires d'analyses biologiques à l'industrie pharmaceutique, en passant par les établissements de recherche, les centres hospitaliers et les professions libérales, une myriade d'acteurs interdépendants et utilisant de plus en plus d'outils numériques, contribuent in fine à la santé des patients que nous sommes tous.

Comment, dans un environnement mondialisé, ouvert et complexe, de l'infiniment grand à l'infiniment petit, pour reprendre une pensée de Pascal dont nous fêtons cette année le 400ème anniversaire de la naissance, aborder sereinement cette question essentielle qu'est la sécurité numérique pour le secteur de la santé avec, au cœur, l'intérêt du patient au centre des préoccupations ?

En partant du diagnostic, comme pour un patient, quels « traitements » conseiller à l'heure où les politiques publiques manquent de lisibilité, les ressources financières demandent des arbitrages permanents et où les ressources humaines se raréfient et sont difficiles à pérenniser au point d'atteindre une pénurie inquiétante ?

À l'heure où, après le RGDP et la loi santé, les réglementations consacrées à la sécurité numérique se développement tous azimuts, avec la très suivie et attendue transposition à venir l'année prochaine de la directive européenne NIS 2, le volet réglementaire est-il la bonne approche ?

Dans ce contexte, le quatrième ouvrage de la collection Regards Croisés du CyberCercle vise à apporter des éclairages, « un recueil de pensées », sur diverses thématiques, non exhaustives d'ailleurs, dans le vaste champ de la sécurité numérique pour le secteur de la santé, et à nous faire réfléchir, chacun, pour passer à l'action, ensemble.

Parce que, encore et toujours, en sécurité numérique, « seul on ne va nulle part, ensemble on va plus loin et plus vite ».

Je vous souhaite une bonne lecture.

Première ascension de la cyber par la face ouest ou le regard totalement décalé d'un RSSI qui ne l'est pas moins

CÉDRIC CARTAU
RSSI et DPO
CHU de NANTES et GHT44

Il est de ces domaines ou sujets de réflexion dont l'intérêt dépasse la matière elle-même. Entendre par cela que si le sujet initial peut nécessiter de la dextérité, de l'expérience voire un haut niveau de compréhension, la pratique finit par faire apparaître une ou plusieurs facettes à priori pas visibles.

Tout le monde connaît l'Histoire du déclenchement de la Première Guerre Mondiale : l'assassinat, à Sarajevo, de l'archiduc François-Ferdinand, héritier du trône d'Autriche-Hongrie, et de son épouse, le 28 juin 1914. Mais les historiens débattent depuis près d'un siècle sur l'analyse réelle des causes de ce premier conflit mondial - et tous d'ailleurs s'accordent à dire que l'attentat susnommé n'était « que » l'étincelle d'une situation qui empirait depuis des décennies, sans cet attentat un autre évènement pas forcément plus visible aurait abouti au même Armageddon. Récemment je suis tombé sur un article qui proposait une vision tout à fait différente de la situation, en mettant notamment l'accent sur le fait qu'à l'époque tous les pays futurs belligérants (sauf la France) étaient des monarchies dont les monarques étaient tous apparentés mais avaient abandonné le pouvoir à leurs Ministres pour mener une vie de loisir. C'est en ce sens que l'Histoire est passionnante : on peut mentalement « tourner » autour d'un fait, d'une période, d'un peuple et avoir des visions totalement différentes selon l'angle d'attaque.

La cyber est de ceux-là : tous les RSSI qui pratiquent la discipline depuis suffisamment longtemps vous diront que leur quotidien de 2023 n'a pas grand-chose à voir avec celui de 2013 voire de 2003. Tout comme pour l'Histoire, il est possible et même souhaitable de mentalement « tourner » autour des concepts régissant la cyber pour disposer d'un autre point de vue, d'un autre angle d'attaque, d'une autre approche. Certaines de ces approches sont au final vaines, sans intérêt, inadéquates, mais certaines finissent par devenir la pensée ou l'approche dominante - une sorte de sélection naturelle appliquée aux idées en somme. Juste pour exemple, quand j'ai démarré en 1999 la préoccupation principale était les antivirus des PC : 24 ans plus tard on parle de SMSI, d'ISO, de cloisonnement, d'audits, etc.

Petit voyage en absurdie, totalement assumé.

Et si la cyber était fractale ?

Une fractale, c'est cette figure mathématique qui a la particularité de montrer une structure similaire quelle que soit l'échelle : en zoomant sur n'importe quelle partie, on retrouve la figure d'origine. En 1975, Benoit Mandelbrot a démontré que les fractales étaient présentes un peu partout dans la nature (la côte bretonne est par exemple une fractale, comme un flocon de neige, etc.).
Un SMSI (Système de Management de la Sécurité de l'Information) est fractal. Cela peut paraître étrange, mais très facile à illustrer. La base d'un SMSI c'est la roue de Deming : PDCA pour Plan Do Check Act. Mais, et c'est là le point qui n'est pas évident à saisir au premier abord, le Plan lui-même doit être révisé (Check) et avoir un plan de correction (Act). Tout comme le Do d'ailleurs. Tout comme le Check aussi (les procédures de contrôle sont avant tout des procédures qui elles-même s'auditent). De sorte que dans le PDCA initial s'enchâsse 4 PDCA, et on peut continuer ainsi de suite sans fin.
En fonction du numéro de la roue dans laquelle tel ou tel agent évolue (le premier PDCA, ou le PDCA du premier P, etc.) les fiches de poste et les missions sont faciles à expliciter.

Et si les assurances cyber étaient... trop peu chères ?

Les assureurs qui ont une offre de protection cyber au catalogue se divisent en deux catégories : ceux qui la maintiennent mais la réduisent fortement, et ceux qui tout bonnement la suppriment.
Les offres maintenues voient leur périmètre réduit (franchise en hausse, garantie tendant à se recentrer sur de l'aide technique en cas d'attaque, etc.) et les prix aussi, ce qui est dangereux à moyen terme. Dangereux car une fois qu'une entreprise aura souscrit une offre, il est facile de tomber dans le travers de « bon ça y est on est assuré on ne craint rien ». Tout contrat qui n'est pas accompagné d'un plan de réduction obligatoire, avec des audits périodiques à la charge financière exclusive du client, des actions techniques pilotées, budgétées et suivies dans le temps, des augmentations sévères de cotisation si l'assuré ne joue pas le jeu n'est qu'un bout de papier inutile. Ce qui ne coûte presque rien ne vaut presque rien.

Le Build c'est du Run, le Run c'est du Build

J'aime ce genre d'inversion qui oblige à faire un 180° sur le point de vue classique.
Le Build - ou l'investissement, ou le CAPEX - consiste à construire quelque chose de nouveau. Dans les DSI on parle de projet, dans la cyber aussi.
Le Run - ou exploitation, ou OPEX - consiste à faire tourner le machin, dans les DSI on parle de MCO (Maintien en Conditions Opérationnelles), dans la cyber aussi.
Mais le Build est aussi du Run : le flux constant de projets (cyber ou pas) oblige à mettre en place des processus documentés et cadrés, à en mesurer l'efficience / efficacité, bref à considérer le portefeuille de projets d'une DSI comme les différents wagons d'un train qui roule continuellement.
Mais le Run est aussi du Build : il faut bien mettre en place une cellule ou équipe MCO, bien définir des conditions qui permettent à un projet de passer du stade Build au stade de « runable » ou exploitable. Il faut « Builder » le processus de Run autant qu'il faut « runner » le processus de Build.

Et si l'on devait se méfier de l'ISO ?

Plusieurs organisations qui se sont engagées dans une certification ISO finissent par faire un constat étonnant : à n'y prendre garde, la démarche ISO finit par diriger tout le monde. Entre les comités machin, les Copils bidule, les audits internes / externes, les plans de remédiation, tout finit par graviter autour de l'ISO qui agit comme une planète à forte masse conditionnant et attirant à elle toutes les décisions managériales. Et c'est une anomalie : une démarche ISO ce n'est rien d'autre que de la Qualité, et ce ne sont pas les qualiticiens qui dirigent l'organisation, pas plus que ce ne sont les juristes, les financiers, les DRH, etc. L'Organisation est dirigée par un Directeur Général, et l'ISO n'est rien d'autre qu'un élément dont il faut tenir compte dans la prise de décision. Trop peu d'ISO c'est mal, mais trop d'ISO tue l'ISO.

Et si la cyber s'inscrivait dans le contexte de la lutte entre le droit Romain et le droit jurisprudentiel ?

Il existe schématiquement deux systèmes juridiques : celui en vigueur dans la plupart des pays latins et basé sur un corpus de règles de droit (lois, décrets, arrêtés), et celui (anglo-saxon) presque exclusivement basé sur la jurisprudence, dont l'évolution permanente constitue le corpus de règles.
On retrouve peu ou prou la même dichotomie en cyber, entre ce qui relève du droit (la PSSI, la fameuse) et ce qui relève de la source jurisprudentielle (les mesures de sécurité MS, ou politiques techniques, elles-mêmes alimentées par le contexte, les incidents, etc.).
Savoir ce qui émane de l'une et influence l'autre fait débat : commence-t-on par la PSSI pour découler des MS, ou fait-on l'inverse ?

Et si la cyber n'était que point de bascule ?

Paul Revere est un personnage peu connu en France mais célébrissime aux USA pour avoir, à lui seul, alerté un nombre considérable de personnes dans le Boston de 1775 sur l'arrivée imminente des armées anglaises, et avoir ainsi indirectement contribué à la réussite du soulèvement qui sera la Révolution Américaine. Malcom Gladwell classifie ainsi dans son ouvrage « Le point de bascule » les typologies de personnages au sein des

organisations - les connecteurs, les mavens, les « vendeurs », etc. - qui sont des nœuds de communication au sein des organisations.
Identifier ces individus, savoir ce que leur typologie d'appartenance leur permet de faire, et savoir identifier soi-même sa propre catégorie permet immanquablement d'améliorer les processus cyber internes.

Et si la cyber n'était que Detritus ?

Sortir au patron d'une BU que son collègue de l'autre BU (de préférence un qu'il ne peut pas piffrer) compte utiliser ses meilleurs scores sur les indicateurs cyber globaux de la boite pour briguer un poste de n+1...c'est faux mais invérifiable, mais surtout jubilatoire. La vanité est le plus vieux défaut du monde, pourquoi ne pas l'utiliser pour faire avancer le schmilblick en cyber ?
Lire et relire « La Zizanie », cet album d'Astérix où le truculent personnage de Detritus fiche le bazar absolument partout où il passe pour parvenir à ses fins. Et essayer de ne pas terminer comme lui : aux fers.

Et si la cyber n'était que management ?

Théorie sur les biais de la prise de décision, Programmation Neuro Linguistique, socio-dynamique : la cyber n'est après tout que management et identification des processus de décision, et si les formations aux biais de décision faisaient partie du package obligatoire chez tout RSSI qui se respecte ?

Et si le seul objectif de la cyber... était de disparaître ?

Dans « Une brève histoire du futur », Michio Kaku (physicien théorique américain) émet l'idée que l'essence même de toute technologie est de disparaître, au sens de ne plus être visible (mais être toujours présente bien entendu). Et de prendre pour exemple le papier.
Le papier tel que nous le connaissons aujourd'hui a d'abord été un produit de luxe utilisé pour des objets dont le tarif allait au-delà de l'entendement : le livre. On raconte qu'une reine de France, au moyen-âge, avait acheté un manuscrit à une abbaye, et avait pour cela payé un troupeau de 200 moutons ! De nos jours le papier est absolument partout, même sur les

murs et nous n'y prêtons même plus attention. Il en va de cela de toutes les technologies, qui passent peu ou prou de « tellement cher que seuls les princes peuvent se les offrir » à « tellement banal qu'on ne les remarque même plus ».
Un jour peut-être pour la cyber ?

La cyber en santé... ou la santé en cyber ?

Et si la cyber était la santé de l'IT ? On y développerait alors des concepts de résilience, terme qui a été introduit en France par Boris Cyrulnik et qui désigne en gros la capacité d'un individu à se relever après un traumatisme (attentat, zone de guerre, etc.). Voir le PCA-PRA au travers du prisme de résilience est intéressant à double titre, bien entendu par les dispositifs techniques qui amène à déployer, mais surtout au travers des processus et protocole de reprise après sinistre. Une résilience cyber en somme, c'est avant tout la capacité de rebondir.

Conclusion

Ces dichotomies sont toutes fausses et vraies à la fois : fausses car la cyber ne peut se résumer à des discussions binaires, vraies parce qu'elle impliquent de prendre un autre point de vue sur ce sujet protéiforme.
Une chose est certaine cependant : de même que la cyber d'aujourd'hui n'a strictement rien à avoir avec celle d'il y a 15 ans, dans 10 ans l'angle d'attaque sera complètement différent.
Management pur ? Certification-centrée ? Technophile ou phobe ? Nul ne sait, mais tout le monde est certain qu'il faut rester en éveil afin d'anticiper le prochain alignement des planètes.

Sécurité numérique : de l'acceptabilité de la contrainte au renforcement de la valorisation d'une organisation

INGRID DUMONT
Coordinatrice scientifique
Projet DRIFT-FH
&
MARINA PISANO
Chercheuse Ph.D
Université Technologique de Compiègne

Notre retour d'expérience s'inscrit dans le cadre du programme de recherche DRIFT-FH (Digitalisation, Risques, Incertitudes et Fragilités des Technologies associées aux Facteurs Humains), qui vise à réduire les vulnérabilités associées aux facteurs humains en sécurité du numérique dans les secteurs de la santé et de la défense. Ce projet transdisciplinaire allie les sciences humaines et sociales et les sciences de l'ingénieur pour atteindre ses objectifs. Lancé en janvier 2022 et financé par l'Agence Nationale de la Recherche (ANR), il entre dans la catégorie sécurité globale et cybersécurité. L'étude que nous vous présentons dans cet article fera l'objet d'une publication scientifique que nous partagerons au CyberCercle et qui vous rendra compte de l'intégralité des résultats. Notre témoignage porte sur l'acceptabilité de la contrainte dans la sécurisation des données au sein des organisations du secteur de la santé et la manière de parvenir à cette dernière.

Le secteur de la santé subit des vagues de cyberattaques mettant à rude épreuve ses diverses organisations, leurs personnels tout comme l'ensemble de leurs parties prenantes. La santé étant un secteur particulièrement prisé par les cyberattaquants, les données de santé sont parmi les plus recherchées sur le marché noir et comptent parmi les plus coûteuses. La question de la protection des données est donc un sujet particulièrement

sensible. L'atteinte à ces données peut constituer dans un même temps une violation du secret médical mais également porter préjudice à la vie privée des personnes concernées. Visé par l'article 9 du Code civil, le respect de la vie privée représente un enjeu important pour les personnes concernées dans les atteintes aux données de santé. De plus, il convient de considérer que la santé n'est pas le secteur le plus aisé en matière de sécurité numérique car le secret médical est un secret partagé et la gestion des accès à ce dernier n'est pas la même selon les acteurs considérés.

De manière générale, lorsque nous parlons de la sécurité des données, il convient de prendre en compte trois critères pour en saisir ses particularités : l'intégrité, la disponibilité et la confidentialité. Selon les acteurs, le degré d'urgence et la gravité de la situation, la priorisation n'est pas la même. En effet, si les médecins privilégient la disponibilité et l'intégrité des données, les patients quant à eux accordent une attention particulière à la confidentialité de l'information (d'autant plus quand une fuite de cette dernière leur fait perdre l'accès à certains droits). Il est donc fondamental de considérer que les acteurs des organisations de santé évoluent dans un environnement empreint du secret médical, et que leur dynamique culturelle les prédispose à la protection du secret. Cela fonde l'expectative d'une acceptation plus importante des mesures de sécurité (techniques et organisationnelles) de l'information par rapport à d'autres secteurs d'activité.

Outre les cybermenaces extérieures, ce secteur doit aussi faire face aux conséquences des vulnérabilités internes qui relèvent des individus et/ou des organisations et de leur environnement et qui peuvent involontairement porter atteinte aux informations (données personnelles et sensibles) des personnes concernées (patients et leur famille -pour les antécédents familiaux-, personnel de l'établissement, partenaires, etc.). Les vulnérabilités internes sont diverses et sont autant des sujets techniques qu'organisationnels et humains.

C'est pourquoi une analyse de risques techno-centrée ne permet pas suffisamment de prendre en compte les mesures organisationnelles de sécurisation. Le Règlement Général de la Protection des Données (RGPD) permet dans le cadre des analyses d'impact sur la vie privée d'allier les

fiabilités techniques et humaines dans l'analyse de risques relatifs aux données et d'intégrer de la sûreté à la sécurité de l'information.

C'est dans ce contexte que nous avons conduit une étude[1] qui porte sur la question de savoir si la manière dont un acteur de santé publique peut, sous couvert d'une mise en conformité à une réglementation visant à renforcer la protection des données, accroître sa fiabilité en s'appuyant sur ses facteurs organisationnels et humains en complément des aspects techniques de la sécurisation de ses systèmes d'information. Sous les aspects d'un contexte de contrainte, l'organisation peut-elle ainsi se créer une opportunité en fédérant l'ensemble de ses parties prenantes autour des enjeux de sécurité de l'information ?
L'étude que nous avons conduite a pour but de favoriser la construction d'une dynamique de changement individuel, collectif et organisationnel au sein d'un organisme de prévention en santé publique via l'intégration de l'ensemble de ses parties prenantes.

Elle présente un double objectif. Le premier objectif relève de la mise en conformité juridique de l'ensemble des pratiques des parties prenantes de l'organisation en considérant le Règlement Général de la Protection des Données Personnelles (RGPD). Le deuxième objectif porte sur la levée de certaines résistances de la part du personnel et du public cible.

L'organisme de prévention en santé publique

L'organisme au sein duquel nous avons conduit cette étude se constitue d'un centre régional et d'antennes locales (par départements) et comporte un effectif compris entre 20 à 49 personnes. Une des principales actions de l'organisme repose sur une mission de service public dans le cadre de la prévention en santé publique, et notamment d'une prise en charge du dépistage de pathologies. Il met ainsi en œuvre la politique de prévention en santé publique tout en coordonnant les divers acteurs intervenant dans le cadre de sa mission (laboratoires, médecins, infirmières, etc.). De plus, il contribue à la formation initiale des médecins et à la recherche médicale dans son domaine d'activité.

Si nous avons choisi cette structure, c'est parce qu'elle a dû faire face dans

le même temps à différentes contraintes organisationnelles, humaines et réglementaires qui ont eu des effets difficiles à gérer et pouvant porter atteinte à son bon fonctionnement. Elle venait notamment d'opérer une refonte de ses systèmes d'information (SI) quand la pandémie de COVID-19 est apparue, aggravant l'instabilité et l'incertitude du contexte (obligation de mettre en place le télétravail, ralentissement des examens de dépistage et des prises en charge), exposé d'autre part à l'attrait des cyberattaquants pour les organisations du secteur de la santé. À cela s'ajoutait le fait que cette structure, qui a des interactions avec des individus multiples pour la réalisation de ses missions, a ainsi une surface d'attaque importante, son système d'information nécessitant de multiples interconnexions augmentant le risque d'une cyberattaque directe ou indirecte contre l'organisme. Ce dernier est aussi un acteur d'un système interdépendant pour la sécurité et la qualité des données de sa population éligible (ou public cible).

Une démarche sur-mesure et co-construite en trois temps pour permettre la conformité au RGPD de l'organisation

Pour conduire cette étude et ainsi favoriser la construction d'une dynamique sur-mesure à la fois individuelle, collective mais aussi organisationnelle, nous avons déployé notre démarche en trois temps, par des étapes à la fois distinctes et complémentaires : 1. Diagnostic ; 2. Ateliers de réflexion et de sensibilisation ; 3. Formalisation des outils adéquats au bon déploiement de la démarche et de son acceptation.

1. Le diagnostic : une première étape d'identification des pratiques et de la libération de la parole des parties prenantes

Le diagnostic est une première étape incontournable de la démarche qui consiste à observer l'organisation et évaluer sa conformité au RGPD selon notre compréhension de son contexte, de son histoire, ses pratiques, son environnement (conditions de travail, réseaux de partenaires, public cible, etc.). Il permet de saisir quelle perception ses parties prenantes (internes et externes) ont de l'autorité et de la protection des données. D'autre part, il est un véritable outil qui permet de libérer la parole et de mettre en

lumière les flux de communication formels et informels au sein de l'organisation. L'analyse des pratiques et des comportements des acteurs est aussi une opportunité d'expliciter l'enjeu de notre étude. Le diagnostic favorise ainsi les échanges, et finalement la transparence et la compréhension de la démarche, indispensables pour dissiper les peurs et lever les freins au changement qui accompagnent tout projet de mise en conformité réglementaire. Grâce au diagnostic, le facteur humain est intégré ; ce dernier étant un élément de succès dans les changements organisationnels (Bareil, 2004)[2].

Si cette phase de diagnostic permet de mettre certes en lumière les points de l'organisation à améliorer, elle favorise aussi et surtout l'identification d'atouts à faire fructifier pour atteindre plus aisément les objectifs fixés (la mise en conformité juridique). Le diagnostic permet l'identification des leviers et des piliers sur lesquels il est possible de nous appuyer dans notre démarche.

Enfin, la restitution du diagnostic représente elle aussi une étape fondamentale pour susciter l'engagement du personnel dans la construction et le développement de la démarche à co-construire. En effet, plus la marche est grande pour atteindre les objectifs fixés, plus il est primordial de donner confiance tant à la direction qu'aux opérationnels. Cette confiance ne peut se faire pleinement si l'organisation est accablée par une mise en avant de ses points faibles. Autrement dit, les stratégies s'appuyant sur la peur ou sur la psychologie inversée, etc. demeurent contre productives.

2. Réflexion et mise en place d'ateliers : une deuxième étape fondamentale pour favoriser la gouvernance, l'implication et la sensibilisation des opérationnels

La réflexion et la mise en place d'ateliers représentent la deuxième étape de notre démarche. Les ateliers sont construits en tenant compte des différentes pratiques quant aux traitements des données (une approche par les métiers - ce qui est prescrit - et les usages - le réel). Ils permettent ainsi de donner du sens à la règle de droit, de transmettre les savoirs essentiels appliqués au groupe concerné et de libérer la parole sur les

usages. Ainsi, l'animation de l'atelier amène à une prise de conscience par les acteurs concernés et de leurs pratiques. Cette prise de conscience, lors de la sensibilisation, facilite l'appropriation des concepts clés de la protection des données par les acteurs de l'organisation et le sens donné à la règle les libère de la contrainte par une compréhension des principes qui sont proches de leurs pratiques ; inconsciemment, ils sont en partie conformes à la norme juridique (par le respect des règles relatives au secret médical) et le passage vers la mise en conformité devient beaucoup moins contraignant.

Une démarche co-construite peut faciliter l'acceptation, l'adaptation des comportements individuels, collectifs et organisationnels, l'implication, la responsabilisation et la satisfaction au travail.

Pour pallier la difficulté de prévenir le risque cyber et pour favoriser une telle dynamique du changement individuel, collectif et organisationnel, il convient de ne pas omettre d'intégrer la hiérarchie non pas pour les comptes rendus d'avancement mais bien comme un acteur à part entière. En effet, l'efficacité personnelle d'une personne peut être liée à sa perception de sa hiérarchie tout comme du degré d'implication de cette dernière (Ayache et Laroche, 2010)[3].

De plus, une hiérarchie qui suit de loin la mise en conformité perd des éléments de compréhension de la situation pour donner les moyens à ses équipes de respecter toutes les règles sans élaborer de stratégies de contournement. Si l'erreur est humaine, il ne faut pas oublier que la faute est souvent organisationnelle même dans le domaine de la sécurité numérique.

Par rapport à des enjeux sociétaux et de santé, la prévention des risques cyber peut pleinement contribuer à la satisfaction des parties prenantes des organisations notamment par le développement d'un leadership singulier enclin aux enjeux individuels, collectifs et organisationnels de son époque mais aussi futurs.

C'est ainsi que la deuxième étape de la démarche favorise au fur et à mesure de son avancée l'apparition d'une autonomisation sur le sujet du

RGPD et de la sécurité des données mais aussi la création d'une responsabilisation de la part de l'ensemble des parties prenantes. C'est d'ailleurs dans ce contexte que nous observons le développement d'un véritable leadership responsable partagé au sein de la structure mais aussi, en dehors.

3. La formalisation de la documentation RGPD : une troisième étape qui rassure et verrouille la démarche sur-mesure et co-construite

Il est humain de percevoir la formalisation de procédures, du fait de leur caractère obligatoire, comme une contrainte. Cette perception est d'autant plus forte dans les organisations autoritaires. En effet, la formalisation permet la justification de la sanction. C'est pourquoi, il appartient à la gouvernance d'établir la confiance en favorisant les organisations apprenantes et en utilisant la formalisation comme un outil d'aide à l'autonomisation des opérationnels. Le cadre, lorsqu'il est connu et compris, a le mérite d'être rassurant et de servir de pilier pour l'autonomisation et la responsabilisation du personnel. Il est essentiel que l'encadrement contribue au partage de la vision de la direction et du sens (le pourquoi de l'action) auprès de tous les acteurs internes pour que ces derniers soient en mesure d'œuvrer dans le même sens et perçoivent leurs rôles et leur utilité pour l'atteinte de l'objectif final.

Dans la conduite d'un changement tel que celui que nous avons opéré, il est important de parvenir à aider et à encourager l'ensemble des parties prenantes à dépasser leurs craintes mais aussi leurs peurs. Cela passe par exemple par le fait de valoriser leurs bonnes pratiques existantes tout comme le fait de les relier au sens de leur mission et de leur travail. Dans le monde de la santé le rapport au secret médical est un appui pour faciliter l'acceptabilité des mesures de sécurité qu'elles soient techniques ou organisationnelles. Le secret médical est un secret partagé sur lequel nous avons capitalisé. La bonne compréhension et gestion du secret médical facilitent l'appropriation des mesures de sécurité préconisées par la réglementation et participent ainsi au développement d'un sentiment de responsabilisation ; car si la sécurité des systèmes d'information est l'affaire de tous, c'est encore plus bénéfique quand chacun en devient le maillon fort !

C'est ainsi que dès lors que la réglementation et les pratiques deviennent limpides pour les parties prenantes, la demande de déploiement d'outils devient naturelle. Leur appropriation en devient ainsi plus rapide et acceptée.

Le renforcement de la fiabilité de l'organisation et la valorisation de son capital social : un résultat au-delà de l'objectif initial de mise en conformité juridique

La valorisation, par cette approche, des pratiques professionnelles génère un levier de motivation, d'implication, de satisfaction, d'engagement et de fidélisation des parties prenantes. La prise en compte de l'humain, à titre individuel et collectif, permet de donner du sens aux procédures et de retenir l'attention de ceux qui devront accepter les « contraintes ».

Au-delà de la co-construction de la démarche proposée avec la gouvernance et les opérationnels, l'enjeu, dans ce type de démarche, est de permettre le développement d'un capital humain nécessaire à l'organisation, et finalement, de le reconstruire puis de le renforcer autour d'une culture partagée de la cybersécurité. Pour le reconstruire et le renforcer, il s'agit donc de considérer que le collectif, et ainsi l'appartenance des acteurs à une même structure, doit favoriser le développement d'une certaine confiance, la circulation de l'information, tout comme le renforcement d'une vision commune. L'ensemble est entretenu à la fois par les interactions sociales mais aussi par le partage de valeurs et d'une culture organisationnelle singulière.

Dans ce prolongement, il s'agit de capitaliser sur ce que l'on nomme « le capital social » (Coleman, 1988[4]; Nahapi et Ghosal, 1998[5]; Putnam, 2000[6]) de l'organisation.

À partir de la confiance partagée entre les acteurs, qui est la base du concept du capital social, leur coopération, engagement réciproque et la cohésion sociale se solidifient. Le capital social devient ainsi un levier fondamental pour permettre, à terme, l'amélioration de la performance organisationnelle et l'accélération de la diffusion des savoir entre les personnes (OCDE, 2001[7]). Dans la mise en place d'une démarche visant

à la mise en conformité juridique d'une organisation, nous appuyons donc l'argument selon lequel la capitalisation portant sur l'association complémentaire du capital humain et du capital social favorise une adaptation et une adaptabilité efficace et rapide face aux enjeux liés à la cybersécurité tout en tenant compte de leur évolution rapide (et une facilitation de la résilience de l'organisation par un renforcement du collectif).

C'est ainsi que l'autonomisation des bonnes pratiques par les opérationnels en matière de sécurisation amplifie la sûreté des informations, et leur communication tout comme de leur verrouillage peuvent être renforcés tant en interne que vis-à-vis des partenaires externes. Les enjeux sont ainsi connus et reconnus par l'ensemble des parties prenantes internes et externes de l'organisation, ce qui peut même donner naissance au développement d'une marque employeur. Cette dernière aide à renforcer le sentiment d'appartenance, de satisfaction et de fierté de la part des équipes internes tout comme la confiance et la bonne réputation de l'organisme auprès des publics cibles.

La mise en conformité et la valorisation des pratiques pour la protection des personnes favorisent donc le développement de la confiance des publics cibles qui peuvent aussi avoir des freins quant au dépistage dans le cadre des politiques de prévention en santé publique, du fait de la peur des conséquences d'une atteinte aux données les concernant. En effet, la hausse des cyberattaques en santé amplifie une forme de déni et de peur de la divulgation, ce qui entraîne des freins au dépistage des pathologies. Or, ces peurs sont des obstacles à la prise en charge précoce et sont à l'origine de « perte de chance » de guérison pour les personnes dépistées tardivement. Toute action, dans ce secteur, en faveur de la protection des données permet une protection du secret médical et de la vie privée. Ainsi la prise de conscience des conséquences des pratiques professionnelles donne du sens aux procédures, et facilite l'adaptation des comportements des différents acteurs concernés et leur responsabilisation. La sécurité des systèmes d'information n'est donc plus seulement l'affaire de tous mais bien de la responsabilité de chacun.

[1] Ce RETEX a été repris dans le cadre du projet DRIFT-FH (Projet-ANR-21-CE39-0015) sélectionné par l'ANR dans le cadre des AAPG2021. Il est coordonné par la Fondation Saint-Cyr et réunit plusieurs partenaires (IRBA, AMSCC, Psycle, COSTECH, HEUDIASYC et IBISC). https://f-sc.org/financement-dun-projet-de-recherche-par-lanr/

[2] Bareil C. (2004), Gérer le volet humain du changement, Collection Entreprendre, Montréal, Les Editions Transcontinental Inc.

[3] Ayache M, Laroche H. (2010), « La construction de la relation managériale. Le manager face à son supérieur », Revue française de gestion, Vol.4, n°203, pp. 133-147.

[4] Coleman J.S. (1988), Social capital in the creation of human capital, American Journal of Sociology, vol.94, n°supplement, p.95-210.

[5] Nahapiet J., Ghoshal S. (1998), Social capital, intellectual capital, and the organizational advantage, The Academy of Management Review, vol.23, n°2, p.242-266.

[6] Putnam R.D. (2000), Bowling alone-The collapse and revival of American community, New York, Simon and Schuster.

[7] Organisation de Coopération et de Développement Economiques (OCDE). (2001), Du bien-être des nations : le rôle du capital humain et social, Editions de l'OCDE, p. 1-7.

La santé au cœur de la tourmente : quelles nouvelles perspectives pour sa cybersécurité, dans un secteur déjà lourdement affaibli ?

LOÏC GUÉZO
Directeur Stratégie Cybersécurité Europe
Proofpoint

Dans un paysage de la menace toujours plus oppressant, la France compte parmi les pays les plus ciblés par les cybercriminels. Et l'un des secteurs le plus pris pour cible a été celui de la santé. La vague de cyberattaques qui a touché le secteur hospitalier français et européen a pris une ampleur sans précédent en 2022 et d'après l'ANSSI (l'Agence Nationale pour la Sécurité des Systèmes d'Information), 10 % du nombre total de compromissions portées à sa connaissance concernait des établissements publics de santé, une hausse de trois points comparés à l'année précédente.
Pour un secteur quasi étranglé par la pression des cybercriminels, il apparaît donc urgent de prendre la mesure du risque cyber et d'adopter des mesures concrètes et fortes pour éviter de sombrer dans un possible chaos numérique. Mais par où commencer ? Proofpoint partage son éclairage sur ces questions et sur les actions concrètes permettant de renforcer la posture en cybersécurité, dans le secteur de la santé et plus largement dans le secteur public.

La cybercriminalité en France

Le paysage de la menace cyber en France et dans le monde est en constante évolution. Les attaques sont de plus en plus ciblées, sophistiquées, et ne connaissent certainement pas de frontières. Dans une conférence plénière[1] organisée au Campus Cyber de La Défense à Paris en novembre dernier, le général de division Marc Boget, chef du ComCyberGend (Commandement de la gendarmerie dans le cyberespace), insistait sur

l'ampleur de la menace à laquelle nos sociétés font désormais face, rappelant que le coût de la cyberdélinquance s'élevait approximativement entre 6 et 7 milliards d'euros par an, et que l'on pouvait observer une nouvelle attaque de rançongiciels toutes les 11 secondes dans le monde.

La menace s'est en effet déplacée des infrastructures vers l'utilisateur.

Le courriel est le premier vecteur d'entrée des cybercriminels (91 % des cyberattaques utilisent l'email selon l'étude Data Breach Investigations report 2019 de Verizon), et leurs stratégies se basent sur des techniques d'ingénierie sociale[2] extrêmement précises, qui jouent sur des mécanismes psychologiques et inconscients, comme la peur, l'urgence, ou l'empathie, pour que la victime ouvre un courriel malveillant, clique sur un lien frauduleux ou télécharge une pièce jointe infectée, ouvrant ainsi la porte aux cybercriminels.

Par les recherches que Proofpoint mène à travers le monde pour remonter la piste des cybercriminels, nous avons pu observer que, si nous sommes bien de plus en plus formés à identifier les courriels frauduleux, les cybercriminels eux, redoublent d'ingéniosité pour nous leurrer. Ces acteurs de la menace établissent un lien de confiance avec leurs victimes en tenant des conversations prolongées ; ils s'appuient sur l'utilisation de services d'entreprises de premier plan, prennent de nouvelles voies, usurpent l'identité de marques connues (comme Microsoft) ou de votre PDG, et pénètrent ainsi dans votre intimité numérique en allant jusqu'à utiliser des fils de conversation déjà existants pour vous tromper.

Ces groupes exploitent évidemment régulièrement notre crainte ou notre curiosité via des références aux thèmes d'actualité, tels que la pandémie de Covid, la guerre en Ukraine[3] et l'appel aux dons pour les réfugiés, ou encore les grands évènements sportifs. À cet instant, les JO 2024 deviennent précisément la nouvelle préoccupation majeure pour les experts de la cybersécurité française.

Dans son rapport sur le Panorama de la menace[4], l'ANSSI aussi note un changement de thématique intéressant dans les campagnes

d'hameçonnage observé. Il ressort ainsi des signalements effectués à l'ANSSI que la thématique des impôts [largement utilisée les années précédentes] est progressivement remplacée par celle de la santé, en usurpant notamment l'identité de l'Assurance Maladie. Les attaquants cherchent ainsi à exploiter le contexte sanitaire et l'actualité liée à la création de « Mon espace santé ».

Les cybercriminels sont majoritairement animés par l'appât du gain, et ils n'hésitent pas pour autant à cibler les établissements de santé subventionnés par les fonds publics, avec peu de moyens (et donc de suffisamment d'expertise allouée à la protection de systèmes hébergeant données personnelles, et sensibles, de premier choix). Exception notable : quand il s'agit d'enfants, où là semble être la limite de leur inhumanité. Récemment le groupe Lockbit a en effet présenté ses excuses[5] après une cyberattaque contre un hôpital pour enfants de Toronto le 18 décembre 2022, et proposé un outil à l'hôpital afin que l'établissement puisse récupérer toutes les données bloquées par l'utilisation d'un de ses logiciels malveillants.

Le secteur de la santé au cœur de la tourmente ?

La vague de cyberattaques qui a touché le secteur hospitalier français a pris une ampleur sans précédent en 2022. Dans son Panorama de la cybercriminalité (Panocrim) de début d'année2023, le Clusif[6] a fait un point sur la menace rançongiciels, à partir de l'analyse de 623 incidents publics survenus au premier trimestre 2022. Conti et LockBit sont les deux qui auraient causé, et de loin, le plus d'incidents. Concernant les outils exploités pour les déployer, le Clusif mentionne BazarLoader, TrickBot, GoziAT et systembc RAT.

Après différentes attaques en début d'année 2022, l'été 2022 a vu une attaque d'une fulgurance extrême, mettant quasiment hors service le Centre Hospitalier Sud Francilien (CHSF)[7] de Corbeil-Essonnes ; tous les logiciels métiers de l'hôpital, les systèmes de stockage (notamment d'imagerie médicale) et le système d'information ayant trait aux admissions de la patientèle étaient alors inaccessibles. Alors que l'Agence Régionale de Santé (ARS) d'Île-de-France déclenchait son plan blanc, le

GIGN aurait même été à la manœuvre pour des négociations avec les cybercriminels derrière le ransomware Lockbit 3.0 ; les demandes initiales de rançons se seraient élevées à dix millions d'euros, somme que les négociateurs du GIGN seraient parvenus à abaisser à 1 million[8]. Le système informatique de l'hôpital a été paralysé pendant deux mois et, le 23 septembre 2022, 11 giga-octets de données exfiltrées lors de la compromission ont été publiés sur le site web du groupe cybercriminel (selon un rapport de l'ANSSI[9]). Parmi les éléments divulgués figuraient notamment des données médicales et personnelles liées aux patients et au personnel hospitalier. Une situation similaire s'est répétée quelques mois plus tard au Centre Hospitalier de Versailles.

En décembre 2022, le journal Numerama[10] notait qu'à Corbeil-Essonnes, « la situation a été si dégradée que le coût total pour un retour à la normale est estimé à deux millions d'euros, soit le double de la rançon demandée par les malfaiteurs pour débloquer les données. » Un rapport du Ponemon Institute[11], l'un des principaux organismes de recherche en sécurité informatique, a en effet établi que le coût moyen des cyberattaques les plus onéreuses ayant touché le secteur de la santé s'établit à 4,4 millions de dollars, dont 1 million en perte directe de productivité. Par ailleurs, plus de 20 % des établissements de santé qui ont été victimes de cyberattaques ont ensuite connu une augmentation du taux de mortalité de leurs patients, et plus de la moitié ont vu une détérioration de la qualité des soins apportés au quotidien.

Numerama recense plus d'une dizaine d'attaques avérées au cours de l'année 2022 :

- Clinique Léonard de Vinci de Chambray-les-Tours : attaque par ransomware le 7 janvier. Les malfaiteurs ont demandé 500 000 euros de rançons[12].
- Cité sanitaire de Saint-Nazaire : attaquée le 12 janvier, les patients sont privés de télévision, d'Internet et de communication avec leurs proches[13].
- Hôpital de Castelluccio, Ajaccio : touché par un ransomware le 28 mars, les soins de radiologie et oncologie étaient suspendus.
- L'hôpital de Saint-Dizier et de Vitry-le-François : victimes d'un

ransomware le 19 avril. Les auteurs exigeaient une rançon de 1,2 million d'euros.
- Centre hospitalier de Mâcon : touché le 27 mai.
- Centre hospitalier de Corbeil-Essonnes : attaque par ransomware le 20 août, revendiquée par Lockbit. Demande de rançon de 1 million d'euros.
- Hôpital de Cahors : cyberattaque le 12 septembre.
- Maternité des Bluets, Paris XIIIe : touchée par un ransomware le 9 octobre, revendiqué par Vice Society.
- Hôpital André-Mignot, Versailles : attaque par ransomware le 3 décembre.
- Centre hospitalier d'Argenteuil (déjoué) : tentative d'intrusion début décembre.
- CHU Nice (déjoué) : touché le 3 décembre, le pare-feu a bloqué l'opération.

Si les responsables de la sécurité des systèmes informatiques (RSSI) dans le secteur de la santé sont extrêmement conscients du risque de cyberattaque contre leur système (sondage Proofpoint[14], mai 2022), ils considèrent que la plus grande vulnérabilité de leur organisation vient de leurs collaborateurs, qui en retour ne se rendent absolument pas compte du rôle actif qu'ils ont à jouer dans la protection de leur organisation.

Le risque est pourtant immense, d'autant que les cybercriminels continuent de développer des techniques de plus en plus ciblées et sophistiquées pour leurrer leurs victimes et pénétrer les systèmes d'information critiques, pour non seulement chiffrer les données sensibles et exiger rançon contre clé de déchiffrement, mais aussi menacer de rendre publiques ou revendre ces données sur le marché noir[15], une technique dite de « double extorsion » qui pose de nouveaux problèmes à terme : n'est-il pas plus impactant (et donc rémunérateur) pour un criminel de faire un chantage à la divulgation de données sensibles, par nature plus difficiles à gérer que simplement bloquer un système, dont le redémarrage dépend finalement et essentiellement du niveau de préparation et d'anticipation de la victime ?

Évolution de la menace cyber : le rançongiciel en déclin ?

Si le dernier Panorama de la menace[16] de l'ANSSI note un léger recul du nombre d'attaques par rançongiciels portées à sa connaissance (209 en 2021 contre 103 en 2022), il démontre en revanche que les organisations du secteur public sont une cible de plus en plus privilégiée par les cybercriminels. Le rapport souligne aussi que les acteurs de la menace s'attaquent de plus en plus aux infrastructures critiques telles que les hôpitaux, de par les raisons évoquées plus haut. La cybersécurité est un sujet nouveau pour beaucoup d'organisations et surtout dans la santé, un secteur jusqu'ici peu confronté à cette nouvelle réalité, qui manque d'expertise au sein de son organisation et dont les moyens dédiés à sa protection sont plus faibles comparés à des entreprises du secteur privé ; sa priorité étant évidemment ailleurs, et ses moyens financiers principalement dédiés à l'équipement des professionnels de santé et aux soins prodigués aux patients.

Dans son rapport[17] annuel sur l'état du phishing dans le monde, Proofpoint montre aussi qu'en France, si 65 % des entreprises interrogées déclarent avoir été confrontées à une tentative d'attaque par rançongiciel au cours de l'année passée, avec infection réussie dans 66 % des cas, seules 53 % d'entre elles disent s'être acquittées de la rançon pour récupérer leurs données, une tendance à contrecourant du reste du monde où la propension à payer aurait augmenté de 6 points depuis 2021.

Le rançongiciel serait donc de moins en moins lucratif, d'autant que les entreprises françaises se montrent de plus en plus résilientes face à la menace : ainsi cette année, le CLUSIF a pu montrer lors de son Panorama Annuel de la Cybercriminalité que des hôpitaux comme Nice et Argenteuil ou des collectivités comme Redon avaient pu stopper dès leurs prémices des attaques par rançongiciel.

En réaction peut-être, les criminels se concentrent maintenant sur d'autres techniques pour escroquer leurs victimes, basées sur l'usurpation d'identité et la compromission de courriel professionnel (BEC), une approche qui en France, a augmenté de 5 points par rapport à 2021 et 80 % des organisations interrogées par Proofpoint ont signalé au moins une

tentative d'attaque BEC l'année dernière, un chiffre supérieur à la moyenne mondiale.

Le terme BEC (pour Business Email Compromise) est peu connu, comparé à des termes comme Phishing ou Rançongiciel. Pourtant, il est responsable de presque la moitié de toutes les pertes financières liées à la cybercriminalité. Les attaques BEC sont incroyablement difficiles à détecter et à éviter, du fait de leur nature. Elles sont conçues pour se fondre dans la masse et ne comportent souvent pas les caractéristiques traditionnelles que sont les URL et les charges utiles malveillantes. Au lieu de cela, les BEC s'appuient sur un réseau complexe de techniques d'usurpation d'identité et d'ingénierie sociale pour tromper les utilisateurs. Dans la plupart des cas, un cybercriminel se fait passer pour une personne ou une entité de confiance, qu'il s'agisse d'un collègue, d'un fournisseur ou même d'un directeur. Après s'être fait reconnaître en tant que cette personne de confiance, l'attaquant envoie ensuite un courriel demandant à la victime d'effectuer une action spécifique, par exemple modifier les coordonnées bancaires d'une facture ou effectuer un virement.

D'autre part, au cours de l'année écoulée, une nouvelle forme de menace s'est aussi imposée ; à son point le plus haut, Proofpoint a suivi plus de 600 000 attaques TOAD par jour[18], un chiffre qui n'a cessé d'augmenter depuis la première mise en application détectée fin 2021.

Les TOAD [pour « Telephone Oriented Attack Delivery »] sont des techniques de « vishing » [contraction de « voice » et « phishing »] et signifie en français hameçonnage par la voix. L'attaque commence par l'envoi d'un faux SMS[19] ou d'un courriel frauduleux, en France dans bien des cas, ces messages alertent sur une activité bancaire suspecte, ou sur l'urgence de mettre à jour son compte de santé Améli pour renouveler une Carte Vitale (qui en réalité n'expire jamais).

Après le téléphone et la voix, c'est désormais la vidéo qui est utilisée… En mars dernier par exemple, la Threat Team de Proofpoint, alertait sur les dernières campagnes de l'acteur de la menace TA499[20], également connu sous les noms de Vovan et Lexus, deux as du canular téléphonique, passés maîtres dans l'art de l'imitation et du maquillage, quand ils n'ont pas

recours à des sosies et au « deep fake », le trucage numérique permettant de remplacer un visage grâce à l'intelligence artificielle (AI). Le duo aurait réussi à piéger des dizaines de personnalités mondiales, de l'ex-premier ministre britannique Boris Johnson à la star Elton John, en passant par l'ex-chancelière Angela Merkel et le président turc Recep Tayyip Erdogan et tout récemment le président François Hollande[21]. Les activités de ce groupe affilié à la Russie se sont intensifiées depuis le début de la guerre en Ukraine, avec plusieurs campagnes de mailing soutenant la propagande pro-russe et visant les gouvernements et personnalités qui auraient pris la parole contre les agissements du président Vladimir Poutine.

Les données des patients valent de l'or pour les cybercriminels

Pourquoi les données de santé sont-elles tant recherchées par les cybercriminels ? Plusieurs raisons expliquent l'importance de ces données à leurs yeux.

Tout d'abord, les données de santé sont particulièrement précises sur les individus, et ne peuvent pas être modifiées. Par exemple, un numéro de sécurité sociale ainsi que le poids, la taille, le groupe sanguin sont tout autant de données qui sont propres aux personnes, contrairement à une donnée bancaire comme un numéro de carte de paiement qui peut être modifiée quasi instantanément. Une fois qu'elles sont identifiées, elles restent, ce qui apporte une valeur non négligeable à ces données.

De plus, la monétisation de ces données est plus aisée. De nombreuses personnes sont prêtes à payer pour protéger des informations aussi personnelles et non modifiables, si elles venaient à fuiter. Par ailleurs, les données de recherches cliniques ou de travaux innovants de R&D ont évidemment une valeur pécuniaire non négligeable : ces données correspondent à des semaines, voire des mois ou des années de recherche par des scientifiques qualifiés. Ces données peuvent être revendues à des organismes privés concurrents peu éthiques, pour des sommes considérables ou être récupérées à des fins d'espionnage étatique[22].

Enfin, la tristement connue fuite de photos dénudées de patients malades

de cancer opérée par BlackCat illustre l'ampleur que peut prendre une fuite de ce type de données[23]. Les conséquences sur les victimes peuvent être terribles, d'autant plus qu'elles n'ont eu à aucun moment le contrôle sur ces photos.

Quelles perspectives pour le secteur de la santé ?

En ce qui concerne le secteur de la santé, comme pour beaucoup d'autres secteurs, des mesures élémentaires restent à prendre. Des mesures essentielles, telles que la mise en place d'une authentification DMARC (Domain Message Authentication Reporting and Conformance) sur les courriels, permettront aux hôpitaux d'avoir une cyber hygiène beaucoup plus poussée. De plus, la loi évolue, avec la prochaine mise en place de la directive NIS 2, qui poussera les organisations à renforcer leur posture cyber. Qu'elle soit choisie ou contrainte légalement, l'amélioration de la posture de cybersécurité ne peut qu'affecter en bien le fonctionnement des hôpitaux. Les soins apportés aux patients ne doivent pas dépendre d'une cyberattaque, et seule l'amélioration du niveau de cybersécurité pourra l'assurer. Les cybercriminels ne sont malheureusement pas prêts d'arrêter leurs activités.

Mais il reste encore beaucoup à faire ! En septembre 2022, Proofpoint a réalisé une analyse de la protection DMARC de l'ensemble des 30 centres hospitaliers universitaires (CHU) français[24]. Le protocole d'authentification DMARC a été conçu pour empêcher les pirates informatiques d'usurper l'identité d'une organisation et de son domaine, en rejetant tous les messages non authentifiés. Fortement recommandé par l'ANSSI, ce protocole permet ainsi de combattre spam, phishing et fraudes par courriels, menaces les plus virulentes à l'échelle mondiale. Les résultats montrent que la moitié des CHU en France ne dispose d'aucun niveau d'authentification requis pour protéger les usagers contre la fraude par email. Parmi ceux ayant publié un enregistrement DMARC, onze ont une protection des plus sommaires, et seulement trois ont un système de mise en quarantaine des courriels douteux. Enfin, un seul CHU parmi les 30 étudiés a mis en place un rejet automatique des courriels suspicieux, la protection DMARC la plus haute qui permet de combattre de façon proactive toutes tentatives d'hameçonnage.

D'un point de vue législatif, la directive NIS 2 adoptée en novembre dernier par le Parlement européen pour consolider la posture cyber des infrastructures essentielles comme la santé, annonce de grands chantiers pour les entreprises de tous les états membres, qui ont maintenant jusqu'à 2024 pour la transposer le texte dans leur législation et le mettre en application sur leur territoire.

Face à l'évolution de la menace, NIS 2 vise à renforcer la résilience des organisations, en particulier l'hygiène informatique de base, la formation à la cybersécurité, les politiques de contrôle d'accès et la gestion des actifs, les procédures de réponse aux incidents et la gestion des crises, la gestion et la divulgation des vulnérabilités, et l'évaluation des mesures de gestion des risques de cybersécurité. Jusqu'à présent, seuls les acteurs de l'énergie, des transports, les banques et institutions financières, la santé, les réseaux d'eau et certaines infrastructures numériques étaient concernés. Le périmètre est désormais élargi à près de 600 types d'entités différentes, dont les administrations publiques et des entreprises allant des PME aux groupes du CAC 40.

La bonne nouvelle est que plus des deux tiers des membres des conseils d'administration français considèrent déjà la cybersécurité comme une priorité absolue. Cependant, cette convergence théorique ne se traduit pas toujours par une action concertée dans la pratique. Si la France est le pays où conseils d'administration et les RSSI sont les mieux alignés (sondage Proofpoint[25], octobre 2022), il reste tout de même un certain chemin à parcourir pour atteindre un niveau de discussion structuré, efficace et approfondi.

Le problème est similaire en ce qui concerne le risque humain. Plus des trois quarts (76 %) pensent que leurs employés comprennent leur rôle dans la protection contre les menaces, mais un peu plus (78 %) affirment que l'erreur humaine est leur plus grande vulnérabilité cybernétique. Il existe donc un fossé entre la compréhension des menaces modernes et la capacité à les tenir à distance. Les méthodes traditionnelles ne sont pas bien comprises et plus d'un tiers des personnes interrogées en France par Proofpoint ne savent pas définir les termes de « logiciel malveillant » (malware), « hameçonnage » (phishing) et « rançongiciel » (ransomware).

Par ailleurs, si 54 % des organisations françaises se sont dotées d'un programme de sensibilisation à la sécurité qui forme l'ensemble de leurs collaborateurs, seulement 30 % effectuent des simulations d'attaque d'hameçonnage ciblées, deux éléments pourtant essentiels à la mise en place d'un programme efficace de sensibilisation à la cybersécurité.

En conclusion, RSSI et conseils d'administration doivent maintenant réellement travailler en étroite collaboration pour faire avancer le sujet et transformer la bonne volonté en action, en créant une culture de la cybersécurité adaptée aux exigences du paysage actuel des menaces. Toutes les parties prenantes et notamment les personnels administratifs et soignants doivent donc apprendre à reconnaître ces menaces et à y répondre pour réduire la probabilité d'une compromission d'établissement.

La sensibilisation et la formation des équipes de façon régulière et à tous les niveaux restent les atouts les plus solides pour faire face à cette problématique mouvante et souvent dévastatrice pour l'organisation touchée par une attaque au cœur de ses systèmes de données. Repasser au papier et au crayon pour soigner dans la tempête a parfois été nécessaire et les hôpitaux ont montré leur résilience, mais il ne faut pas perdre de vue que dans la santé, les dommages collatéraux iront potentiellement jusqu'à la vie des patients.

[1] https://www.proofpoint.com/fr/blog/corporate-news/proofpoint-collabore-avec-la-frenchtech-cyber-pour-faire-front-contre-la-menace
[2] https://www.proofpoint.com/fr/resources/threat-reports/2022-social-engineering-report
[3] https://www.proofpoint.com/us/blog/threat-insight/good-bad-and-web-bug-ta416-increases-operational-tempo-against-european
[4] https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-001/
[5] https://www.ouest-france.fr/monde/canada/canada-une-cyberattaque-vise-un-hopital-pour-enfants-des-pirates-presentent-leurs-excuses-bf3dde76-8ab6-11ed-9f02-83dfd627f7a1#:~:text=Apr%C3%A8s%20une%20cyberattaque%20contre%20un,un%20de%20ses%20logiciels%20malveillants.
[6] https://clusif.fr/
[7] https://www.iledefrance.ars.sante.fr/cyber-attaque-au-centre-hospitalier-sud-francilien-chsf-lars-ile-de-france-coordonne-la-continuite
[8] https://www.lemagit.fr/actualites/252525365/Hopital-de-Corbeil-Essonnes-une-discussion-inhabituelle-sans-negociation-perceptible
[9] https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-001/
[10] https://www.numerama.com/cyberguerre/1219264-cyberattaque-la-liste-des-hopitaux-touches-en-2022.html
[11] https://www.proofpoint.com/fr/resources/threat-reports/cost-of-insider-threats
[12] https://www.lejsl.com/sante/2022/05/30/le-centre-hospitalier-victime-d-une-cyberattaque
[13] https://www.saintnazairenews.fr/news/cite-sanitaire-de-saint-nazaire-une-cyberattaque-vise-les-tvs-telephones-et-le-wifi
[14] https://www.proofpoint.com/fr/resources/white-papers/voice-of-the-ciso-report
[15] https://www.bfmtv.com/tech/cybersecurite/des-pirates-diffusent-des-radiographies-de-patientes-atteintes-d-un-cancer-du-sein-pour-obtenir-une-rancon_AV-202303100472.html
[16] https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-001/
[17] https://www.proofpoint.com/fr/resources/threat-reports/state-of-phish
[18] https://www.proofpoint.com/fr/resources/threat-reports/state-of-phish
[19] https://www.zdnet.fr/actualites/les-metamorphoses-du-phishing-39950868.htm
[20] https://www.proofpoint.com/us/blog/threat-insight/dont-answer-russia-aligned-ta499-beleaguers-targets-video-call-requests
[21] https://www.huffingtonpost.fr/international/article/guerre-en-ukraine-francois-hollande-piege-par-vovan-et-lexus-deux-humoristes-russes_216326.html
[22] https://www.brighttalk.com/webcast/13513/562166?utm_source=brighttalk-portal&utm_medium=web&utm_campaign=topic&utm_content=upcoming
[23] https://www.bfmtv.com/tech/cybersecurite/des-pirates-diffusent-des-radiographies-de-patientes-atteintes-d-un-cancer-du-sein-pour-obtenir-une-rancon_AV-202303100472.html
[24] https://www.proofpoint.com/fr/blog/email-and-cloud-threats/cybercriminalite-quand-le-secteur-de-la-sante-se-retrouve-mal-en-point
[25] https://www.proofpoint.com/fr/resources/white-papers/board-perspective-report

Cybersécurité : Terra Incognita ?

PHILIPPE LOUDENOT
Cyber Security Strategist - BlueFiles
Senior Advisor - CyberCercle

« Les hommes n'acceptent le changement que dans la nécessité et ne voient la nécessité que dans la crise ». Cette maxime d'un des pères de la construction européenne, Jean Monnet, se mesure tous les jours sur différents sujets. En matière numérique, les différents incidents révélés qui émaillent depuis ces dernières années les médias, démontrent régulièrement que la cyber sécurité n'est finalement prise en compte qu'à l'issue d'une crise pouvant être majeure.

Le numérique connaît un essor prodigieux avec le développement des objets connectés et les nouvelles méthodes de travail s'appuyant sur la dématérialisation progressive. De ce fait, les risques liés au numérique sont passés en quelques années, d'une dimension quasi anecdotique à une menace multiple, structurée et organisée, pouvant provoquer des dégâts considérables tout aussi multiple (techniques, image de marque, juridiques et financiers notamment) pouvant conduire jusqu'à mettre en jeu la vie de personnes. C'est très inquiétant.

Au-delà de faire peur en agitant le « spectre » de la menace, le point positif est que l'on sait comment traiter ces risques. Mais encore faut-il le faire et pour cela il est essentiel de faire prendre conscience de ces risques afin de pouvoir les anticiper, se protéger et, le cas échéant, rebondir.
Le secteur de la santé semble prédisposé à la compréhension de cette problématique dont l'approche est, à priori, similaire. En effet, le numérique peut s'identifier au monde de la santé, à tel point que de nombreux termes ou concepts lui sont empruntés. Malheureusement, en matière de sécurité numérique, à l'instar de la santé, les problèmes ne sont encore que trop souvent vus dans l'urgence et le curatif. Pour preuve, en médecine, on admire bien plus un chirurgien capable d'un exploit

médiatique qu'un Ignace Philippe Semmelweis, médecin obstétricien hongrois qui œuvra pour l'hygiène. Il démontra l'utilité du lavage des mains après la dissection d'un cadavre avant d'effectuer un accouchement. Ses travaux permettant de faire du préventif ont malheureusement mis des années avant d'être adoptés. En médecine, son cas est régulièrement cité en exemple d'une situation où le progrès a été freiné par l'inertie bien en place. En matière de sécurité numérique, l'hygiène doit être de mise et comme en santé, le préventif est moins coûteux que le curatif.

En santé, comme dans la quasi-totalité des secteurs d'activités, l'avènement du « tsunami numérique » est un fait constaté tous les jours. Source de progrès et d'augmentation de chances de guérison voire de survie pour les patients (et nous en sommes tous, avérés ou en devenir), il est cependant impossible d'éviter le débat sur les dépendances créées par les technologies numériques. Le numérique est partout et même là où il n'était pas attendu : outre les systèmes d'information hospitaliers « métiers » au profit des professionnels de santé et des patients et les systèmes d'information administratifs (gestion RH, financière…), ils sont présents dans les dispositifs biomédicaux, les systèmes de gestion technique centralisée (GTC) ou de bâtiment (GTB) et… l'ensemble des objets connectés dont certains implantés chez les patients.

Ces différentes composantes, aujourd'hui, peu ou prou interconnectées et de plus en plus ouvertes, disposant chacune de leur propre historique et d'architecture particulière, posent la problématique de la maîtrise des processus et de leurs informations et donc, in fine, de la prise en compte de la sécurité numérique.

L'évolution des traitements de l'information, la mise en place de convergences technologiques (ordinateurs, réseaux, protocoles d'échanges, appareils biomédicaux) font des systèmes d'information numériques autant de cibles individuelles. Incidents et attaques sont régulièrement déclarés. Elles peuvent être lancées par des individus, des groupes d'individus, guidés par l'appât du gain mais aussi résulter d'actions plus stratégiques menées par des États ou de grandes organisations afin de déstabiliser un pays. Enfin, il convient de ne pas oublier les nombreux incidents ou attaques liés aux mésusages, non respect des procédures, manque de sensibilisation... à l'humain !

Par chance, aucun incident d'ampleur équivalente à ce qui est arrivé en 2017 en Angleterre - avec l'arrêt d'activités pendant plusieurs jours d'établissements de santé et l'évacuation d'une partie de leurs patients - n'est arrivé chez nous. D'où, la question, devenue « marronnier » du cyber : « ce n'est pas de savoir si mais quand arrivera l'incident ? ».

Nous pouvons compléter cette question par les 4 « Comment ? ».

Comment :
• Se protéger ?
• Se défendre ?
• S'assurer de la continuité des missions ?
• Se reconstruire ?

À l'heure de l'interconnexion globale des réseaux de communication, de la convergence numérique et de l'accroissement exponentiel de la puissance des moyens techniques utilisés, chacun est confronté à des changements rapides, porteurs de nouvelles opportunités et en conséquence, porteur de nouveaux risques qu'il est de plus en plus difficile de percevoir. Dans un monde numérique banalisé et en constante évolution, la sécurité numérique reste un concept difficilement assimilé et accepté par tous. Il est désormais impératif de bien comprendre qu'il ne s'agit pas que d'une question technique. Les enjeux de la sécurité numérique représentent un défi majeur dans des environnements aux technologies en constante évolution. Quel que soit le secteur d'activité, il est essentiel de mettre en place une véritable gouvernance de la sécurité adaptée à la culture de l'organisation, capable de fédérer l'ensemble des actions. La sécurité ne peut pas être considérée comme une pratique à part : elle doit s'appuyer sur la gouvernance globale et s'intégrer dans la stratégie de l'organisation.

Malheureusement, il peut être regretté l'utilisation du préfixe « cyber » aujourd'hui décliné à toutes les sauces : cyberpirate, cyberdélinquance, cyberattaque… autant de néologismes, dont le mot « cybersécurité » qui a totalement envahi nos espaces. Nous pourrions ainsi ajouter la cybernaïveté, le cyberjem'enfoutisme ou le cyberAlzheimer. Avec le terme de cybersécurité, mis à part une vague idée de protection sur les réseaux

informatiques contre des pirates venus de tous les coins, sait-on ce qu'il englobe exactement ? Cette utilisation n'altère-t-elle pas la vision que l'on devrait en avoir ? Aujourd'hui, la sécurité numérique est encore trop vite et trop souvent instrumentalisée, considérant que cela n'est qu'un problème technique et une question de déploiement de solutions. Si dans un contexte numérique exponentiel, multipliant les interconnexions, il faut bien sûr se protéger des agressions extérieures par des moyens techniques, il nous faut également revenir aux fondamentaux et ne pas oublier certaines bases.

En feuilletant d'ancien cours dispensés par le SCSSI et la DCSSI (ancêtres de l'actuelle ANSSI), la protection des systèmes d'informations que l'on réduit aujourd'hui à la sécurité numérique était mise en avant, quel que soit le type de menaces, avec différents exemples expliquant que depuis la nuit des temps, les hommes ont éprouvé le besoin de protéger certaines informations. En reprenant comme base la gestion des risques, la sécurité numérique permet de ne pas rester centrer exclusivement sur les menaces ni les vulnérabilités mais bien sur les impacts qui concernent au final les métiers, et ne pas oublier qu'elle repose sur trois piliers ; Disponibilité, Intégrité et Confidentialité auxquels il est possible d'ajouter Traçabilité ou Preuve (critères DICT).

L'un des critères les plus essentiels et les plus surveillés en santé concerne la confidentialité. Pourtant, en données de santé, différentes informations sensibles sont encore envoyées ou reçues sans protection. Un défaut d'intégrité de données médicales peut être catastrophique pour un patient. Pour rappel, l'intégrité, consiste à s'assurer que les données n'ont pas été falsifiées et qu'elles sont donc correctes. Enfin les systèmes, les applications et les données ont peu de valeur pour un professionnel de santé et ses patients s'ils ne sont pas disponibles lorsque les utilisateurs autorisés en ont besoin.

Bien évidemment, l'analyse de risques reposant sur ces critères DICT, se construit sur la base des besoins « métier ». À titre d'exemple, la perception « métier » entre un psychiatre et un urgentiste concernant la disponibilité, l'intégrité et la confidentialité n'est pas la même.
Mettre en œuvre une gouvernance de la sécurité numérique de façon

performante et peu coûteuse est possible ! Cela permet de réellement commencer par faire du préventif plutôt que du curatif en limitant les surcoûts directs ou indirects - et de très loin supérieurs - induits obligatoirement par tout incident numérique. La meilleure façon de se protéger et de se préparer à gérer un incident consiste à adopter un processus de gestion des risques dans une démarche d'amélioration continue en prenant en considération les vrais besoins en matière de sécurité : ceux des métiers. Cette approche reste la mieux adaptée aux besoins réels, la plus efficace et la moins chère.

En conclusion, les termes de gestion des risques liés au numérique, de sécurité des Systèmes d'Information et de confiance numérique, régulièrement abordés, sont étroitement liés. Le premier est une démarche pour appréhender les risques auxquels l'organisation est exposée via ses systèmes numériques. Le deuxième se rapproche des moyens mis en œuvre pour défendre le patrimoine informationnel de l'organisation qui n'est pas exclusivement numérique. Le dernier doit permettre à l'organisation de tirer parti de la chaîne de valeur liée aux dispositifs mis en place pour assurer la confiance.

La « cyber sécurité » ou devrait-on dire aujourd'hui la « sécurité et confiance numériques » doit être au cœur de la stratégie des entreprises en prenant soin de bien objectiver ses principaux enjeux qui concernent :

- Le contenu : protéger ses données et/ou celles qui sont confiées, sécuriser les transferts, sauvegarder ses documents et toutes ses données numériques…
- Le contenant : protéger ses infrastructures du piratage externe ou interne, prévenir du mésusage…

afin de faciliter la coopération entre acteurs professionnels de santé et patients/familles/accompagnants, inter-structures, public et privé, en confiance.

Une telle mise en œuvre permet de faire de la sécurité numérique une véritable source de création de valeur et non d'être identifiée comme une contrainte légitime et pesante avec pour objectif de satisfaire les exigences d'une direction. Elle permet aussi d'expliquer simplement, pour tout type d'organisation et à l'ensemble des acteurs les risques et les enjeux à traiter

afin de concilier les visions, d'harmoniser les actions, d'évaluer et contrôler ces dernières.

La gouvernance est le prérequis pour assurer une sécurité efficiente des systèmes d'information dans le domaine de la santé. Si cela est mis en œuvre, si l'intégration de la sécurité est intégrée dès les phases de réflexion et à haut niveau pour conduire la transformation numérique, des entreprises comme des organismes publics de santé, les directions s'apercevront rapidement que la sécurité, loin d'être un centre de coût, est un véritable levier de performance.

Si depuis quelques années, la sécurité numérique prend une part croissante dans nos vies professionnelles et personnelles (le règlement général sur la protection des données (RGPD) par exemple, n'est rien d'autre qu'une application de la sécurité numérique dans nos vies quotidiennes), elle ne peut que poursuivre sa progression sous l'effet de notre dépendance croissante au numérique. Les recherches sur les big data et les IA renforceront le besoin de protection des données et la sécurité de ces données. En effet, l'apprentissage automatique et la capacité de traitement constituent un atout de développement important tout en impliquant un espace supplémentaire à sécuriser.

NIS V2, suffit-il de légiférer pour augmenter le niveau de maturité cyber d'un secteur ?

FABIEN MALBRANQUE
RSSI
Health Data Hub

Confucius écrivait en 520 avant J-C « *Celui qui déplace la montagne, c'est celui qui commence à enlever les petites pierres* ». S'agissant de la cybersécurité, la directive NIS rédigée à partir de 2013, adoptée le 6 juillet 2016 par l'UE, transposée en France le 27 février 2018 rendue applicable par décret le 25 mai 2018 semble faire partie des premières pierres. Quel bilan pour le secteur santé après ces quatre années de travail avant que le coup d'accélérateur ne soit donné avec la transposition française de NIS V2 attendue pour 2024 ?

Le principe de réalité, celui du terrain, a-t-il été oublié ?

État des lieux légaux

La directive sur la sécurité des réseaux et de l'information (NIS) est le premier texte législatif européen sur la cybersécurité. Son objectif spécifique, pour tous les États membres, était d'atteindre un niveau commun élevé de cybersécurité pour les opérateurs tributaires des réseaux ou systèmes d'information qui fournissent un service essentiel dont l'interruption aurait un impact significatif sur le fonctionnement des économies ou des sociétés…

Trois critères sont considérés :

- Ce service est essentiel au maintien d'activités sociétales ou économiques critiques ;

- La fourniture de ce service est tributaire des réseaux et des systèmes d'information ;
- Un incident sur ces réseaux et systèmes aurait un effet disruptif important sur la fourniture dudit service.

Bien qu'elle ait renforcé les capacités des États membres en matière de cybersécurité, sa mise en œuvre s'est avérée difficile.

Une nouvelle proposition, NIS V2, s'appuie sur les acquis de la directive NIS 1 et renforce les exigences en matière de sécurité, vise à assurer la sécurité des chaînes d'approvisionnement, à rationaliser les obligations de déclaration, à introduire des mesures de surveillance et des exigences d'application plus strictes, en introduisant des sanctions harmonisées dans l'ensemble de l'Union européenne.

Par ailleurs, une extension sans précédent du périmètre des structures impactées est proposée par le champ d'application de NIS2 (Directive (EU) 2022/2555, 14 December 2022[1]), en désignant davantage d'entités et de secteurs cibles de la mise en œuvre des règles induites par la directive.

L'objectif est louable, il s'agit d'accroître le niveau de cybersécurité en Europe à long terme.

La commission européenne a adopté son rapport le 28 octobre 2021, tandis que le Conseil a arrêté sa position le 3 décembre 2021. Les co-législateurs sont parvenus à un accord provisoire sur le texte le 13 mai 2022. L'accord politique a été formellement adopté par le Parlement puis par le Conseil en novembre 2022. Il est entré en vigueur le 16 janvier 2023 et les États membres disposent désormais de 21 mois, soit jusqu'au 17 octobre 2024, pour transposer ses mesures en droit national. Les fiches « Législation de l'UE en cours » sont mises à jour à des étapes clés de la procédure législative.
Au plus tard le 17 avril 2025, les États membres établissent une liste des entités essentielles et importantes ainsi que des entités fournissant des services d'enregistrement de noms de domaine. Les États membres réexaminent et, le cas échéant, mettent à jour cette liste régulièrement et, par la suite, au moins tous les deux ans.

Au plus tard le 17 avril 2025, puis tous les deux ans, les autorités compétentes notifient à la Commission et au groupe de coopération le nombre d'entités essentielles et importantes pour chaque secteur.
Au plus tard le 17 octobre 2027, puis tous les 36 mois, la Commission examine le fonctionnement de la présente directive et fait rapport au Parlement européen et au Conseil.

Obligations importantes

Selon l'article 20 (Gouvernance), les organes de direction des entités essentielles et importantes doivent approuver les mesures de gestion des risques de cybersécurité prises par ces entités, superviser leur mise en œuvre et peuvent être tenus pour responsables des infractions.

Selon l'article 20, les États membres veillent à ce que « les membres des organes de direction des entités essentielles et importantes soient tenus de suivre une formation » et encouragent les entités essentielles et importantes à proposer régulièrement une formation similaire à leurs employés, afin qu'ils acquièrent des connaissances et des compétences suffisantes pour leur permettre d'identifier les risques et d'évaluer les pratiques de gestion du risque de cybersécurité et leur impact sur les services fournis par l'entité.

Selon l'article 21 (Mesures de gestion du risque de cybersécurité), les entités essentielles et importantes doivent prendre des mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui pèsent sur la sécurité des réseaux et des systèmes d'information qu'elles utilisent pour leurs activités ou pour la fourniture de leurs services, et pour prévenir ou réduire au minimum l'impact des incidents sur les destinataires de leurs services et sur d'autres services.
En tenant compte de l'état de l'art et, le cas échéant, des normes européennes et internationales pertinentes, ainsi que du coût de la mise en œuvre, les mesures visées garantissent un niveau de sécurité des réseaux et des systèmes d'information adapté aux risques encourus. Lors de l'évaluation de la proportionnalité de ces mesures, il est dûment tenu compte du degré d'exposition de l'entité aux risques, de la taille de l'entité et de la probabilité d'occurrence d'incidents et de leur gravité, y compris

leur impact sociétal et économique.

Les mesures sont fondées sur une « approche tous risques » qui vise à protéger les réseaux et les systèmes d'information ainsi que l'environnement physique de ces systèmes contre les incidents, et comprennent au moins les éléments suivants déjà présents dans la Politique de Sécurité des Ministères Sociaux publiée au journal officiel en octobre 2015 :

- Des politiques d'analyse des risques et de sécurité des systèmes d'information (*Référence PSSI MCAS octobre 2015 INT-HOMOLOG-SSI : Homologation de sécurité des systèmes d'information*) ;
- Le traitement des incidents (1er octobre 2017 article 110 de la Loi de modernisation de notre système de santé du 26 janvier 2016) (*Référence PSSI MCAS octobre 2015 TI-OPS-SSI : chaînes opérationnelles SSI*) ;
- La continuité des activités, notamment la gestion des sauvegardes et la reprise après sinistre, ainsi que la gestion des crises (*Référence PSSI MCAS octobre 2015 ARCHI-STOCKCI : architecture de stockage et de sauvegarde, PCA-MINIS : définition du plan ministériel de continuité d'activité des Systèmes d'Information*) ;
- La sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs directs ou ses prestataires de services (*Référence PSSI MCAS octobre 2015 DEV-SOUS-TRAIT : intégrer des clauses SSI dans les contrats de sous-traitance de développement informatique*) ;
- La sécurité dans l'acquisition, le développement et la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités (*Référence PSSI MCAS octobre 2015 DEV-INTEGR-SECLOC : intégrer la sécurité dans les développements locaux*) ;
- Les politiques et procédures permettant d'évaluer l'efficacité des mesures de gestion des risques liés à la cybersécurité (*Référence PSSI MCAS octobre 2015 CONTR-BILAN-SSI : bilan annuel*) ;
- Les pratiques de base en matière de cyber hygiène et la formation à la cybersécurité (*Référence PSSI MCAS octobre 2015*) ;
- Les politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement ;
- La sécurité des ressources humaines, les politiques de contrôle d'accès

et la gestion des actifs (*Référence PSSI MCAS octobre 2015 RH-SSI : charte d'application SSI, RH-MOTIV : choix et sensibilisation des personnes tenant les postes clés de la SSI, RH-CONF : personnels de confiance, RH-UTIL : sensibilisation des utilisateurs des systèmes d'information, RH-MOUV : gestion des arrivées, des mutations et des départs, RH-NPERM : gestion du personnel non permanent (stagiaires, intérimaires, prestataires …*) ;
- L'utilisation de solutions d'authentification multifactorielle ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes de communication d'urgence sécurisés au sein de l'entité, le cas échéant.

La nouvelle directive NIS 2, principaux éléments de discrimination d'avec NIS 1

La nouvelle proposition de la Commission vise à combler les lacunes de la précédente directive NIS, à l'adapter aux besoins actuels et à la rendre pérenne.

À cette fin, la proposition de la Commission élargit le champ d'application de la directive NIS actuelle en ajoutant de nouveaux secteurs en fonction de leur importance pour l'économie et la société, et en introduisant un plafond de taille clair - ce qui signifie que toutes les moyennes et grandes organisations des secteurs sélectionnés seront incluses dans le champ d'application. En même temps, elle laisse aux États membres une certaine marge de manœuvre pour identifier les entités plus petites présentant un profil de risque élevé en matière de sécurité.

La proposition :
- Supprime la distinction entre les opérateurs de services essentiels et les fournisseurs de services numériques. Les entités seront classées en fonction de leur importance et divisées en catégories essentielles et importantes, qui seront soumises à des régimes de surveillance différents.
- Renforce et rationalise les exigences en matière de sécurité et d'information pour les entreprises en imposant une approche de gestion des risques, qui fournit une liste minimale d'éléments de sécurité de base qui doivent être appliqués. La proposition introduit des dispositions plus

précises sur le processus de notification des incidents, le contenu des rapports et les délais.

En outre, la Commission propose d'aborder la question de la sécurité des chaînes d'approvisionnement et des relations avec les fournisseurs en exigeant des entreprises qu'elles s'attaquent aux risques de cybersécurité dans les chaînes d'approvisionnement et les relations avec les fournisseurs. Au niveau européen, la proposition renforce la cybersécurité de la chaîne d'approvisionnement pour les technologies clés de l'information et de la communication. Les États membres, en coopération avec la Commission et l'ENISA, peuvent procéder à des évaluations coordonnées des risques des chaînes d'approvisionnement critiques, en s'appuyant sur l'approche fructueuse adoptée dans le cadre de la recommandation de la Commission sur la cybersécurité des réseaux 5G.

La proposition :
- Introduit des mesures de surveillance plus strictes pour les autorités nationales, des exigences plus strictes en matière d'application et vise à harmoniser les régimes de sanctions dans les États membres.
- Renforce également le rôle du groupe de coopération dans l'élaboration des décisions politiques stratégiques et accroît le partage d'informations et la coopération entre les autorités des États membres. Elle renforce également la coopération opérationnelle, notamment en matière de gestion des cybercrises.
- Établit également un cadre de base avec des acteurs clés responsables de la divulgation coordonnée des vulnérabilités nouvellement découvertes dans l'UE et crée un registre de l'UE dans ce domaine, géré par l'agence européenne pour la cybersécurité (ENISA).

Adaptation au domaine hospitalier et connexes

En France pour le secteur santé, les établissements support des groupements hospitaliers de territoire (136 GHT créé en juillet 2016) ont été désignés opérateurs de services essentiels. Cette désignation est le fruit d'un échange entre les ministères sociaux et l'Agence Sécurité des Systèmes d'Information.

Au regard du nombre d'incidents cyber sécurité ayant touché durablement les établissements (Arles, Dax, Villefranche-sur-Saône, Rouen, ApHp, Versailles, Corbeil…) il pourrait être intéressant de s'interroger sur l'efficacité du dispositif d'autant que pour répondre aux menaces croissantes liées à la numérisation et à la multiplication des cyberattaques, la Commission a présenté une proposition visant à remplacer la directive NIS si difficile à mettre en oeuvre sur le secteur.

Toute avancée légale censée améliorer l'existant s'affronte à la réalité du terrain. En l'occurrence et s'agissant du secteur de la santé, les mêmes causes produisent les mêmes effets. Cohérence, gouvernance, homogénéité, compétences, ressources, contrôle et sanction sont encore et toujours des maillons fragiles voire défaillants. On rappellera que le secteur doit adresser les patients avant toute chose et non pas le marché. Les deux points structurants de la cybersécurité en santé sont la bonne prise en charge des patients et le caractère optimal de l'utilisation et de la préservation des ressources publiques.

NIS 2, dans son application, pour faire preuve d'efficacité, doit tenir compte des points suivants :

- Le législateur et ses organisations donnent-ils l'exemple ?
- Les directeurs d'établissements ont-ils compris les enjeux et savent-ils de quoi l'on parle ?
- Les acteurs de santé ont-ils été formés aux aspects cognitifs et comportementaux qui représentent 80% des fragilités ?
- Les techniciens sont-ils compétents, quelles sont les méthodes de contrôle ?

- Les établissements ne peuvent-ils pas bénéficier d'outils communs mutualisés générateurs de performance, d'économie et de synergie ?
- Les techniciens bénéficient-ils d'outils de veille et de partage d'information communs ?
- Quels sont les outils de formation continue disponibles et déployés alors que la cyber malveillance évolue très vite (no code Hacking, New AI) ?
- Quels sont les outils de contrôle et de sanctions réelles appliquées sur le terrain ?

[1] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022L2555

Données de santé : comment concilier le besoin d'innovation, de sécurité et le respect des libertés et valeurs fondamentales

GARANCE MATHIAS
Avocat Associé
Fondateur Mathias Avocats[1]

Les récents bouleversements de nos sociétés, notamment depuis la pandémie, ont mis en exergue tout à la fois l'importance dans notre vie quotidienne de notre système de santé, ainsi que sa fragilité, révélant un besoin fort de sécurité technique et réglementaire.

Face au développement du numérique, un constat s'impose : les données de santé sont au cœur de l'innovation. La santé numérique (e-santé) est une réalité, qui se traduit par un usage quotidien, par les professionnels de santé, de l'intelligence artificielle et des objets connectés, afin d'améliorer la prévention et la qualité de soins de l'ensemble des citoyens. Nos données de santé sont donc traitées, stockées et circulent en masse au sein d'une chaîne d'acteurs hétérogènes (médecins, hébergeurs, etc.). Cet usage croissant et la circulation exponentielle de nos informations médicales n'ont de cesse d'accroître la valeur de ces dernières. C'est pourquoi elles sont les cibles privilégiées des cyberattaquants, comme l'ont montré des affaires récentes (notamment les cyberattaques contre les hôpitaux de l'Assistance publique-Hôpitaux de Paris, AP-HP, en septembre 2021, l'hôpital de Dax en février 2021 et l'hôpital de Corbeil-Essones en août 2022). Nonobstant ce risque prégnant de cyberattaques, le besoin de confiance en nos systèmes repose sur la sécurité juridique et technique[2], indispensable au déploiement de notre santé numérique, ainsi qu'à son progrès.

Les innovations et nouvelles applications en matière de santé, notamment au travers de l'usage du big data et de l'intelligence artificielle[3] ne doivent pas s'effectuer au détriment de l'éthique et du respect des droits des individus. Dans ce contexte, un cadre juridique exigeant doit être élaboré pour garantir la confiance de l'ensemble des acteurs et des citoyens : la cybersécurité de la santé doit être une évidence[4].

Ainsi, face à ces enjeux de société et d'éthique, quelle définition des données de santé ? Comment encadrer la cybersécurité des données de santé en Europe ? Comment ne pas freiner l'innovation ? Comment garantir la souveraineté numérique de nos données et de notre système de santé ?

Donnée de santé : une définition élargie pour une protection accrue

Dans la plupart des pays, les données de santé font l'objet d'une réglementation spécifique en ce qu'elles touchent à l'individu et aux intérêts vitaux[5]. Ainsi, l'un des apports du Règlement Général sur le Protection des Données, Règlement (UE) 2016/679 du 27 avril 2016, (ci-après RGPD) a été de définir les données de santé comme « *les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* »[6]. C'est donc une définition large englobant l'état mental et physique d'un individu qui a été choisie par le législateur européen pour définir le champ d'application des données de santé.

Ce sont des données *sensibles*[7], ce qui a pour conséquence d'avoir des exigences de sécurité et juridiques renforcées (comme la réalisation d'une analyse d'impact sur la protection des données[8]).

La jurisprudence a également élargi ce champ d'application. Ainsi, dans un récent arrêt de la Cour de justice de l'Union européenne[9] sont considérées comme étant des « données sensibles » « *toute donnée relative à la santé physique ou mentale passée, présente ou future d'une personne (y compris la fourniture de services de soins de santé) qui révèle des informations sur l'état de santé de la personne* ». Une interprétation aussi large des

« données de santé » permet de regrouper sous ce terme des informations concernant directement la santé mais aussi des informations qui ne deviennent des données de santé que lorsqu'elles sont combinées à d'autres informations ou que si elles sont transmises dans un contexte médical.

À titre d'exemple, certains compteurs intelligents ont des capteurs sensibles aux données individuelles de consommation qui sont utilisées dans des projets de recherche sur les maladies chroniques ou le vieillissement. De plus, comme le met en exergue la récente délibération de la Cnil, les données collectées au travers des réseaux sociaux peuvent être qualifiées de données de santé puisqu'elles peuvent être utilisées afin de mettre en place des modèles de surveillance épidémiologique[10]

À l'instar de l'Union européenne, d'autres pays ont choisi d'avoir une protection renforcée desdites données de santé. Les États-Unis notamment ont adopté une législation spécifique (HIPAA[11]) avec une définition large desdites données et des exigences de sécurité renforcées.

Quel régime juridique en France ?

La loi du 24 juillet 2019 relative à l'organisation et la transformation du système de santé[12] a créé une plateforme des données de santé (dite « Health Data Hub », HDH), destinée à faciliter le partage des données de santé issues de sources très variées afin de favoriser la recherche.[13]

La plateforme a signé, le 15 avril 2020, un contrat avec une filiale irlandaise de la société Microsoft, dont le siège est aux États-Unis, pour l'hébergement des données et l'utilisation de logiciels nécessaires à leur traitement. Ce choix a fait l'objet d'un avis critique de la CNIL, selon lequel : « *En raison de la sensibilité et du volume des données ayant vocation à être hébergées au sein de la Plateforme, pour lesquelles le niveau de protection technique mais aussi juridique le plus élevé doivent être assurés, y compris en matière d'accès direct par les autorités de pays tiers, la CNIL a fait part de son souhait que son hébergement et les services liés à sa gestion puissent être réservés à des entités relevant exclusivement des juridictions de l'Union européenne*. »[14]

Dans ce contexte, par crainte de possibles transferts de données vers les États-Unis, des associations et collectifs (professionnels du secteur de la santé et de l'informatique médicale) ont demandé au juge des référés du Conseil d'État de suspendre en urgence la plateforme Health Data Hub. Dans sa décision, le Juge des référés du Conseil d'État a relevé que la Cour de justice de l'Union européenne (dans sa décision dite « Schrems 2 »)[15] n'avait pas jugé que le droit européen de la protection des données interdirait de confier le traitement de données, sur le territoire de l'Union européenne, à une société américaine. En conséquence, le juge n'a pas relevé d'illégalité grave et manifeste qui justifierait la suspension immédiate du traitement des données par cette plateforme, sous réserve de « *prendre des précautions particulières, sous le contrôle de la CNIL* ».[16]

Le débat reste ouvert, en particulier au regard des annonces selon lesquelles le contrat avec Microsoft devrait perdurer jusqu'en 2025.

Plus de sécurité dans l'Union européenne : vers un espace européen des données de santé ?

Face à l'étendue du champ d'application des données de santé, en lien avec le développement des applications de santé, des dispositifs médicaux connectés et de l'intelligence artificielle, la Commission européenne s'est emparée de ce sujet fondamental pour l'ensemble des citoyens, soulignant que : « *la transformation numérique est essentielle pour fournir de meilleurs soins de santé aux citoyens, pour construire des systèmes de santé plus solides et plus résilients, pour soutenir la compétitivité et l'innovation à long terme*. »[17]

C'est dans ce contexte qu'a été présentée la proposition européenne de création d'un espace européen des données de santé[18], visant à garantir aux individus le contrôle de leurs propres données et permettant une meilleure prestation des soins de santé. Cette proposition doit également permettre à l'UE de tirer pleinement parti du potentiel offert par un échange sûr et sécurisé de l'utilisation et la réutilisation des données de santé. Cette vision partagée par l'ensemble des États membres, s'inscrit au sein de notre socle culturel et politique commun qui anime le projet européen. L'Union fédère ainsi une vision commune des États membres et a une position de force par rapport aux autres acteurs mondiaux à

laquelle aucun État, seul, ne pourrait prétendre.

Ainsi, afin de remplir ces objectifs ambitieux liés à la souveraineté numérique, des obstacles doivent être dépassés. Premièrement, la Commission européenne considère que les individus font face à de nombreux défis lorsqu'il s'agit d'accéder et de transférer leurs données de santé au sein d'un même État membre, et entre ces derniers. En effet, il existe une hétérogénéité entre les différents États membres, puisque tous n'ont pas mis en place de système d'échange électronique de données de santé, empêchant l'effective interopérabilité des systèmes. En témoigne la gouvernance des données de santé dans les pays européens, à ce jour hétérogène, puisque les structures existantes au sein des États membres sont soumises, soit à un régime centralisé, soit à un régime décentralisé. À ce titre, la Finlande, (Findata) et la France (Health Data Hub) ont des plateformes centralisées des données de santé, alors qu'en Espagne, des plateformes (comme IACS-BIGAN, pour l'Aragon) opèrent dans un système décentralisé.

L'espace européen des données de santé devrait favoriser l'échange de différents types de données de santé électroniques et l'accès à ces dernières, y compris les dossiers médicaux électroniques, les données génomiques, les registres de patients, etc. Il devrait faciliter la fourniture des soins de santé et contribuer à la recherche, à l'innovation, à l'élaboration de politiques et à la réglementation en matière de santé ainsi qu'à la médecine personnalisée (utilisation secondaire des données de santé électroniques). L'autre point important de vigilance, concerne la nécessité d'héberger les données de santé dans l'Union européenne, en raison de leur sensibilité et de leur volume.[19]

La Commission européenne a rappelé les interdépendances sectorielles très fortes et donc la nécessité d'une stratégie de cybersécurité à l'échelle européenne[20] : « *La cybersécurité fait partie intégrante de la sécurité des Européens. Qu'ils aient recours à des appareils, réseaux électriques, banques, aéronefs, administrations publiques ou hôpitaux connectés, les citoyens doivent pouvoir avoir l'assurance qu'ils seront protégés contre les cybermenaces. […] Les transports, l'énergie, la santé, les télécommunications, la finance, […] dépendent fortement de réseaux et de systèmes d'information de plus en plus interconnectés.* »

Indépendamment des textes en cours de transposition, notamment la directive européenne dite « NIS 2 » [21], plusieurs textes sont en cours d'adoption à savoir :

- le « Cyber Resilience Act »[22], un projet de règlement européen visant à améliorer la cybersécurité des produits et des services numériques dans l'Union Européenne ;
- plus spécifiquement en matière de santé, une proposition de directive qui porte sur la résilience des entités critiques et les obligations de cybersécurité imposées à certains secteurs, dont la santé [23]; ou encore
- le projet de « Cyber Solidarity Act »[24] qui vise à renforcer la coopération européenne en matière de réaction aux cyberattaques.

Conclusion

Les données numériques sont indispensables dans notre quotidien et les données de santé sont d'une utilité considérable pour le bon fonctionnement et la performance du système de santé, au service de ses utilisateurs et de ses bénéficiaires (citoyens, professionnels de santé, chercheurs). Notre cadre réglementaire doit donc être opérationnel et efficient tout en étant protecteur aussi bien de nos libertés que des intérêts économiques. Tel est le défi que les pouvoirs publics et l'ensemble des acteurs du secteur de la santé doivent relever afin d'être parties prenantes dans cette construction réglementaire.

L'impératif technique doit se traduire en termes juridiques pour instaurer la confiance. Gageons qu'accompagnant les innovations et avancées technologiques dans le domaine de la santé, notre cadre juridique sera façonné pour être plus protecteur, plus résilient, mais aussi aisément applicable et porteur de valeurs communes.

Le droit est et sera un instrument, un pilier de notre souveraineté numérique essentiel pour avoir une autonomie stratégique européenne dans le secteur-clef de la santé.

[1] L'auteur tient à remercier Madame Eva Aspe, en charge des affaires publiques au sein de Mathias Avocats pour sa contribution.

[2] À cet égard, citons une décision récente de la CNIL, qui a prononcé une sanction de 380 000 euros à l'encontre de la société DOCTISSIMO pour avoir enfreint la réglementation sur les données personnelles, notamment concernant le recueil du consentement des personnes à la collecte et l'utilisation de leurs données de santé, et pour ne pas avoir respecté les règles sur les cookies. https://www.cnil.fr/fr/donnees-de-sante-et-utilisation-des-cookies-doctissimo-sanctionne-par-une-amende-de-380-000-euros

[3] Proposition de Règlement européen sur l'intelligence artificielle, COM/2021/206 final, 21 avril 2021 : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52021PC0206

[4] Comme l'a rappelé le Président Emmanuel MACRON dans sa déclaration relative aux cyberattaques dans les hôpitaux et à la stratégie nationale sur la cybersécurité, le 18.02.2021 : https://www.elysee.fr/emmanuel-macron/2021/02/18/strategie-nationale-cybersecurite. Voir aussi, les mesures mises en place pour « accompagner et appuyer les structures de santé et du médico-social dans la gestion des actes de cyber malveillance » : https://esante.gouv.fr/strategie-nationale/cybersecurite

[5] Comme le précise le Règlement Général sur le Protection des Données, Règlement (UE) 2016/679 du 27 avril 2016, dans le « Considérant 2 : Les principes et les règles régissant la protection des personnes physiques à l'égard du traitement des données à caractère personnel les concernant devraient, quelle que soit la nationalité ou la résidence de ces personnes physiques, respecter leurs libertés et droits fondamentaux, en particulier leur droit à la protection des données à caractère personnel. Le présent règlement vise à contribuer à la réalisation d'un espace de liberté, de sécurité et de justice et d'une union économique, au progrès économique et social, à la consolidation et à la convergence des économies au sein du marché intérieur, ainsi qu'au bien-être des personnes physiques. », https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679E

[6] Cf. article 4 du RGPD, « Définitions »

[7] Cf. Considérant 35 et article 4§15 du RGPD

[8] Une analyse d'impact sur la protection des données (AIPD) est une étude qui doit être menée lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées : https://www.cnil.fr/fr/definition/analyse-dimpact-aipd

[9] Par un arrêt du 1er août 2022, la Cour de justice de l'Union européenne (CJUE) a clarifié sa position concernant le traitement de données à caractère personnel susceptibles de divulguer indirectement des informations relevant de catégories particulières de données (CJUE, 1er août 2022, Aff. C 184/20) : https://www.avocats-mathias.com/donnees-personnelles/interpretation-large-des-categories-particulieres-de-donnees.

[10] https://www.cnil.fr/fr/donnees-de-sante-et-utilisation-des-cookies-doctissimo-sanctionne-par-une-amende-de-380-000-euros

[11] Health Portability and Accountability Act, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

[12] Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé, https://www.legifrance.gouv.fr/loda/id/LEGIARTI000038824934/2019-07-27

[13] Les missions de la Plateforme sont prévues par l'article L. 1462-1 du Code de la santé publique. Elles consistent à :
- réunir, organiser et mettre à disposition des données, issues notamment du système national des données de santé (SNDS) et promouvoir l'innovation dans l'utilisation des données de santé ;
- informer les patients, promouvoir et faciliter l'exercice de leurs droits ;
- contribuer à l'élaboration des référentiels de la CNIL ;
- faciliter la mise à disposition de jeux de données de santé présentant un faible risque d'impact sur la vie privée ;
- contribuer à diffuser les normes de standardisation pour l'échange et l'exploitation des données de santé ;
- accompagner, notamment financièrement, les porteurs de projets sélectionnés dans le cadre d'appels à projets lancés à son initiative et les producteurs de données associés aux projets retenus.

[14] CNIL, 9 février 2021 : https://www.cnil.fr/fr/la-plateforme-des-donnees-de-sante-health-data-hub

[15] Arrêt dans l'affaire C-311/18 du 16 juillet 2020, https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091fr.pdf

[16] Cf. décision du Juge des référés du Conseil d'État, extrait : « Si le risque ne peut être totalement exclu que les services de renseignement américains demandent l'accès à ces données, il ne justifie pas, à très court terme, la suspension de la Plateforme, mais impose de prendre des précautions particulières, sous le contrôle de la CNIL. » : https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2020-10-13/444937

[17] Communication de la Commission européenne, Un espace européen des données de santé: exploiter le potentiel des données de santé pour les citoyens, les patients et l'innovation, 3.5.2022 COM(2022) 196 final

[18] Proposition de Règlement du Parlement Européen et du Conseil relatif à l'espace européen des données de santé, 3.5.2022, COM(2022) 197 final : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52022PC0197

[19] Voir l'avis commun, du 12 juillet 2022, du Comité européen de la protection des données (CEPD) et du Contrôleur européen de la protection des données, sur ce règlement : https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202203_europeanhealthdataspace_en.pdf

[20] Communication du 16.12.2020, JOIN(2020) 18 final : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52020JC0018

[21] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union dite « NIS 2 : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0080.01.FRA&toc=OJ%3AL%3A2022%3A333%3ATOC

[22] Proposition de Règlement européen concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques, 5.9.2022 COM(2022) 454 final, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52022PC0454

[23] Proposition de directive du Parlement européen et du Conseil sur la résilience des entités critiques, 16.12.2020, COM(2020) 829 final : htttps://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:52020PC0829

[24] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0209

Cybersécurité et santé : constat et réponses

MYRIAM QUÉMÉNER
Magistrat
Docteur en droit

Le secteur de la santé est régulièrement visé par les cybercriminels car les données des patients permettent de leur livrer beaucoup d'éléments pour dresser le profil numérique de leurs futures victimes. Face à ce fléau, une véritable stratégie se met en place à la fois sur le plan juridique, institutionnel et opérationnel.

Depuis de nombreux mois les hôpitaux et les établissements médicaux dans leur ensemble sont victimes de cyberattaques et plus largement le domaine de la santé[1]. En 2022, par exemple le centre hospitalier sud francilien de Corbeil-Essonnes et l'hôpital de Versailles ont été visés par ces cyber-attaques, lesquelles ont entraîné également la divulgation d'une partie des dossiers médicaux. Plus récemment, en janvier 2023, le groupe Elsan qui assure la gestion de l'accueil d'environ 140 cliniques en France a été pris pour cible, occasionnant la déstabilisation ponctuelle du fonctionnement de deux établissements à Fréjus et Draguignan.

Les atteintes informatiques contre les systèmes de santé ont un nombre quasi constant sur ces deux années. Ces attaques ciblent toute la chaîne médicale. Pour 78%, elles ont impacté des organismes recevant des patients (centres hospitaliers, cliniques privées, Ehpad, maisons de santé ou de convalescence…). D'autres établissements de santé ont également été victimes (laboratoires d'analyse & pharmaceutique, mutuelles, pharmacies, sociétés d'ambulances, cabinets dentaires, ordres…). Pour les trois quarts, il s'agissait d'attaques par rançongiciels.

Le rançonnage numérique est une activité criminelle utilisant un programme informatique aux fins d'extorsion de fonds. Les logiciels malveillants ont pour objectif de rendre inaccessibles les fichiers d'une

entité, historiquement par blocage du système d'information, aujourd'hui par un chiffrement robuste. Une fois les données chiffrées, le paiement d'une rançon en crypto-monnaies est exigé des victimes en échange du déchiffrement de leurs données. Dans le même temps, les cybercriminels pratiquent un second type d'extorsion. Ils ne se limitent plus à rendre inaccessibles les systèmes, ils exfiltrent désormais les données de leurs victimes.

Le 5 juillet 2023, l'Agence de l'Union européenne pour la cybersécurité (*European Union Agency for Cybersecurity, ENISA*) a publié son premier rapport sur la cybersécurité dans le secteur de la santé[2]. Elle a analysé 215 incidents qui ont eu lieu dans des hôpitaux, des laboratoires, des mutuelles, des organismes publics de santé ou encore des industries pharmaceutiques, entre janvier 2021 et mars 2023. Le rapport indique que les professionnels de santé représentent 53% du nombre total d'incidents du secteur hospitalier avec 42% des incidents signalés, soit 89 au total.

Pour ce qui est de la répartition par pays, la France a connu 43 incidents et au total, l'Union européenne a connu 91 incidents, contre 84 en 2022. Sur les trois premiers mois de 2023, elle en compte déjà 40. L'agence européenne nuance cependant ces chiffres qui n'impliquent pas forcément une hausse des attaques. « *Une telle augmentation peut avoir lieu dans un contexte de maturation d'un secteur en matière de détection et de signalements d'incidents, ce qui peut être lié à l'effet des obligations légales de signalements d'incidents en vigueur dans l'Union européenne* ». La présence de données de santé dans ces établissements en fait des cibles attrayantes pour les acteurs de la cybermenace qui profiteraient de l'opportunité pour faire de l'extorsion sous la menace de divulgation. En 2023, l'ENISA remarque aussi la hausse des « attaques par déni de service distribué ». Elles ont lieu par le biais d'un épuisement du service et de ses ressources, ou « en surchargeant les composants de l'infrastructure du réseau » précise l'agence. Dans 40% des cas, le responsable de l'incident est inconnu, note par ailleurs l'ENISA. Quant aux motivations des cybermenaces, elles sont pour 83% financières, 10% idéologiques, 1% liées à de l'espionnage, et pour 6% d'une autre nature.

Une atteinte à un système de traitement automatisé de données (ASTAD) peut entraîner la suspension temporaire de l'activité médicale des établissements qui en sont victimes. Cette rupture d'activité peut alors entraîner des conséquences particulièrement importantes sur les prises en charge et la continuité des soins (transfert de patients, arrêt des systèmes monitoring, etc.) et/ou sur leur accès aux numéros d'urgence (arrêt des systèmes de numéros d'urgences, etc.). Ces attaques, notamment celles touchant les centres hospitaliers, peuvent mettre la vie des patients en danger. De la pharmacie au dossier médical d'un hôpital, le parcours santé d'un patient est désormais totalement numérisé. En outre, les matériels de soins des établissements de santé sont connectés. Dès lors, le blocage du système informatique d'un établissement met à mal la continuité et l'effectivité des soins. En pratique, les établissements victimes sont contraints de revenir à un « traitement papier », et doivent parfois procéder en urgence à des transferts de patients (exemple : transfert des bébés du service néonatalogie du CH Sud francilien de Corbeil Essonne). Rappelons qu'un patient est décédé en Allemagne lors de son transfert à la suite de la cyber-attaque commise à l'encontre de la clinique universitaire de Düsseldorf.

La remise en état des systèmes informatiques peut durer plusieurs mois, obligeant parfois à une reconstruction complète des structures. Par exemple, l'hôpital de Dax, victime d'une cyberattaque en 2020, a mis plus de deux mois à récupérer l'accès à une messagerie électronique.
Les données personnelles et les données de santé des patients, y compris leurs dossiers médicaux, sont les principales cibles (63 cas recensés), soit 30% des cas. Les autres cibles sont les systèmes informatiques et réseaux non médicaux (26%), les systèmes d'information (23%) et les données de la structure et de son personnel (15%).

Le rapport indique également que les incidents ont eu des conséquences en matière de vol de données (43%), de services de santé perturbés (22%) et de services non liés aux soins (26%), sans compter les pertes financières. En 2022, une étude estimait le coût médian d'un incident de sécurité majeur dans le secteur de la santé à 300 000 €.

Quelles réponses juridiques ?

Les attaques numériques correspondant à des atteintes à un système automatisé de traitement de données (ASTAD), sont prévues et réprimées par les articles 323-1 à 323-4 du Code pénal.

Le développement de ces attaques et leurs incidences potentiellement graves pour la santé des personnes ont conduit à l'insertion dans le code pénal d'une nouvelle circonstance aggravante de mise en danger d'autrui appliquée aux ASTAD dans le cadre de la loi n°2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'Intérieur.

Le nouvel article 323-4-2 du Code pénal dispose ainsi que « *lorsque les infractions prévues aux articles 323-1 à 323-3-1 ont pour effet d'exposer autrui à un risque immédiat de mort ou de blessures de nature à entraîner une mutilation ou une infirmité permanente ou de faire obstacle aux secours destinés à faire échapper une personne à un péril imminent ou à combattre un sinistre présentant un danger pour la sécurité des personnes, la peine est portée à dix ans d'emprisonnement et à 300 000 € d'amende.* »

Lorsque la circonstance aggravante de mise en danger de la vie d'autrui a vocation à être retenue à l'occasion de faits d'atteinte à un système de traitement automatisé de données commis au moyen d'un dispositif de type rançongiciel les procureurs de la République locaux sont invités à prendre attache avec la section J3 du parquet de Paris aux fins d'engager une démarche concertée destinée à apprécier l'opportunité d'un dessaisissement à son profit.

L'identification de l'échelon pertinent de traitement s'appréciera par ailleurs à la lumière de plusieurs critères objectifs de saisine susceptibles de résulter du nombre d'auteurs ou de victimes, de la technicité des moyens employés, du mode opératoire utilisé, de la dimension nationale ou transnationale des faits ou de l'infrastructure criminelle sous-jacente, de la qualité des victimes de la cyber-attaque ou encore de l'importance du préjudice en présence.

Dans tous les cas, est rappelée la nécessité, préalablement à tout dessaisissement, de veiller à ce que les premières investigations réalisées par les services enquêteurs du ressort des parquets initialement saisis comportent les éléments matériels relatifs à la caractérisation de la cyber-attaque nécessaires à l'appréciation par le parquet JIRS ou le parquet JUNALCO (J3).

En outre, la directive Network and Information Security 2[3](NIS 2) oblige désormais les directions à s'engager pleinement sur la thématique de la cybersécurité pour accroître le niveau de cybersécurité au sein de l'Union. Transposée par une législation nationale d'ici octobre 2024, la directive NIS 2 élargira le périmètre des anciens organismes de services essentiels (OSE) régulés en opérant une distinction entre « entités essentielles » et « entités importantes »), à des milliers d'entités correspondant à 35 secteurs (administrations centrales et régionales, certaines collectivités territoriales, transports, secteur bancaire, infrastructures des marchés financiers, santé, eau, infrastructures numériques, la gestion des services TIC, espace, gestion des déchets, distributeurs alimentaires, etc.) et 600 types d'entreprises allant des PME (de plus 50 employés ou affichant un chiffre d'affaires ou un bilan supérieur à 10M€) aux groupes du CAC40. À cette occasion, le nombre d'entités visées par l'ANSSI sera, au minimum, multiplié par 10. La directive NIS 2 incite également toutes les entités, qu'elles soient régulées ou non, à recourir à des outils de cybersécurité en sources ouvertes.

Santé et mesures de cybersécurité

Le ministre de la santé et de la prévention, a dévoilé en mai 2023 la feuille de route du numérique en santé pour la période 2023-2027. Dont l'un des axes doit conduire à décupler la vigilance cyber pour empêcher que les hôpitaux ne deviennent des « cybercibles ». Il a abouti à l'installation d'un comité de pilotage interministériel dédié à la question de la cybersécurité des établissements de santé avec la réalisation au moins une fois par an d'une simulation de crise cyber.

L'Agence du Numérique en Santé joue un rôle central en la matière, en particulier grâce au « *Computer Emergency Response Team* »[4] (CERT Santé)

qu'elle héberge et qui accompagne les établissements de santé dans la veille sur les menaces de cybersécurité et la réponse à incident ; il s'agit du premier CERT sectoriel[5] en France et partenaire privilégié de l'Agence nationale de sécurité des systèmes d'information (ANSSI).

L'Agence du Numérique en Santé développe une stratégie ministérielle de cybersécurité pour l'écosystème, un cadre constitué de règles communes de régulation et d'échanges, autour de l'interopérabilité et de la sécurité. À l'écoute de ses bénéficiaires et de l'écosystème, elle accompagne les industriels et anime une démarche globale de référencement et d'audit. Sur le volet de la sécurité notamment, l'ANS produit des référentiels et des guides ; elle définit aussi les exigences cyber de la doctrine du numérique en santé, et gère le schéma de certification des hébergeurs de données de santé. Elle met en place des sessions de formation destinées en priorité pour les entreprises du numérique en santé proposant des services ou des produits numériques innovants.

La Task force cybersécurité est coordonnée par la Délégation au numérique en santé et réunit la DGOS (Direction Générale de l'Offre de Soins), l'ANSSI (Agence nationale de sécurité des systèmes d'information) et l'Agence Numérique en Santé (ANS); ainsi que les ARS et les groupements régionaux d'appuis de la e-santé (GRADeS) sous l'autorité des agences régionales de santé (ARS).Cette Task force travaille également en proximité avec les fédérations hospitalières et les responsables de sécurité des systèmes d'information. De nombreux efforts sont réalisés et dès à présent, plus de 500 établissements de santé ont désormais réalisé au moins un premier exercice de gestion de crise cyber[6].

La plupart des derniers rapports publiés comme par exemple celui de l'institut Montaigne sur la cybersécurité ou celui de l'Agence européenne pour la cybersécurité (ENISA) présentent un panorama des menaces d'origine cyber visant le secteur et souligne la nécessité de la mise en place d'une véritable stratégie[7] coordonnée. Un guide sur la cybersécurité a été diffusé[8] sur la base d'une adaptation de celui de l'ANSSI et la CPME. Les actions des agences et autorités publiques, l'ANSSI, Cybermalveillance.gouv.fr, s'accélèrent pour accompagner la transformation des établissements de santé pour une cybersécurité efficace.

Le CERT Santé dans son dernier rapport[9] fait aussi des recommandations communiquées aux structures comme la réduction de la surface d'attaque en désactivant les comptes, protocoles et services qui ne sont pas indispensables. Il préconise d'appliquer une politique de mot de passe suffisamment robuste afin d'éviter d'être la cible de cyberattaque. Il est aussi conseillé d'améliorer le suivi des correctifs par une veille des composants exposés sur internet et de les mettre à jour régulièrement. La priorité doit être donnée aux correctifs de sécurité correspondants à des vulnérabilités critiques afin de se prémunir au plus vite d'attaques cherchant à les exploiter. Il est conseillé d'analyser régulièrement les journaux de ses équipements périmétriques pour vérifier si elles ont été exploitées et en cas de doute renouveler l'ensemble de ses comptes. Il convient de renforcer les configurations et la sécurisation des accès car beaucoup de failles détectées lors des audits concernent une mauvaise configuration des protocoles utilisés[10] ou une divulgation d'informations sensibles. L'ensemble de ces vulnérabilités peut être corrigé assez simplement par la mise en œuvre de bonnes pratiques. Enfin, lors de la contractualisation d'une prestation avec un tiers, il est essentiel d'inclure des engagements sur le maintien en conditions de sécurité ainsi que la possibilité de réaliser des audits.

On constate véritablement le développement d'une stratégie étatique globale en matière de protection des données de santé des citoyens.

[1] Voir par exemple : Sénat. Question nº 21286, du 11 mars 2021. Piratages de données médicales et cybersécurité des laboratoires français JO Sénat 23 Juin 2022, p. 2999, https://www.lamyline.fr
[2] https://www.ENISA.europa.eu
[3] https///www.ssi.gouv.fr, Directive NIS 2 : ce qui va changer pour les entreprises et l'administration françaises | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)
[4] https://www.cyberveille-sante.gouv.fr/
[5] https://esante.gouv.fr/produits-services/cert-sante
[6] https://esante.gouv.fr/espace-presse
[7] https://www.institutmontaigne.org/ressources/pdfs/publications/cybersecurite-passons-lechelle
[8] https://esante.gouv.fr/sites/default/files/media_entity/documents/ANS_GUIDECYBER_PHASE%201-EXE%20-V2.pdf
[9] https://www.cyberveille-sante.gouv.fr/sites/default/files/media/document/2023-06/ANS_CERTSant%C3%A9_Rapport_Public_Observatoire_Signalements_ISSIS_2022_VF_0.pdf
[10] Par exemple le protocole SSL/TLS utilisé dans le cadre d'échanges chiffrés https

Table des matières

CyberCercle - 92 Cours Lafayette, 69003 Lyon
contact@cybercercle.com - cybercercle.com

« Sécurité numérique en Santé » est le quatrième ouvrage de notre Collection CyberCercle - Regards croisés lancée fin 2020.

Des livres collectifs qui associent pour chaque numéro des auteurs représentant différentes organisations, publiques et privées, autour d'une thématique déterminée dans le champ de la confiance et de la sécurité numériques.

Des livres collectifs qui peuvent se lire de la première à la dernière page, ou de façon séquencée, par des entrées « auteur » ou « thématique ».

Des livres collectifs qui n'ont pas l'ambition d'être exhaustifs mais qui ont pour vocation, grâce à des contributions de personnalités expertes complémentaires, d'apporter aux lecteurs des éléments d'analyse de confiance propres à enrichir leur connaissance du sujet et leur réflexion.

La Collection CyberCercle - Regards croisés s'inscrit ainsi, à travers ses publications, comme une référence dans le panorama français de réflexion sur les sujets de confiance et de sécurité numériques, un outil de travail au service de la décision.

Cet ouvrage dédié à la sécurité numérique en santé, secteur particulièrement ciblé aujourd'hui par les cyberattaques, répond à plusieurs enjeux de ce secteur, dont la résistance et la résilience sont fondamentales pour le bon fonctionnement de la société et la sécurité des patients que nous sommes tous.

Cet ouvrage a été réalisé avec le soutien de

AvantdeCliquer.com L'humain au cœur de la cybersécurité
BlueFiles
proofpoint.
CERTitude NUMERIQUE
LE GROUPE LA POSTE

PRIX : 21€
9 782494 223110