DOSSIER CYBERSÉCURITÉ – PARTIE I

Cyberattaques : pourquoi le monde de la santé est-il une cible ?

Vincent Trely[1,2]

1- Président – Association pour la sécurité des systèmes d'information de santé (Apssis) – Duneau – France
2- Directeur associé – Cabinet Weliom – Saint-Herblain – France

✉ **Vincent Trely** – Cabinet Weliom – Immeuble Opale B – 3, impasse Serge Reggiani – 44800 Saint-Herblain – France
E-mail : vtrely@weliom.fr

Les centres hospitaliers de Villefranche-sur-Saône, de Dax, d'Oloron-Sainte-Marie, de Narbonne, de Montpellier, d'Arles, de Périgueux font partie de la longue liste des structures de santé publiques ou privées attaquées par des virus informatiques ces douze derniers mois, selon un mode opératoire bien connu : le rançongiciel. Celui-ci, avec plus ou moins de virulence, bloque les systèmes informatiques en les chiffrant, rendant inopérants les services numériques et les accès aux fichiers de travail des agents, et détaille les modalités de paiement d'une rançon en cryptomonnaie censée offrir le retour à la normale. Agnès Buzyn, à l'époque ministre des Solidarités et de la Santé, avait déclaré en 2019 que « *la cybersécurité des établissements de santé devenait une priorité nationale* », bientôt imitée par le président de la République lui-même, Emmanuel Macron prenant la parole le 19 février 2021 sur le sujet. Pourquoi un

Résumé

Les centres hospitaliers de Villefranche-sur-Saône, de Dax, d'Oloron-Sainte-Marie… font partie de la longue liste des structures de santé attaquées par des virus informatiques cette année, selon un mode opératoire bien connu : le rançongiciel. Celui-ci bloque les systèmes informatiques en les chiffrant, rendant inopérants les services numériques et les accès aux fichiers de travail des agents, et détaille les modalités de paiement d'une rançon censée offrir le retour à la normale. Le problème est tel que le président de la République a pris la parole le 19 février 2021 sur le sujet. Alors pourquoi un tel engouement des criminels pour le secteur de la santé ? Plusieurs études estiment que la cybercriminalité est déjà la troisième économie mondiale, derrière la Chine et les États-Unis, et que son volume financier dépassera les 10 500 milliards de dollars en 2025. L'argent n'est plus toujours la cible primaire, les données l'ayant remplacé. Le secteur de la santé est très attractif en termes de contenus ! Rempli de données à caractère personnel, il constitue une mine d'or pour le crime organisé. Les intérêts du système de santé pour les pirates sont donc multiples : extraire les données pour les revendre sur le marché noir de l'internet, exercer un chantage financier sur l'institution dont les données ont été volées, les utiliser pour fabriquer de fausses identités, de faux documents… La formation des professionnels de santé aux bons usages des technologies numériques et à la cybersécurité est essentielle et sera intégrée à tous les cursus de formation des acteurs en santé afin de conforter les pratiques « d'hygiène numérique ». L'humain reste le meilleur moyen d'assurer au système de santé un haut niveau de sécurité, en le formant à la vigilance, un juste milieu entre la naïveté et la paranoïa !

Mots-clés : Système de santé – Cybercrime – Rançongiciel – Gestion du risque – Sensibilisation.

Abstract

Cyberattacks: why is healthcare targeted?

The hospitals of Villefranche-sur-Saône, Dax, and Oloron-Sainte-Marie… feature on the long list of healthcare facilities attacked this year by digital viruses following a well-known modus operandi: ransomware. This software blocks digital systems by encoding them so that digital services and access to workstations become inoperative. At the same time, it details the mode of payment of the ransom that is supposed to get things back to normal. The problem is such that the President of the French Republic spoke on the matter on 19 February 2021. Why are criminals so attracted by healthcare? Several studies estimate that cybercrime has now reached the third place in global economy, behind China and the USA, and its financial volume will exceed 10,500 billion dollars in 2025. The primary target is no longer money which has been replaced by data. Indeed, the healthcare sector is extremely attractive in terms of content! The personal data it contains represent a gold mine for organised crime. Healthcare data are extremely interesting for pirates: they may be extracted and sold on the internet black market, institutions whose data have been stolen may be blackmailed, and the data can be used to forge identities and papers. Training healthcare staff to the correct use of digital technology and cybersecurity is crucial and will be integrated to all healthcare staff training programmes so as to support the development of "digital hygiene". Human beings remain the best warrant for a highly secure healthcare system, hence the point of promoting staff vigilance and awareness to just the right level between naivety and paranoia!

Keywords: *Healthcare systems – Cybercrime – Ransomware – Risk management – Awareness-raising.*

tel engouement des criminels pour le secteur de la santé ? Pour quelles raisons s'en prendre à un hôpital, à une maison de retraite ou à un centre de santé ?

Le cybercrime en pleine croissance !

La croissance du cybercrime n'est pas un phénomène récent. Dès les prémices de la troisième révolution industrielle, celle des technologies numériques, l'écosystème de la criminalité internationale s'est très vite adapté et organisé, comprenant que « le business » du futur se ferait via les réseaux d'échanges de données, les plates-formes de services informatisées et que l'or du XXIe siècle serait « la data », les milliards de données produites et stockées par des systèmes déployés partout sur la planète. Plusieurs études, dont celle du Club des juristes publiée en 2021, estiment que la cybercriminalité est déjà la troisième économie mondiale, derrière la Chine et les États-Unis, et que son volume financier dépassera les 10 500 milliards de dollars en 2025 [1]. Quel est aujourd'hui l'intérêt d'aller braquer une agence bancaire, de risquer 10 ans de prison et une balle dans la peau pour quelques milliers d'euros ? L'argent n'est plus « réel », il est dématérialisé. Et l'argent n'est plus toujours la cible primaire, « la data », « les données » l'ayant remplacé.

Les secteurs de la banque/assurance, de l'industrie de pointe et des grands groupes du CAC 40 ont connu leurs premiers déboires dans les années 2000 et en ont tiré les leçons. Les récentes attaques du groupe Bouygues construction, de Covea ou de la banque centrale européenne rappellent que le risque zéro n'existe pas, mais pour autant, s'attaquer à ces mastodontes devient complexe et coûteux. Plusieurs mois de préparation, des équipes de hackers très performants et une organisation bien huilée sont nécessaires, pour des résultats toujours aléatoires, alors que les établissements de santé sont des cibles bien plus faciles. Les fragilités de ces institutions s'expliquent par trois principaux facteurs : une surface de numérisation plus récente, avec le déploiement massif de l'informatique sur les 15 dernières années dans pratiquement tous les métiers et la mise en œuvre de multiples services communicants vers les citoyens et les patients, des investissements techniques et humains qui n'ont pas suivi, laissant la part belle à des matériels vieillissants, voire totalement obsolètes et truffés de failles de sécurité connues et documentées, et un manque de sensibilisation du personnel, rarement formé aux bons usages du numérique, à l'hygiène informatique et aux « gestes barrières ». Ces trois facteurs connus des criminels les orientent naturellement vers ces systèmes, plus poreux, plus fragiles et tout aussi lucratifs. N'oublions pas que les cybercriminels, en bons chefs d'entreprise, recherchent eux aussi le meilleur retour sur investissement possible !

Si les grands groupes sont aujourd'hui mieux protégés contre les attaques informatiques, à la fois grâce à des investissements plus soutenus et des politiques de sécurité matures, ils ne sont pas pour autant sans intérêt pour le cybercrime, et en particulier pour le volet cyber espionnage consistant à dérober tout type d'information stratégique dans le cadre de la guerre économique qui fait rage ! Mais c'est une affaire d'agences de renseignement, les Américains, les Chinois et les Russes se partageant les trois premières places du podium, ce qui n'est pas nouveau. Soyons heureux de savoir que l'Europe est en train de se doter, elle aussi, d'une « force cyber » offensive afin de pouvoir enfin jouer d'égal à égal avec nos alliés ou nos ennemis, en fonction de contextes géopolitiques instables.

L'intérêt croissant pour les données de santé

Il serait très naïf de croire que l'intérêt croissant pour le système de santé ne se base que sur ses faiblesses. Le secteur est très attractif en termes de contenus ! Rempli de données à caractère personnel, administratives, de santé, de situation, il constitue une mine d'or intarissable pour le crime organisé. Le Règlement général sur la protection des données (RGPD), mis en application par la Loi le 25 mai 2018, impose aux organisations, dans son article 32, de mettre en œuvre toutes les mesures de sécurité relatives à la protection des données, afin de protéger les citoyens contre la fuite, la destruction ou la corruption de leurs données [2]. Les amendes en cas de manquement sont non négligeables (entre 400 000 et 600 000 euros prononcés contre des hôpitaux européens, 30 000 euros contre l'Office HLM de la Métropole de Rennes, 204 millions d'euros pour British Airways, 20 millions d'euros pour le Groupe Marriott…).

Alors quels intérêts pour les pirates ? Ils sont multiples : extraire les données pour les revendre sur le marché noir de l'internet (et rassurez-vous, il y a de nombreux acheteurs !), exercer un chantage financier sur l'institution dont les données ont été volées (et qui pèsera le pour et le contre entre le paiement du chantage ou celui de l'amende, de l'atteinte à l'image et des éventuelles poursuites engagées par des citoyens fâchés de voir leur vie privée et leur dossier médical s'étaler sur les réseaux sociaux), utiliser les données dérobées pour fabriquer de fausses identités, de faux documents, voire pour s'en prendre directement aux personnes physiques (le vol de plus de 25 000 dossiers de psychiatrie en Finlande en 2020 a donné lieu à des prises de contact et à des chantages directs auprès des patients, sur le mode « *j'ai votre dossier psychiatrique devant moi, alors c'est 1 000 euros ou je le publie et informe votre famille et votre employeur* »). Comme le disait Claude Lelouch dans *Hommes, Femmes, mode d'emploi* : « *Le pire n'est jamais décevant* » !

L'organisation politique et l'analyse des incidents de sécurité

L'article L.1111-8-2 du code de la santé publique institue l'obligation de signalement des incidents de sécurité des systèmes d'information (SI). Le décret d'application n°2016-1214 du 12 septembre 2016 précise que les incidents graves de sécurité des SI du secteur santé doivent être signalés sans délai à compter du 1er octobre 2017 pour les établissements de santé, les hôpitaux des armées, les centres de radiothérapie et les laboratoires de biologie médicale [3]. Enfin, l'arrêté du 30 octobre 2017 présente les modalités de signalement et de traitement des incidents graves de sécurité des SI [4]. L'objectif de ce processus de signalement est double : recenser les incidents et leur typologie afin de factualiser la situation et d'adapter la riposte, accompagner, le cas échéant, les structures en difficulté, comme cela a pu être le cas pour le centre hospitalier universitaire de Rouen ou l'hôpital de Villefranche-sur-Saône. Il est probable que ce dispositif s'étende encore, ce qui serait normal, tant pour la surveillance cyber de notre système de santé que pour l'information transparente des usagers. En complément de ces dispositions, le président de la République a annoncé, en février 2021, l'accélération du déploiement du « service national de cybersurveillance en santé » en partenariat avec l'Agence du numérique en santé (ANS) et le développement des moyens du dispositif « cyberveille en santé » pour augmenter les capacités de réaction et d'appui aux structures en cas d'incidents ou de cyberattaques. Encore trop d'établissements restent « frileux » à déclarer un incident de sécurité, habités par un sentiment de honte ou une peur de mauvaise publicité. Il faut dépasser ce sentiment naturel et entrer définitivement dans une dynamique de transparence et de coopération. Ce qui arrive aux uns arrivera aux autres et aucune autorité ne considère aujourd'hui qu'une cyberattaque est la conséquence a priori d'un manquement. Les déclarations constituent un indicateur factuel et performant, et contribuent clairement à faire progresser l'écosystème.

Lors des annonces du président de la République, la formation des professionnels de santé aux bons usages des technologies numériques et à la cybersécurité est annoncée comme essentielle et prioritaire. La sensibilisation à la cybersécurité sera intégrée dans tous les cursus de formation des acteurs en santé afin de conforter les pratiques « d'hygiène numérique » dans un contexte de renforcement de la convergence et de l'interopérabilité des SI comme de la fluidité du parcours ville-hôpital. Il est grand temps de corriger cette anomalie qui a consisté depuis 15 ans à mettre entre les mains des soignants et des agents publics en général des voitures de course sans leur avoir fait passer ni le Code de la route, ni le permis de conduire.

L'humain est et restera le meilleur moyen d'assurer au système de santé un haut niveau de sécurité, en le formant à la vigilance, un juste milieu entre la naïveté et la paranoïa !

Le responsable de la sécurité des systèmes d'information : pièce maîtresse du dispositif de lutte contre la malveillance

Longtemps considéré comme un « geek[1] » un peu paranoïaque, le responsable de la sécurité des systèmes d'information (RSSI) est en passe d'être enfin reconnu comme pièce maîtresse du dispositif de maîtrise du SI et de lutte contre les multiples menaces internes et externes. Il devient essentiel de lui donner une existence et un soutien, par un courrier de nomination explicite, signé de la direction générale et largement diffusé, une indépendance, par son rattachement à une direction « neutre » (qualité, juridique ou générale), et des moyens, avec le souhait ministériel d'une meilleure prise en compte de la cybersécurité dans tous les projets de SI.

Les discussions sur le positionnement du RSSI ne sont pas récentes, et ce dans tous les secteurs d'activité. On peut raisonnablement acter deux principes : le RSSI doit pouvoir exercer, c'est-à-dire travailler pour le compte de l'institution qu'il sert avec tout le soutien nécessaire des autorités administratives et cœur de métier ; le RSSI doit pouvoir assurer un rôle de conseil et de contrôle des pratiques de la direction des systèmes d'information (DSI), en bonne intelligence et dans le cadre d'objectifs partagés.

Enfin, dans sa communication du 22 février 2021, le ministère des Solidarités et de la Santé précise : « *Face à l'augmentation de la menace, il n'est plus possible de faire de la cybersécurité une variable d'ajustement des projets informatiques des établissements de santé. Ainsi, aucun projet ne pourra désormais faire l'objet d'un soutien de la part de l'État si une part de à 5 à 10% de son budget informatique n'est pas dédiée à la cybersécurité* » [5]. Après tout, lorsque l'on achète une voiture, les freins et les ceintures de sécurité ne sont pas des options ! Cette règle devrait naturellement s'imposer à tout projet numérique, quel que soit son porteur.

Mettre en œuvre une politique de sécurité exigeante

Politique de sécurité des systèmes d'information (PSSI) et analyse des risques constituent les deux fondements de la mise en œuvre stratégique et opérationnelle d'un programme de sécurité global. En ce qui concerne les analyses des risques, la réalité impose

1- Anglicisme. Personne passionnée par les nouveautés techniques, et particulièrement par l'informatique, l'internet, les jeux vidéo (Source : Le Robert).

la nécessité de faire évoluer les modèles existants, basés sur des fichiers Excel® (Microsoft, Redmond, États-Unis) et la méthode EBIOS®[2] 2010, et de mettre en œuvre un cycle de vie opérationnel et efficient. L'Agence nationale de la sécurité des systèmes d'information (Anssi) recommande maintenant l'usage de la méthode EBIOS® Risk Manager, qui adopte une approche de management du risque numérique partant du plus haut niveau (grandes missions de l'objet étudié) pour atteindre progressivement les fonctions métier et technique, par l'étude des scénarios de risque possibles. C'est une petite révolution conceptuelle et les structures de santé vont devoir réviser ce volet de la gestion des risques, en intégrant cette nouvelle méthode et en s'outillant avec des outils labellisés et adaptés aux enjeux.

PSSI, analyse des risques, chartes, gestion des habilitations, puis des droits, traçabilité, supervision, sauvegardes testées, plan de continuité d'activité, intégration de la sécurité dans les projets sont autant de thématiques que l'on retrouve dans l'ISO 27001. Si l'on ajoute le respect non négociable du RGPD, qui exige des mesures de sécurité adaptées à la criticité des données et des traitements, donc des processus, et les textes français et européens qui qualifient les données à caractère personnel d'ultra-sensibles, on converge vers la nécessité d'une certification officielle. Alors pourquoi ne pas exiger des SI des établissements de santé qu'ils soient certifiés ISO 27001 et ISO 27701, pour le moins sur le périmètre d'exploitation ? Le SI serait ainsi certifié, comme d'autres processus (les laboratoires de biologie par exemple) et soumis à un plan d'amélioration continu régulièrement challengé. Le futur référentiel Maturin-H, en cours d'élaboration par le ministère et les représentants des grandes organisations de la santé, devra répondre à ces enjeux.

L'avenir est-il dans le *cloud* ?

Lors du discours que l'on peut qualifier d'historique du 17 mai 2021, les trois ministres Bruno Lemaire, ministre de l'Économie, des Finances et de la Relance, Amélie de Montchalin, ministre de la Transformation et de la Fonction publique et Cédric O, secrétaire d'État chargé de la transition numérique et des communications électroniques ont décliné la stratégie « *cloud* » de l'État. À l'intérieur même de la révolution numérique, il existe des « sous-révolutions ». La première fut l'avènement du PC[3], la seconde celle de l'internet et la troisième est celle du « *cloud computing* », c'est-à-dire de l'informatique en nuage. Lors de cette intervention, les ministres ont posé la doctrine et déclaré : « *Cette nouvelle doctrine s'applique aux ministères et organismes placés sous leur tutelle, et s'incarnera dans une circulaire. Le cloud devient dorénavant la méthode d'hébergement par défaut pour les services numériques de l'État, pour tout nouveau produit numérique et pour les produits connaissant une évolution substantielle. Les recrutements et les programmes de formation continue destinés aux agents de l'État dans la filière numérique comporteront un volet cloud* » [6].

On peut aisément en déduire que l'État en général et le système de santé dans la continuité vont entrer dans un processus d'externalisation de leur informatique traditionnelle, et donc sous-traiter l'ensemble des couches informatiques : hébergement du *hardware* et donc des données auprès d'opérateurs spécialisés et reconnus, usage de logiciels métier à distance en mode SaaS[4], utilisation de technologies de sécurité externalisées. Les établissements de santé, progressivement, n'auront plus à gérer qu'un parc d'ordinateurs et d'imprimantes, une liaison réseau fibre optique de qualité, et l'ensemble des services sera opéré par des industriels dont c'est le métier. Nous suivrons ainsi le modèle des États-Unis, du Canada, du Royaume-Uni, de la Corée du Sud… où l'immense majorité des entreprises privées, des hôpitaux et des collectivités ont depuis longtemps procédé à un recentrage sur leurs cœurs de métier et ont confié la gestion de leurs systèmes d'information à des opérateurs privés. C'est alors que le débat sur notre souveraineté prend tout son sens, avec le nécessaire recours à des opérateurs français ou européens, malgré les offres alléchantes et parfois, disons-le, efficaces et modernes des géants américains et chinois tels Microsoft (Richmond, États-Unis), Amazon (Seattle, États-Unis), Google (Mountain View, États-Unis) ou Huawei (Shenzhen, Chine) par exemple. ■

2- EBIOS : Expression des besoins et identification des objectifs de sécurité (marque déposée par le secrétariat général de la Défense et de la Sécurité nationale).

3- *Personal computer*, ordinateur personnel.

4- *Software as a service*, logiciel en tant que service : modèle d'exploitation commerciale des logiciels dans lequel ceux-ci sont installés sur des serveurs distants plutôt que sur la machine de l'utilisateur (d'après Wikipédia).

Références

1- Le club des juristes. Le droit pénal à l'épreuve des cyberattaques. Paris, 2021. 90 p. Accessible à : https://www.leclubdesjuristes.com/wp-content/uploads/2021/04/rapport_cyberattaques_DEF2_WEB.pdf *(Consulté le 7-12-2021)*.

2- Commission nationale de l'informatique et des libertés. Le règlement général sur la protection des données – RGPD. 23 mai 2018. Accessible à : https://www.cnil.fr/fr/reglement-europeen-protection-donnees *(Consulté le 6-12-2021)*.

3- Décret n° 2016-1214 du 12 septembre 2016 relatif aux conditions selon lesquelles sont signalés les incidents graves

de sécurité des systèmes d'information. JORF n° 0214 du 14 septembre 2016. Accessible à : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033117678 *(Consulté le 6-12-2021)*.
4- Arrêté du 30 octobre 2017 relatif aux modalités de signalement et de traitement des incidents graves de sécurité des systèmes d'information. JORF n°0261 du 8 novembre 2017. Accessible à : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000035986261/ *(Consulté le 6-12-2021)*.
5- Ministère des Solidarités et de la Santé. Sécurité des réseaux informatiques des établissements de santé : le gouvernement renforce sa stratégie [internet]. Paris, 22 février 2021. Accessible à : https://solidarites-sante.gouv.fr/actualites/presse/communiques-de-presse/article/securite-des-reseaux-informatiques-des-etablissements-de-sante *(Consulté le 6-12-2021)*.
6- Ministère de l'Économie, des Finances et de la Relance. Bruno Le Maire, Amélie de Montchalin et Cédric O ont présenté la stratégie nationale pour le cloud [vidéo]. 17 mai 2021. Accessible à : https://www.economie.gouv.fr/cloud-souverain-17-mai *(Consulté le 6-12-2021)*.

Citation
Trely V. Cyberattaques : pourquoi le monde de la Santé est-il une cible ? Risques & Qualité 2021;(18)4;214-218.

Historique
Reçu 4 décembre 2021 – Accepté 8 décembre 2021 – Publié 17 décembre 2021

Financement : l'auteur déclare ne pas avoir reçu de financement.

Liens d'intérêt : l'auteur déclare ne pas avoir de lien d'intérêt.

R&Q
www.risqual.net