AVIS D'EXPERT

LES HÔPITAUX SERONT-ILS UN JOUR ÉPARGNÉS PAR LA MENACE CYBER ?

Victor Poitevin
Editorial & Digital Manager, Stormshield

Le volume des incidents de sécurité des établissements de santé s'est envolé entre 2020 et 2021 : 35% d'augmentation aux États-Unis, 45% en Espagne et jusqu'à 50% en Allemagne et en France... Une situation critique quand ces environnements sensibles ont besoin en moyenne de 28 jours pour retrouver une activité normale. Malgré les aides et l'accompagnement apportés notamment par les États, pourquoi les centres hospitaliers sont-ils encore aujourd'hui vulnérables ?

Analyse et réaction d'experts sur un phénomène qui inquiète professionnels de santé et grand public.

DES INITIATIVES POUR FAIRE FACE À LA MENACE CYBER

La fragilité des établissements de santé a été mise en lumière par la pandémie de Covid-19, début 2020. Les centres hospitaliers sont alors frappés et paralysés par des cyberattaques presque quotidiennement sans distinction de taille ou de lieu géographique. L'AP-HP en mars 2020, Dax, Oloron-Sainte-Marie et Villefranche-sur-Saône en février 2021, Arles en août 2021, le GHT Cœur Grand-Est en avril 2022, ou encore Corbeil-Essonnes plus récemment en août 2022. Une liste qui semble interminable…

Pour autant, **la vulnérabilité des établissements de santé n'est pourtant pas une nouveauté et préoccupe les professionnels depuis plus d'une décennie**. Une première initiative pour parler de cybersécurité des établissements de santé voit le jour en France dès 2011, dans la ville du Mans. Avec le souhait de se rencontrer et d'échanger, le premier Congrès National de la Sécurité des Systèmes d'Information de Santé est organisé sous l'impulsion de **Vincent Trely**, RSSI du CHU du Mans. En 2013, toujours en France, la Loi de programmation militaire (LPM) consacre la notion d'OIV (opérateurs d'importance vitale). Un acronyme qui catégorise alors un ensemble d'entreprises et d'organisations ayant un caractère indispensable à la survie de la nation. Même si la liste ne sera pas diffusée publiquement, de premiers grands hôpitaux y sont alors intégrés. La même année, l'American Association Hospital (AHA) commence à publier des alertes et des rapports sur les cyberattaques ciblant les établissements de santé sur le territoire américain. Quelques années plus tard, en juillet 2016, la directive NIS (*Network and Information Security*) est adoptée au niveau européen (avant sa deuxième version, NIS2). Elle prévoit notamment le durcissement de la cybersécurité d'opérateurs issus de secteurs clés, à travers la création de la notion d'OSE (opérateurs de services essentiels), un autre acronyme qui viendra compléter celui des OIV. En 2017, la refonte des Groupements de Coopération Sanitaire (GCS) des établissements de santé français permet de faciliter et développer les échanges entre RSSI des groupements de santé.

La prise de conscience semble donc relativement ancienne, tout du moins au niveau des professionnels du secteur de la santé (comme les RSSI ou encore l'ANSSI). **De quoi assurer une certaine protection face aux menaces cyber ?** Malheureusement, la crise sanitaire et l'explosion des cas de cyberattaques contre des hôpitaux ont eu raison de cet optimisme. Selon l'analyste américain **Brett Callow,** près de 170 attaques de ransomware ont infecté près de 1 800 cliniques et établissements de santé aux États-Unis sur la période 2020-2021. En France, l'ANSSI relevait en moyenne un incident par semaine dans un établissement de santé en 2021 et annonçait que 27 établissements avaient été victimes d'une cyberattaque sur cette même période. Un triste record.

En réaction à ces nouvelles attaques, le secteur se mobilise de nouveau. Dès février 2020, certaines entreprises privées de cybersécurité mettent en place gratuitement des actions de soutien aux établissements de santé. En parallèle, l'ENISA publie un guide qui recense les 10 bonnes pratiques à mettre en œuvre au sein des établissements de santé pour faire face aux cyber-menaces. Puis, en mars 2020, plus de 3 000 professionnels de la cybersécurité se regroupent sous le nom de COVID-19 Cyber Threat Coalition, dans le but d'échanger autour d'analyses et d'indicateurs de compromission. Des flux de Threat Intelligence sont alors produits bénévolement et partagés au travers de la communauté. En septembre 2020 ensuite, l'État français se dote d'un fonds de 136 millions d'euros avec le plan France Relance, dont le volet cybersécurité a pour objectif d'augmenter la sécurité des infrastructures critiques comme celles des établissements de santé. Quelques mois plus tard, le ministère de la Santé augmente ce budget de 350 millions d'euros pour les hôpitaux. En avril et en juin 2021, l'État allemand publie une ordonnance ayant pour but de contraindre les prestataires de services utilisant des infrastructures critiques, dont les hôpitaux, à se conformer à un durcissement de leur cybersécurité tandis que les autorités françaises intègrent de leur côté 135 groupements hospitaliers à la liste d'opérateurs de services essentiels (OSE). Enfin, en août 2022, le gouvernement français annonce un budget supplémentaire de 20 millions d'euros à l'ANSSI afin de renforcer l'accompagnement des établissements de santé.

Face à la menace cyber, les établissements hospitaliers ne sont donc pas seuls. Mais est-ce suffisant ?

POURQUOI LES HÔPITAUX SONT-ILS ENCORE VULNÉRABLES ?

Devant de tels moyens, accompagnements et initiatives, les établissements de santé restent vulnérables. Mais pourquoi ? Dans les faits, **la raison majeure semble simple tant la surface d'attaque des hôpitaux est conséquente.**

Le renouvellement du matériel informatique dans les environnements de santé génère de premières contraintes. Lorsqu'un équipement informatique classique est renouvelé tous les 5 ans, les dispositifs médicaux ont des modèles de rentabilité pouvant atteindre une quinzaine d'années de fonctionnement. De ce fait, les systèmes intègrent aujourd'hui des technologies en fin de vie qui ne sont plus maintenues. « *Ces investissements de plusieurs dizaines ou centaines de milliers d'euros se font sur dix ou quinze ans,* explique **Charles Blanc-Rolin,** ancien RSSI d'établissement de santé et chef de projet sécurité numérique en santé au GCS e-santé Pays de la Loire. *Il n'est pas rare de retrouver des systèmes Windows, ou Windows XP qui n'est plus supporté depuis 2014. Parfois même avec des versions de Windows encore plus anciennes et sur lesquelles il n'existe plus de correctif de sécurité. On se retrouve avec de vraies passoires et des systèmes très vulnérables. À cela s'ajoute le marquage CE, qui est réglementaire pour le constructeur. Mais qui est aussi contraignant pour l'établissement de santé, qui ne peut pas appliquer de modification sur ce dispositif, comme une mise à jour de correctif de sécurité, sans perdre ce marquage CE* ». Dans le but de prévenir le risque d'utilisation de systèmes d'exploitation non maintenus, les politiques de sécurité informatique doivent,

au contraire, pouvoir s'adapter, comme le souligne Charles Blanc-Rolin : « *c'est important de mettre en place un plan de continuité d'activité et un plan de reprise d'activité mais il est également primordial d'avoir des procédures dégradées. Aujourd'hui, on met beaucoup d'outils de sécurité, mais on en oublie les bases et la nécessaire souplesse à avoir.* »

« Il n'est pas rare de retrouver des systèmes Windows, ou Windows XP qui n'est plus supporté depuis 2014. Parfois même avec des versions de Windows encore plus anciennes et sur lesquelles il n'existe plus de correctif de sécurité. »

Charles Blanc-Rolin, chef de projet sécurité numérique en santé au GCS e-santé Pays de la Loire

En parallèle, **les hôpitaux sont soumis à une numérisation à marche forcée depuis plus d'une décennie,** générant d'autres contraintes. **Jean-Sylvain Chavanne**, RSSI du CHU de Brest et du Groupement Hospitalier de Territoire de Bretagne Occidentale, détaille : « *pour donner un exemple, le périmètre à sécuriser pour le CHU de Brest est composé de 140 applications métiers, 350 serveurs virtuels, 6 000 postes de travail, 10 000 objets connectés sur le réseau, 20 000 équipements biomédicaux (comme des pousses-seringues, des IRM, des caissons hyperbars…), 2,7 pétaoctets de stockage de données brutes à sauvegarder. Ce qui en fait un périmètre très large. En parallèle de cela, les centres hospitaliers ont connu une numérisation à marche forcée depuis les années 2010, financée par une succession d'appels à projets, sans budgets associés pour les maintenir. Mécaniquement, les hôpitaux se retrouvent avec une grosse dette technique qu'il faut rattraper au fur et à mesure.* » Dans le prolongement de cette numérisation, **les établissements de santé se sont vus également fragilisés par la démocratisation des produits connectés**. La médecine et ses usages évoluant sans cesse et les domaines de l'imagerie médicale, de l'hospitalisation à domicile ou encore de l'identification des patients ont été bouleversés par ces innovations comme le rappelle Charles Blanc-Rolin : « *avec les nouveaux usages, comme le tracking patient avec des bracelets RFID, on peut savoir exactement où se situe le patient au sein d'un hôpital pour améliorer son parcours de soins. Il faut donc cadrer ses nouveaux usages numériques et ajouter une couche de sécurité sans engendrer de dette technique* ». Du fait de la multiplication de ces objets dans les services de santé, l'élargissement non contrôlé de la surface d'attaque est un problème que Jean-Sylvain Chavanne analyse au travers de trois risques majeurs : « *Le premier risque, est la non-maîtrise des objets connectés qui sont déployés dans un système d'information hospitalier. C'est le cas d'un fournisseur qui arrive et se branche sur le réseau sans mesure de sécurité mise en œuvre. Le deuxième risque se trouve dans les relations contractuelles. Sans contrat avec des sous-traitants ou des fournisseurs, aucune obligation de sécurité n'est exigée, comme la mise à jour des logiciels concernés. Et enfin, le troisième risque, ce sont les logiciels embarqués eux-mêmes, véritables "boîtes noires". Si nous ne savons pas ce qu'ils contiennent, nous ne pouvons pas maîtriser la sécurité et patcher les vulnérabilités. En décembre dernier, c'est arrivé avec Log4Shell, où nous avons dû contacter 200 fournisseurs d'équipements médicaux pour savoir si leur logiciel l'embarquait ou non.* »

« Les centres hospitaliers ont connu une numérisation à marche forcée depuis les années 2010, financée par une succession d'appels à projets, sans budgets associés pour les maintenir. Mécaniquement, les hôpitaux se retrouvent avec une grosse dette technique qu'il faut rattraper au fur et à mesure. »

Jean-Sylvain Chavanne, RSSI du CHU de Brest

Mais l'humain est également un facteur de vulnérabilité dans les hôpitaux. Soumis à un manque d'effectif, les équipes informatiques sont concentrées sur l'objectif de fournir rapidement l'information. Au risque parfois de s'affranchir des règles de sécurité évidentes. C'est dans ce cadre que les équipes SSI des centres hospitaliers sensibilisent le personnel et reviennent parfois sur des libertés que les professionnels de santé n'auraient pas dû avoir et qu'il faut déconstruire, comme l'analyse Jean-Sylvain Chavanne : « *Actuellement, nos équipements de sécurité bloquent un spam toutes les 50 secondes et un virus toutes les heures. Il faut sensibiliser et éduquer sur le fait que nous n'avons pas une pleine liberté d'utilisation des logiciels qui stockent et gèrent des données de santé. Par exemple, le personnel médical ne doit pas avoir les diagnostics de leurs patients sur leur téléphone personnel. Nous rappelons les bonnes pratiques tout au long de l'année.* » Un personnel médical sous pression constante, qui a tendance à prendre des raccourcis pour se concentrer sur son métier de soin, et qu'il faut rendre réceptif au sujet de la cybersécurité. Un vrai défi pour les RSSI, qui peuvent s'inspirer de la communication qu'un directeur d'hôpital parisien a adressé à ses collaborateurs.

Obsolescence du matériel, culture du risque à parfaire, problématique de recrutement ; il reste encore de nombreux points à régler au sein des établissements hospitaliers pour assurer une réelle cybersécurité de ces infrastructures vitales.

VERS UN FRONT ÉLARGI DE LA MENACE CYBER AUTOUR DE LA DONNÉE DE SANTÉ

Au regard de ces différentes difficultés, Charles Blanc-Rolin souligne que **l'enjeu vital de la sécurité des établissements de santé concerne la donnée des patients et leur prise en charge.** « *Les cyberattaques par ransomware notamment peuvent paralyser un hôpital et diminuer les chances de prise en charge des patients. Les soignants, sans accès aux données ni aux diagnostics, devront faire de la médecine de guerre. Ce qui induit une dégradation de la qualité de soin. C'est là, le vrai danger.* »

« Les soignants, sans accès aux données ni aux diagnostics, devront faire de la médecine de guerre. Ce qui induit une dégradation de la qualité de soin. C'est là, le vrai danger. »

Charles Blanc-Rolin, chef de projet sécurité numérique en santé au GCS e-santé Pays de la Loire

Mais les données de santé ont en parallèle un autre intérêt pour les cyber-criminels. Au-delà du caractère personnel et usuel de certaines données comme le nom, prénom et date de naissance, ces données peuvent parfois contenir un aspect bien plus personnel pouvant engendrer des scénarios de demandes de rançons terrifiantes pour les victimes elles-mêmes. C'est précisément ce qui est arrivé aux patients de la société Vastaamo durant l'année 2020. Ce regroupement de 25 centres de psychothérapie en Finlande a été victime d'une fuite de données, contenant le suivi psychiatrique de ces patients. Comme le rapportait VICE, 30 000 patients avaient ainsi reçu une demande de rançon à régler sous 24h sous peine de divulgation. Une évolution dans la méthode des cyberattaques, où la rançon est la plupart du temps associée à une entreprise. Mais dans ce cas, les patients se sont retrouvés en première ligne. Plus de 25 000 plaintes ont été déposées auprès des autorités, faisant de cette cyberattaque la plus grande affaire criminelle de l'histoire de la Finlande. Quelques mois plus tard, l'autorité finlandaise de protection des données infligera à l'entreprise une amende de 608 000 € pour avoir enfreint le règlement général sur la protection des données. La France ne sera pas épargnée, puisqu'à la même période, 500 000 dossiers médicaux furent dérobés à un groupement de laboratoires de l'ouest de la France. Selon une étude américaine de mars 2022, **les données de santé auraient une valeur 25 fois supérieure à celle d'une carte de crédit.**

Si les données de santé sont une manne financière pour les cyber-criminels, les données de l'univers de la santé peuvent être un objectif de puissances étatiques. Obtenir des informations sur le développement de vaccin lors de la crise sanitaire a ainsi été une priorité pour certains pays ne disposant pas de moyens de recherche et développement. Selon le *Wall Street Journal,* pas moins de six entreprises pharmaceutiques incluant Johnson & Johnson et Novavax Inc auraient été ciblées à la même période par des cyber-activistes Nord-Coréens. À la fin de l'année 2020, ce même groupe, en se faisant passer pour un cabinet de recrutement, aurait approché les salariés de l'entreprise Astrazeneca à l'aide de fausses offres d'emploi dans le but de faire transiter au sein de l'entreprise des documents contenant des charges malicieuses. Cette même année, en France, sur 24 incidents comptabilisés dans le secteur de la santé, sept concernaient l'industrie pharmaceutique, d'après **Charlotte Drapeau,** cheffe du bureau Santé et Société au sein de l'ANSSI. Une tendance de fond selon le *HIPAA Journal* : le nombre de brèches majeures concernant des vols de données de santé est passé aux États-Unis de 368 en 2018 à 714 en 2021.

Pour Jean-Sylvain Chavanne, l'ensemble des cyberattaques ayant ciblé les laboratoires pharmaceutiques français ne sont pas l'œuvre de cyber-criminels classiques : « *Tous les établissements pharmaceutiques Français qui ont développé un vaccin contre la Covid-19 ont été victimes d'une cyberattaque. Devant un tel constat, il est difficile de se dire que c'est ici le résultat d'actions opportunistes des attaquants. On est ici dans un souhait de déstabilisation ou d'espionnage industriel.* »

Les raisons de la vulnérabilité des établissements de santé sont donc complexes. Héritées de problématiques structurelles au secteur, elles ne pourront certainement pas être résolues en quelques mois. Pour effacer les dettes techniques, répondre aux problèmes de sous-effectif ou encore réduire la surface d'attaque, le secteur de la santé doit agir dès à présent. Et pour cela, il peut compter sur le soutien des États. Pour (re) faire de l'hôpital un espace connecté et sécurisé.

STORMSHIELD

Stormshield, filiale à 100% d'Airbus CyberSecurity, propose des solutions de sécurité de bout-en-bout innovantes pour protéger les réseaux (Stormshield Network Security), les postes de travail (Stormshield Endpoint Security) et les données (Stormshield Data Security).

www.stormshield.com

Version 1.1 - Copyright Stormshield 2023