Face au risque cyber

Quelle priorité pour renforcer la cyber-résilience SI à l'hôpital ?

« Celui qui excelle à résoudre les difficultés le fait avant qu'elles ne surviennent. » Sun Tzu

Béatrice BÉRARD Officier de sécurité des systèmes d'information, Hospices civils de Lyon, GHT Rhône Centre
Cédric CARTAU Responsable de la sécurité des systèmes d'information, délégué à la protection des données, CHU de Nantes, GHT44
Christine PICHON Directrice des systèmes d'information, CHU de Rennes
Guilhem SAVEL Responsable de la sécurité des systèmes d'information, CHU de Bordeaux, GHT Alliance de Gironde
Hugo AGUADO Directeur du numérique et du système d'information hospitalier, CH de Perpignan
Jacques LABIDURIE Responsable de la sécurité des systèmes d'information, CHU de Limoges, GHT du Limousin
Julien BERTHEL Directeur des systèmes d'information, CHRU de Tours, GHT Touraine Val de Loire
Philippe LECA Directeur des systèmes d'information CHU de Lille, GHT Lille Métropole Flandre Intérieure

En matière de cyberattaque, la seule question à se poser est : quand la subirons-nous ? Si les attaques sont inévitables, que faisons-nous pour diminuer le risque de survenance et ses impacts ? Et que faire, « en plus », sachant que la menace est omniprésente ? Cet article est consacré à la capacité d'un établissement ou d'un GHT à renforcer la cyber-résilience de son équipe dédiée au système d'information (SI). Plus globalement, et considérant que la sécurité SI est l'affaire de tous, il conviendrait également de concevoir des actions de sensibilisation régulière, voire des plans de formation spécifiques dédiés aux utilisateurs du SI afin qu'ils s'approprient les bons comportements. Et de façon à renforcer la résilience fonctionnelle, il est essentiel d'implémenter des exercices cyber avec une implication métiers qui permettent de réviser ou de mettre au point leurs modes dégradés. Ces axes, et d'autres, pourraient faire l'objet de prochains articles.

En mai 2017, WannaCry[1], une cyberattaque mondiale massive, jette les bases d'une nouvelle forme de menace à caractère multiforme. Son impact sur le système de santé du Royaume-Uni (UK's National Health Service NHS) sera puissant.

Ces derniers mois, en France et dans le monde, les cyberattaques ont défrayé la chronique. Les centres hospitaliers de toute taille n'ont pas fait exception à la règle : Rouen, Albertville, Dax, Narbonne, Villefranche-sur-Saône, Paris… À la différence des autres secteurs d'activité, l'impact de ces attaques touche directement la prise en charge sanitaire des patients. Et peut même occasionner des situations dramatiques.

Des cybermenaces qui s'adaptent

Depuis 2017, les hôpitaux ont largement ouvert l'accès à leurs données pour les partager, les échanger et les rendre aisément accessibles aux usagers et professionnels de santé. En parallèle, les modes d'attaque ont évolué. L'avènement de l'Internet haut débit et l'exposition croissante des applications sur Internet (applications métiers, e-mail, extranet, intranet) y ont largement contribué. Certaines de ces attaques visent à détruire des données (virus, *malwares*), voler des moyens d'accès (hameçonnage ou *phishing*), d'autres ont pour cible les infrastructures (attaque par déni de service) ou le vol de données (injection SQL). Certaines méthodes, plus pernicieuses encore, prennent en otage les données des établissements (*ransomwares*) et pratiquent un chantage à la divulgation.

Ces pratiques ne vont pas s'atténuer. La valeur marchande des informations que produit l'hôpital suscite sur le marché noir d'Internet (*darknet*), où des données patient s'y monnaient autour de 250 $, un réel intérêt.

Nous avons changé de paradigme

Pour répondre aux besoins d'informatisation des services et souvent à effectifs constants, nous avons augmenté le périmètre fonctionnel, augmenté les interconnexions, augmenté les systèmes à maintenir à jour, autorisé des accès distants et donc augmenté le périmètre à sécuriser.

Il ne faudrait pas croire que votre équipe dédiée au système d'information ne fait rien[2], ne s'inquiète pas, ne consacre pas une part de son budget et de son temps à traiter le problème. Bien au contraire. Depuis plusieurs années, votre équipe SI dédie une partie de ses activités à maintenir vos activités professionnelles en sécurité. Elle a installé des antivirus pour protéger les postes et les messages électroniques, des *firewalls* pour filtrer les flux d'échanges d'informations – qu'ils proviennent de l'extérieur ou l'intérieur de vos sites – et cloisonné les réseaux informatiques. Elle a appliqué des règles d'accès et des moyens d'authentification, des bastions pour contrôler la nocivité des pièces jointes et elle a limité les accès à certains sites sur Internet. Pourtant, est-ce suffisant ?

Le changement de paradigme vient du changement de comportement des cybercriminels. Leur objectif est d'exploiter de multiples failles et d'agir sur les maillons faibles pour prendre le rôle d'administrateur du système. Nous faisons face, désormais, à des adversaires qui viennent sur notre terrain avec des moyens d'action et des techniques en constante évolution.

Dès qu'un éditeur communique sur une faille de sécurité, ce qu'il accompagne généralement d'un correctif, une course de vitesse s'engage entre les hackers et la DSI de l'établissement de santé. Le premier exploite la faille de sécurité pour introduire son *malware*. Le second déploie le correctif sur l'ensemble de ses postes ou serveurs. Le problème réside dans le délai, de plus en plus rapide, pour exploiter une faille de sécurité. Autrement dit, le délai de réactivité laissé à votre équipe, pour protéger vos actifs, a considérablement diminué.

Cette menace en mutation constante prend la forme d'un nouveau risque à couvrir. Elle questionne la capacité de nos systèmes à être cyber-résilients. Prendre conscience de la nécessité de couvrir ce nouveau risque ne met pas un établissement de santé à l'abri d'une attaque. Elle permet en l'anticipant de savoir réagir et de diminuer les impacts.

Comment aider les équipes SI à maintenir le SIH cyber-résilient ?

À l'échelle nationale, directives et incitations financières ne manquent pas. Le programme Hop'En puis l'aide du Ségur du numérique (SUN-ES) intègrent dans leurs prérequis des actions visant au renforcement de la sécurité. L'instruction n°SG/DSSIS/2016/309 du 14 octobre 2016 comporte un plan d'actions à six, douze et dix-huit mois pour l'application des mesures prioritaires de niveaux 1, 2 et 3. Dernièrement, l'Agence nationale de la sécurité des systèmes d'information (ANSSI), de concert avec les ministères, a décidé en avril 2021 d'élargir la liste d'opérateurs de services essentiels (OSE) aux centres hospitaliers de taille importante, proposant en appui une démarche d'accompagnement au titre du plan France relance.

Dès qu'un éditeur communique sur une faille de sécurité, ce qu'il accompagne généralement d'un correctif, une course de vitesse s'engage alors entre les hackers et la DSI. Le délai de réactivité laissé à votre équipe SI, pour protéger vos actifs, a considérablement diminué.

Toutes ces mesures incitatives vont dans le bon sens. Nous savons ce qu'il faut faire, comment le faire et pouvons bénéficier d'aides financières. Dès lors, pourquoi rencontrons-nous encore d'énormes difficultés à exécuter tous nos plans d'actions ?

Chaque année, il faut prioriser les ressources dédiées au système d'information. Entre la fourniture de nouvelles applications, la mise à niveau des outils attendus par nos utilisateurs et l'investissement dans la sécurité, c'est le principe des vases communicants. Nous savons qu'il faut renforcer la sécurité mais nous devons aussi répondre aux besoins de l'établissement. Ce constant travail de priorisation est très dépendant du prisme utilisé par les instances d'arbitrage des projets au sein des établissements. La continuité des efforts en est parfois affectée, lorsque les réallocations de ressources sont soumises à la priorité du moment.

Comme indiqué *supra*, face à une menace en constante évolution, nous devons aborder la cyber-résilience comme un processus qualité. Il n'y a pas de choix à

1. https://fr.wikipedia.org, WannaCry.
2. https://cyberguerre.numerama.com, 9 sept.2021 https://cyberguerre.numerama.com/13210-si-les-hopitaux-se-font-attaquer-cest-parce-que-leur-securite-est-nulle.html

MOYENS À ENGAGER POUR ATTEINDRE UN NIVEAU DE SÉCURITÉ SATISFAISANT, ET SON MAINTIEN TABLEAU 1

Pour un GHT théorique ayant un parc de **10000 postes de travail**.
Les donnés présentées ont une marge +/- 20%.
La proportionnalité permet à chacun de se positionner par rapport à cette matrice.

Médiane	Atteindre le niveau	Maintenir le niveau
Moyens financiers	Non modélisable[1]	667 K€/an 556 K€ / an[2] 445 K€/an
Moyens humains	1560 JH 1300 J/H 1040 JH	1320 jh/an 1100 JH / an[3] 880 jh/an

1) Doit faire l'objet d'un audit spécifique pour chaque GHT/Etablissement.
2) Couvre les prestations et maintenances
3) Soit 5 ETP sur la base de 220 J/ETP.

Source : juin 2021, CNSI, GT - DSI/RSSI, "Étude des moyens financiers et humains pour la protection cyber des SI hospitaliers".

effectuer entre les projets et la sécurité. Les ressources dédiées à la sécurité devront rester pérennes. En 2021, une étude, menée pour la conférence nationale des directeurs généraux de CHU par des représentants des directions de systèmes d'information et des responsables de la sécurité des systèmes d'information d'établissements hospitaliers publics, a montré que pour répondre à ce nouveau risque, il ne suffira pas de décliner des certifications, des audits et des plans d'actions, ni d'ajouter des briques techniques. Fondée sur les recommandations de l'APSSIS[3], l'étude montre qu'au-delà des investissements nécessaires, il faudra sensiblement renforcer les équipes informatiques des établissements pour garantir un niveau de sécurité satisfaisant dans le temps (à hauteur de cinq ETP pour un parc de dix mille postes de travail). Sans ce renforcement humain, toutes les mesures seront temporaires. TABLEAU 1

Abordons la cyber-résilience comme un processus qualité. Il n'y a pas de choix à effectuer entre les projets et la sécurité. Les ressources dédiées à la sécurité devront rester pérennes.

INVESTISSEMENTS ET CHANTIERS TABLEAU 2

	Les chantiers	Atteindre le niveau K€	Atteindre le niveau J/H	Maintenir le Niveau K€	Maintenir le Niveau J/H
1	Sécurisation AD		150	0	60
2	Segmentation réseau		300	50	75
3	Sécurisation de 4 serveurs DIAMOND		120	30	37,5
4	Adaptation de l'infrastructure système		250	0	162,5
5	Sauvegarde		80	100	125
6	Sécurisation DMZ		125	50	132,5
7	Sécurisation du parc de terminaux		80	0	350
8	Protection AV		100	50	62,5
9	SIEM/SOC		50	225	125
10	gestion de crise		30	0	18,75
11	Compétences (besoins de formations)		0	50	62,5
	TOTAL		**1285 (1300) J/H**	**555 (556) K€/an**	**1211 (1100) J/H**

Chaque donnée représente la médiane d'un GHT/Etablissement avec 10000 PC.
La valeur entre parenthèses dans le total représente la médiane du total et non la somme des médianes par chantier.
C'est celle-ci qui est prise comme référence dans le tableau de synthèse des moyens à engager.

Source : juin 2021, CNSI, GT - DSI/RSSI, "Étude des moyens financiers et humains pour la protection cyber des SI hospitaliers".

Un autre tableau, tiré de cette étude, représente les investissements à conduire, au regard des différents chantiers de sécurité, pour devenir cyber-résilient. À l'exception du chantier 9, tous peuvent se décliner dans un établissement ou un GHT. Le chantier 9 sera plutôt étudié à l'échelle d'un regroupement de GHT, régionale ou nationale. TABLEAU 2

Les moyens de mener à bien les chantiers de cyber-résilience sont multiples : augmenter les effectifs dédiés à la sécurisation des SI, favoriser une réorganisation par redéploiement interne au sein de la DSI, de l'établissement, du GHT. Car plus l'établissement étend ses systèmes numériques, plus s'accroît son périmètre de systèmes à protéger et donc d'exposition aux risques. Dans le cas d'un redéploiement interne de temps agent ou de ressources vers la sécurité, l'impact consistera en une réduction de capacité à conduire les projets. Il convient d'assurer un équilibre de plus en plus complexe entre la capacité de maintenir la sécurité et la capacité de déployer les projets.

En matière de sécurité incendie, il ne viendrait à l'idée de personne de remettre en question les normes et investissements. Toutes choses étant égales par ailleurs, c'est pourtant ce que nous faisons collectivement en matière de cybermenace : nous espérons que le danger passe à côté.

À l'échelle nationale ou au sein des établissements publics de santé, nous n'avons pas attendu 2021 pour agir sur le champ de la cybersécurité. Mais le périmètre couvert par le numérique, d'une part, et le niveau de risque des menaces, d'autre part, augmentent.

Il convient de prendre acte de la nécessité de renforcer, et de maintenir, les équipes des établissements dédiés aux risques cyber, et ce à plusieurs niveaux. Les établissements doivent s'en saisir et étudier les moyens d'y parvenir. La gouvernance nationale doit passer de l'aide ponctuelle à un accompagnement durable, afin de maintenir les actions de sécurisation à un seuil optimum. Il importe enfin de prendre en considération nos experts du terrain en incluant des représentants dans chacune des strates de la gouvernance nationale cyber et ses travaux associés.

Renforcer la mise à niveau, maintenir en condition de sécurité notre système d'information hospitalier, associer notre expertise dans la gouvernance nationale : tel est notre pari en promouvant notre approche auprès des établissements et des autorités.

3. www.apssis.com, onglet « Nos actions », rubrique Publications : « Guide cyber-résilience. Tome 2 – Les cyberattaques », Cédric Cartau.