LES GUIDES DU RESAH

COMMENT SE PRÉMUNIR DES CYBERATTAQUES ?

resah
Réseau des Acheteurs Hospitaliers

Appuyons la transformation du système de santé par les achats

47, rue de Charonne
75011 PARIS
www.resah.fr

Directeur de la publication : Dominique LEGOUGE
Directrice de la communication : Sandrine BOURG
Responsable éditorial : Jean-Marc BINOT

Ont contribué à la rédaction de ce guide :

Vincent BRANGER, *cofondateur et directeur général d'Ilki*

Bertrand LOUVOIS, *ancien DSI d'hôpital, directeur du pôle achats SI-télécoms du Resah*

Benjamin SERRE, *Chief Development Officer, Orange Cyberdéfense.*

Illustrations : ©freepick

Avant-propos

Informatisation des procédures, équipements biomédicaux connectés, échanges électroniques, stockage des données, plateformes de suivi des patients, téléconsultations... le secteur de la santé a massivement procédé à la digitalisation de ses activités ces dernières années afin d'améliorer la prise en charge des soins. La pandémie et l'essor du télétravail ont encore accéléré le mouvement.

Revers de la médaille, cette omniprésence du numérique dans le quotidien des établissements sanitaires et médico-sociaux n'est pas sans risque. Car dans le même temps, la cybercriminalité est montée en flèche. En 2020, le nombre de cyber-attaques en France a été multipliée par 4 selon l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Vols de données, blocage des systèmes d'informations, tout est bon pour faire de l'argent et exiger des rançons.

Cette menace est à prendre au sérieux. À l'image des entreprises et des collectivités territoriales, plusieurs hôpitaux et EHPAD, victimes d'intrusion, se sont retrouvés brutalement désorganisés, voire paralysés. Se protéger passe évidemment par l'acquisition d'outils adéquats, mais aussi par la définition d'une politique de sécurité informatique structurée et pérenne et la sensibilisation de l'ensemble des acteurs de l'organisation.

INTRODUCTION

Au début de l'année 2021, alors que la crise sanitaire fait rage, plusieurs hôpitaux font les frais d'intrusion dans leurs systèmes d'informations. Une cyberattaque est recensée par semaine selon les estimations du secrétariat d'Etat à la transition numérique. À tel point que le Président de la République tire la sonnette d'alarme, invitant hôpitaux et structures médico-sociales à consacrer systématiquement 5 à 10 % du budget informatique à leur cybersécurité.

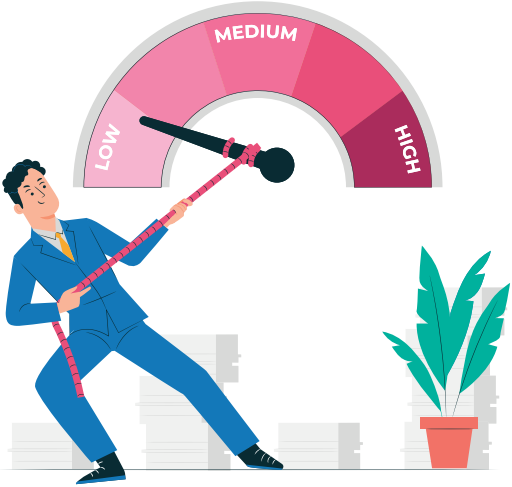
Il n'est plus possible de faire de ce sujet « une variable d'ajustement des projets informatiques des établissements de santé » prévient le gouvernement qui élève la problématique au rang de priorité nationale.

Les pouvoirs publics annoncent, dans le même temps, que 25 millions d'euros seront consacrés par l'ANSSI à la réalisation d'audits dans les hôpitaux, en plus des 350 millions prévus dans le cadre du Ségur de la Santé pour la sécurisation informatique des structures sanitaires et médico-sociales.

Un hôpital ou un EHPAD a certainement plus de chance d'être victime d'un hacker que d'un incendie. C'est pourquoi le cyber-danger doit être prévenu à l'instar de tous les risques auxquels sont confrontés les établissements et pour lesquels des dispositifs de vigilance ont été mis en place.

D'autant que les « failles » et recettes utilisées par la plupart des cyber-pirates sont connues : absence de mise à jour des programmes et outils informatiques, prise en compte insuffisante de l'aspect cybersécurité dans les achats des équipements et des solutions, surveillance opérationnelle lacunaire, comportements inadaptés de personnels peu formés et peu sensibilisés à la question.

TABLE DES MATIÈRES


LOW
MEDIUM
HIGH

1

UNE MENACE GRANDISSANTE

Chaque année, les cyber-attaques se font de plus en plus nombreuses. Entreprises privées, institutions, collectivités locales et hôpitaux sont les victimes de pirates informatiques qui s'introduisent dans les systèmes d'information, bloquent leur fonctionnement ou dérobent des données. Le phénomène est mondial.

En matière de cyber-risque, les hôpitaux ne font pas exception à la règle. En 2017, le système national de santé (NHS) du Royaume-Uni a particulièrement été frappé par la vague WannaCry. Le NHS a dû mettre hors ligne plus d'un tiers de ses SI, soit parce qu'ils avaient été touchés, soit parce qu'ils étaient en danger.

Ce qui a considérablement ralenti les performances et les soins apportés aux patients dans de nombreux établissements de santé. Démarrée en Ukraine la même année, l'attaque NotPetya a paralysé le groupe de santé américain Heritage Valley (Pennsylvanie), en cryptant ses serveurs et ses postes de travail.

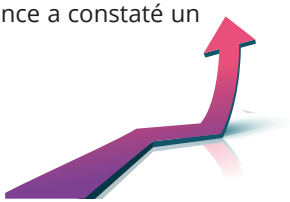
Retour au papier et au crayon

En France, la presse se fait régulièrement l'écho d'hôpitaux frappés par ce fléau. En juin 2019, un pirate parvient à s'introduire dans le réseau de l'hôpital d'instruction des armées Sainte-Anne à Toulon. Deux mois après, le groupe Ramsay Santé annonce que les SI de ses 120 établissements français ont été endommagés par un virus. En novembre de la même année, le cas du CHU de Rouen défraie la chronique. En raison du blocage informatique, les équipes hospitalières sont obligées de reprendre papier et crayon pendant plusieurs jours pour gérer les admissions, les prescriptions, les comptes-rendus, avec un allongement des délais de prises en charge.

Les cas se répandent. Alors que les actes de cyber-malveillance représentaient 43% des incidents de sécurité signalés du secteur sanitaire en 2019, leur part est passé à 60% en 2020. Dans un rapport établi en 2021 sur l'état de la menace cyber sur les établissements de santé, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) constate que les attaques contre le secteur sont en « nombre croissant » depuis sept ans, en indiquant toutefois qu'il ne s'agit pas d'un cas spécifique puisque la tendance à la hausse de la cybercriminalité est globale.

L'épidémie Covid-19, facteur d'accélération

À l'image de tous les évènements majeurs, la crise sanitaire a été un terreau fertile pour la prolifération de « maliciels ». Les pirates informatiques ont utilisé à leur profit la nécessité urgente de trouver rapidement des équipements et du matériel pour lutter contre la pandémie et l'explosion du télétravail pour diffuser méls et messages contenant des programmes malveillants.
Selon les données fournies par l'entreprise Check Point, les attaques contre les organismes de santé auraient crû considérablement pendant la crise sanitaire, de + 45% de novembre à décembre 2020 à l'échelle mondiale, contre une augmentation moyenne de 22% des cyber-attaques observée au cours de la même période dans les autres secteurs industriels.
Toujours selon la même source, le nombre moyen d'attaques hebdomadaires dans le secteur des soins a atteint 626 en novembre, contre 430 en octobre. Le Canada a connu la flambée la plus spectaculaire avec un + 250 %, suivi par l'Allemagne avec une hausse de 220 %. L'Espagne a vu le nombre de cas doubler, et la France a constaté un bond de 26%.



Vingt-sept cyberattaques d'hôpitaux en 2020 ont été recensés dans l'hexagone. Et il ne s'agit pas forcément de grandes structures. Le CH de Marmande-Tonneins (Lot-et-Garonne) en est victime en juillet. En décembre 2020, c'est au tour du CH d'Albertville-Moûtiers et des EHPAD USLD Claude-Léger (Albertville) et Les Cordeliers (Moûtiers) d'être frappés par un rançongiciel qui endommage leur SI. Les connexions Web sont coupées. Le CH de Narbonne est lui aussi touché par une attaque à la même période. Le début de l'année 2021 est marqué par une nouvelle succession d'attaques. En janvier, la clinique de l'Anjou à Angers, proie d'un virus, doit passer en mode dégradé. Infiltré par le rançongiciel Ryuk, le CH de Dax ne peut plus, à l'entame du mois de février, accéder à ses données, désormais chiffrées. Les téléphones et les ordinateurs ne fonctionnent plus. Le centre de vaccination Covid doit même fermer ses portes. Comme à Rouen, l'hôpital landais est obligé de revenir au mode papier.
Quelques jours plus tard, l'hôpital de Villefranche-sur-Saône subit un raid informatique du même programme malveillant. L'établissement est obligé de déconnecter tous ses postes de travail et ses téléphones, à l'exception du standard des urgences.

CELA N'ARRIVE PAS QU'AUX AUTRES

Les CHU et les CH de taille importante ne sont pas les seuls dans le viseur des hackers. En mars 2021, l'hôpital d'Oloron Sainte-Marie (320 lits et places, Pyrénées-Atlantiques) est la cible d'une attaque au rançongiciel qui entrave le bon fonctionnement de son système informatique, compliquant par exemple l'accès aux données patients et la gestion des stocks de médicaments. Au lieu des traditionnelles fenêtres, les écrans des ordinateurs du CH ont affiché un message en anglais : l'établissement devait verser une somme en bitcoins équivalent à 50 000 dollars américains. Début avril, le CH de Saint-Gaudens (Haute-Garonne) subit les foudres de cybercriminels, obligeant l'hôpital à fermer ses serveurs afin d'éviter la propagation d'un virus. L'informatique et la téléphonie sont interrompues, les ordinateurs éteints. Quelques jours plus tard, la Fondation Hopale est obligée de fermer son centre de vaccination Covid-19 de Berck-sur-Mer pendant plusieurs jours à la suite d'une intrusion informatique. L'accès au réseau internet est coupé et les disques de partage inaccessibles.

Le coût d'une cyberattaque

Les impacts d'une intrusion informatique sont multiples. Une attaque altère en premier lieu la prise en charge des patients, en perturbant et en désorganisant l'activité (plannings, dossiers et résultats des examens non consultables, dysfonctionnement possible des plateaux techniques et des équipements biomédicaux ...) générant une pression et un stress supplémentaire pour les équipes. Lors de l'attaque en 2021, l'hôpital de Dax a été obligé de déprogrammer certaines opérations ou des soins et de réorienter des patients vers d'autres établissements.
Elle peut déboucher aussi sur le versement d'une rançon en échange d'un déblocage du réseau. Si la règle en France est de ne jamais céder au chantage, des établissements américains acceptent de débourser pour recouvrer l'intégrité de leur SI. En termes d'image, une attaque réussie et médiatisée endommage la réputation d'un établissement.
Une intrusion malveillante va également obliger la structure à reconstruire son environnement numérique, remise en route qui pourra prendre plusieurs semaines, voire plusieurs mois. En 2017, suite à WannaCry, la NHS a été obligée de reporter 19 000 rendez-vous de patients et la dépense liée à la remise en route informatique (récupération des données, mises à jour) a été estimée à 92 millions de livres sterling.

UNE FACTURE DE 40 000 EUROS POUR LE CH D'ISSOUDUN

Caché dans une pièce jointe d'un mél, le virus Antirecuva ANDB est repéré en octobre 2019 à l'hôpital d'Issoudun, obligeant la structure à éteindre tous les ordinateurs. Si l'hôpital a refusé de payer la rançon (900 dollars), il a été obligé de remettre d'équerre son système et s'équiper d'un nouveau pare-feu, soit une facture oscillant entre 40 et 45 000 euros selon la direction de l'établissement.

Il faut ajouter à ces dépenses d'éventuelles sanctions pécuniaires infligées par la CNIL pour non-respect du Règlement Général sur la Protection des Données (RGPD), notamment lors de fuites de données de santé sensibles.

À RETENIR

La fréquence et le volume des cyber-attaques ne cessent de s'aggraver. Tous les secteurs d'activité sont touchés, y compris le secteur sanitaire et médico -social. N'importe quel établissement, quelle que soit sa taille ou sa localisation, peut être victime d'un pirate informatique. Et une intrusion dans le système d'information détériore la prise en charge des patients non seulement à court terme, mais parfois pendant des mois.


VIRUS
DETECTED!
ERROR

2

LES PRINCIPAUX **RISQUES**

De plus en plus fréquentes, les cyber-attaques sont également polymorphes. Le groupement d'intérêt public (GIP) cybermalveillance.gouv.fr a inventorié près de 44 types de malveillance informatique : diffusion de virus, arnaques au faux support technique, chantages à la webcam, faux ordres de virement, défiguration de sites web...

Le fléau du rançonnage

Cependant, s'agissant des hôpitaux, le risque majeur consiste dans le rançonnage, racket informatique considéré comme la « menace la plus immédiate » aussi bien pour son volume que sa fréquence, selon le rapport de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) publié en 2021 sur « l'état de la menace cyber sur les établissements de santé ». Toujours selon le GIP cybermalveillance.gouv.fr qui la qualifie de « fléau », cette famille d'attaque est passée du 6e au 1er rang entre 2019 et 2020.

Opérées grâce à des programmes spécialisés (ransomware) aux noms baroques (Ranion, Dharma, Sodinokibi, DoppelPaymer, Maze, Netwalke, Magneto...), ces intrusions, limitées à un poste de travail il y a une dizaine d'années, contaminent désormais l'ensemble d'un SI et cherchent à bloquer leurs fonctions vitales. Concrétisées par le chiffrement des données et leur inaccessibilité, elles entravent les activités, désorganisent, retardent la prise en charge des patients et peuvent déboucher sur la paralysie de certains services. Elles peuvent aussi occasionner la perte définitive de données.

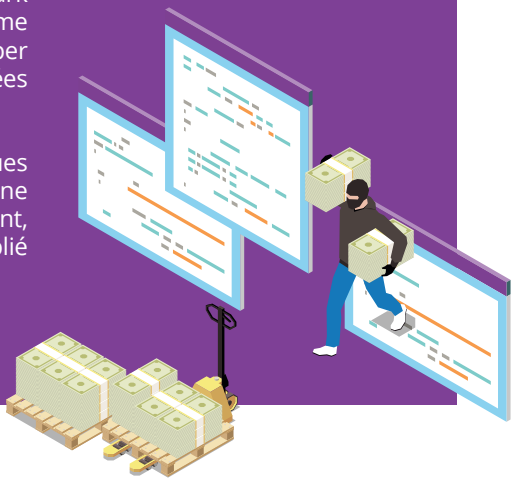
Dans la plupart des cas, les cyberpirates promettent le retour à la normale en échange du versement d'une somme d'argent, et, parfois, menacent de publier des bases de données subtilisées. Tandis que certains hôpitaux nord-américains acceptent de payer les rançons, la règle en France est de ne jamais céder. L'hôpital n'a en effet aucune garantie qu'il obtiendra une clef de déchiffrement. Par ailleurs, cette clef n'aboutit pas toujours à la récupération intégrale des données chiffrées.

Néanmoins, en dépit de cette ligne de conduite, les établissements de santé continuent d'être malmenés. Cela s'explique par le fait que, dans 90% des cas, les pirates informatiques, en raison des techniques utilisées, ignorent exactement quelle est la nature de l'organisation qu'ils infiltrent.

670 000 DOLLARS DE BUTIN

Victime du rançongiciel SunCrypt, l'hôpital américain de Newark (New Jersey) a versé la somme de 670 000 dollars pour stopper la diffusion en ligne de données patients dérobées.

Les agresseurs informatiques assuraient avoir récupéré une base de 240 giga-octets et avaient, pour prouver leur sérieux, publié 48 000 documents.



Contrairement aux idées répandues, les hôpitaux ne sont pas ciblés, sauf cas particuliers par exemple lorsque le but de la cyberattaque est l'espionnage industriel ou le vol de données. En septembre 2021, l'AP-HP s'est fait ainsi dérober des fichiers concernant 1,4 million de personnes testées en Ile-de-France dans le cadre du dépistage Covid (identité, numéros de Sécurité sociale et coordonnées, résultats du test). L'intrusion aurait pu être la conséquence d'une faille de sécurité d'un outil de partage de fichiers.
Cependant, les établissements de santé sont aujourd'hui régulièrement frappés avant tout parce qu'il s'agit de structures très connectées, avec un nombre important de postes de travail informatiques et de dispositifs biomédicaux reliés à des réseaux, et sans doute un degré de sensibilisation moindre au cyber-risque.

Ne pas mordre à l'hameçon

Trois techniques sont généralement utilisées par les pirates numériques. Le « hameçonnage » (phishing en anglais) est la plus commune. Un agent reçoit un courriel qui cherche à attirer son attention et qui contient une pièce jointe ou un lien. Objectif des escrocs : pousser le destinataire à cliquer sur ce lien ou à ouvrir le document qui peut être un PDF, un tableur ou un simple traitement de texte, afin d'installer un outil malveillant. Ce dernier va rechercher une vulnérabilité sur le poste de travail, par exemple un logiciel, un programme, voire un pilote de périphérique (la commande d'une imprimante) qui n'a pas été mis à jour depuis des mois, voire des années, faute de ressources humaines ou financières.
L'autre solution, pour le « hacker », consiste à recourir à un identifiant volé. Il faut savoir que des bases de login/mot de passe sont disponibles sur internet, gratuitement ou de manière payante, notamment sur le darknet (espace internet parallèle non référencé par les navigateurs traditionnels). Ces filons ont été constitués à la suite de précédentes intrusions informatiques ou de comportements imprudents, par exemple l'utilisation de messagerie professionnelle à des fins personnelles sur des sites non sécurisés, comme l'inscription à des newsletters associatives.

L'exploitation des failles de sécurité est une troisième voie. Les pirates vont profiter de la vulnérabilité d'adresses IP (site institutionnel de l'hôpital, site de ses unités de recherche, formulaires en ligne pour les patients, systèmes d'accès à distance...), de serveurs, de VPN, ou de programmes.
Il est important de comprendre qu'il est enfantin de retrouver sur internet, via des moteurs de recherche, les vulnérabilités les plus connues et d'exploiter leurs failles grâce à des tutoriels également disponibles en ligne.

2 000 DOLLARS POUR 50 000 IDENTIFIANTS D'AGENTS HOSPITALIERS

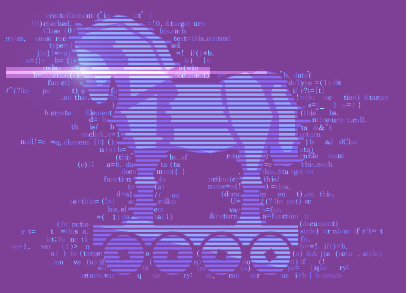
Le rapport de l'ANSSI concernant l'état de la menace cyber sur les établissements de santé mentionne qu'un forum cybercriminel mettait en vente une base de 50 000 comptes utilisateurs appartenant à des agents hospitaliers contre la somme d'environ 2 000 dollars.

Certains gangs informatiques se sont spécialisés dans la vente de ces moyens d'intrusion. Ils s'infiltrent et cherchent à se constituer un stock de machines « compromises », afin de les commercialiser auprès d'autres pirates, en échange d'une rétrocession d'une partie des rançons. Démantelé au début de l'année 2021 par Europol, le groupe qui exploitait le programme malveillant Emotet disposait par exemple d'un parc de 1 200 000 ordinateurs.

LES DM, CHEVAUX DE TROIE

Omniprésents, les dispositifs médicaux connectés représentent des sas d'intrusion potentiels si les modes de communication entre leurs différentes interfaces ne sont pas suffisamment sécurisés.
En théorie, rien n'empêcherait un cyberpirate malintentionné de bloquer le fonctionnement d'un DM, de l'éteindre, ou de modifier les informations transmises par la machine aux équipes soignantes en faussant le diagnostic. Experte norvégienne en cybersécurité, Marie Moe, elle-même porteuse d'un défibrillateur, a découvert de nombreuses failles de ce dispositif et montré qu'il est à la fois possible de récupérer les données et de les éteindre à distance.
L'Atlas des SIH 2018 de la DGOS indique que seuls 41% des équipements biomédicaux connectés au réseau sont inclus dans le périmètre de la sécurité du système d'information. Dans 1 cas sur 4, aucune analyse de risque n'est réalisée lors de l'arrivée d'un nouveau matériel.

Il en va de même pour les outils de télémédecine en plein essor, notamment depuis la crise sanitaire. Conséquence, en cas de vulnérabilité, un cybercriminel peut tout à fait s'immiscer sur une plateforme de télésurveillance et récupérer les données de santé, les publier ou les commercialiser sur les marchés parallèles. Selon Vincent Trély, président de l'Association pour la sécurité des systèmes d'information de santé (APSSIS), les bases de données médicales pouvaient se revendre 30 à 200 bitcoins en 2019 (la valeur du bitcoin a oscillé entre 3 400 et 10 800 euros durant cette année).



Les étapes de la chaîne d'attaque (kill chain)

Quelle que soit la technique employée, le cybercriminel a un premier objectif en tête : s'emparer d'une machine, « le patient zéro », grâce à laquelle il pourra accéder au SI.

Une fois introduit dans la bergerie, le loup informatique recherche de nouvelles vulnérabilités, dans le butde devenir administrateur du système, autrement dit détenir tous les droits, y compris celui de bloquer l'accès à toutes les données de sauvegarde, ou pire les détruire.

Cette phase de découverte des lieux et de repérage peut durer un certain temps, jusqu'à plusieurs mois. En raison du nombre de machines compromises disponibles à l'échelle planétaire, les pirates ont en effet l'embarras du choix et manquent de temps pour traiter l'ensemble du parc qu'ils ont à disposition.

Lorsqu'il a inventorié les données les plus importantes et compris leur politique de sauvegarde, le cyber-brigand exfiltre parfois des bases, puis déclenche son attaque. Il interdit alors l'accès aux serveurs, aux données et à leurs sauvegardes, élément stratégique du SI. Très souvent, l'offensive est déclenchée la nuit, un dimanche ou jour férié pour limiter la capacité de réaction de la victime.

À RETENIR

Les attaques ciblées concernant les établissements hospitaliers existent lorsqu'il s'agit de dérober des bases de données ou des dossiers patients. Toutefois, en règle générale, ce n'est pas le cas.

Cherchant à aller au plus simple, les cyber-pirates sont avant tout opportunistes. Ils vont profiter des effets d'aubaine : base de login/mots de passe volés et disponibles en ligne, sécurité informatique insuffisante avec des programmes et des sites non mis à jour, ou tournant sur des systèmes d'exploitation obsolètes, naïveté des personnels...

Si hôpitaux ou établissements médico-sociaux sont victimes d'attaques informatiques, c'est avant tout en raison d'une « hygiène numérique » insuffisante ou de vulnérabilités de leurs systèmes d'informations.

Le mode opératoire d'une cyber-incursion est long. Le déclenchement de l'attaque est en réalité la dernière étape du processus, même s'il semble le premier pour l'hôpital ou la clinique.

3

LES PARADES

Il ne faut jamais mésestimer le risque d'une cyber-attaque et naturellement se doter de boucliers (pare-feu, filtrage Web, système de gestion de droit d'accès aux applications, protection renforcée des comptes à privilège, sondes autonomes de détection et de protection d'intrusion, antivirus serveurs et postes de travail...). Pourtant, même avec le meilleur matériel du monde, une organisation pourra faire les frais d'une tentative de « hacking ».

Aujourd'hui, sans viser la perfection, se doter d'une politique de sécurité a minima sera en mesure de décourager une grande partie des cyber-escrocs. Il faut garder à l'esprit que le pirate informatique soupèse le rapport enjeu/effort. En effet, leur « terrain de jeu » est tellement vaste qu'il ne perdra pas son temps à essayer de contourner d'éventuels obstacles. Dans la majorité des cas, il recherchera une proie plus facile à dépouiller.

En outre, la cybersécurité ne se limite pas à la simple acquisition de matériel dernier cri. Elle repose sur une démarche rigoureuse et itérative, fondée sur le principe d'amélioration continue (PDCA, Plan Do Act Check) et une organisation structurée par le système de management de la sécurité de l'information (SMSI, défini par la norme Iso 27001).

Adopter une démarche d'amélioration continue

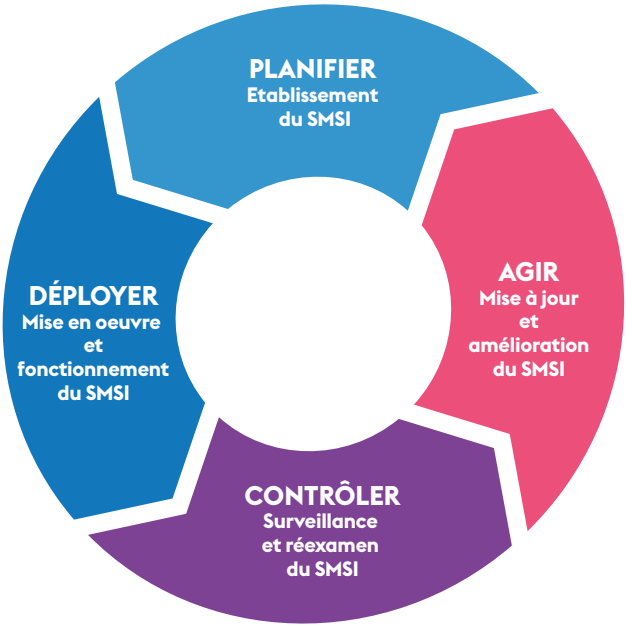
Elle comprend 4 étapes :

1- Évaluation des risques et de leur criticité pour estimer les forces et faiblesses de l'établissement : quels risques et quelles menaces, sur quelles données et quelles activités, avec quelles conséquences ?

2- Recherche et sélection des parades : que va-t-on sécuriser, quand et comment ?

3- Déploiement des protections : processus et procédures, éléments techniques de protection, formation et sensibilisation, mise en place d'une chaîne d'alerte ;

4- Vérification de leur efficacité : audits organisationnel et documentaire, tests de fonctionnement en mode dégradé, tests de reprise de données, tests d'attaque malveillante.



SMSI : Système de management de la sécurité de l'information

Ce travail doit être reconduit au moins chaque année, avec une analyse des risques qui va déboucher sur un plan d'actions afin de corriger les failles (sécurisation des bases de données, mises à jour, cloisonnement de réseaux...). Le plan d'analyses des risques et le plan d'actions doivent être présentés à la direction générale.

Conserver une bonne hygiène numérique

Une des composantes d'une hygiène numérique minimale est la mise à jour de manière périodique et continue des outils informatiques utilisés par l'établissement en termes de sécurité. Autrement dit, un SI vulnérable s'apparente à une maison dont la porte serait grande ouverte : il va attirer les cybercriminels.
En raison de l'importance et de la diversité des matériels, la tâche est plus ardue dans un établissement de santé. Cela passe déjà par la tenue d'une cartographie complète des outils usités et d'un inventaire des dispositifs les plus fragiles. Puis par la définition d'un programme de correctifs à appliquer, en fonction de la criticité et des priorités.
De manière identique, il est recommandé de privilégier des mots de passe complexes avec authentification forte, et de s'assurer, avec l'aide d'outils dédiés, qu'ils ne sont pas compromis et disponibles sur le Darknet.

Cloisonner autant que possible

Le cloisonnement des réseaux ressemble à une digue qui pourra empêcher un pirate informatique d'infecter l'ensemble d'un système d'information.

Par conséquent, ce cordon sanitaire limitera les dommages. Il en va de même pour les comptes d'administration et les postes dédiés à cet usage.

Prendre soin de ses sauvegardes

Le rapport 2020 de l'Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé insiste sur ce sujet. Dans la plupart des cas, au moment de l'attaque, il n'existe pas d'outils de déchiffrement du rançongiciel employé. La seule issue pour l'établissement repose donc sur les sauvegardes qui doivent être stockées à part du SI pour empêcher leur chiffrement et préserver la possibilité d'un retour rapide à la normale. Lorsque la sauvegarde n'est pas touchée, il est envisageable de reconstruire un SI dans un laps de temps oscillant entre deux et quatre semaines.

Monter la garde en permanence

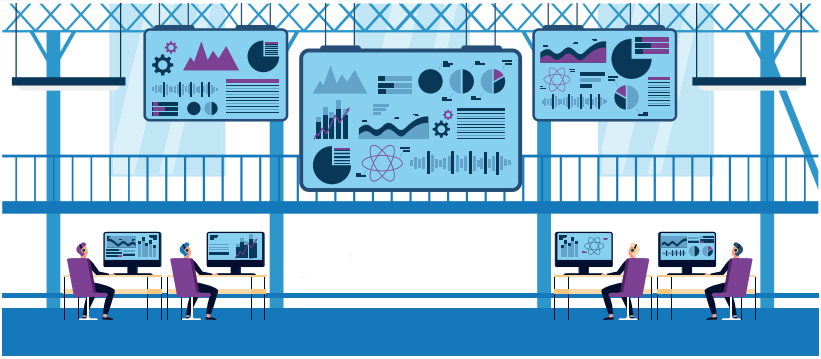
S'agissant du phishing, la plupart des spécialistes l'affirment : s'équiper de pares-feux ou d'antivirus n'éradique pas le risque. D'abord parce qu'ils ne seront pas forcément capables de détecter les derniers rançongiciels élaborés ou ceux à venir. Par ailleurs, ces défenses, pour éviter de paralyser sans arrêt une machine, ne bloquent les intrusions que s'ils sont certains qu'il s'agit d'applications malveillantes. Dans le cas contraire, ils émettent des alertes qu'il faut naturellement analyser pour séparer le bon grain de l'ivraie. Encore faut-il qu'une personne soit à la fois disponible et capable de le faire. Cette absence ou ce déficit de vérification d'éléments anormaux facilitent très souvent le travail des cyber-pirates. Si les études menées par la DGOS dans son Atlas des SI indiquent que 96%

des établissements comprennent un RSSI dans leurs effectifs, en pratique ces professionnels ne consacrent pas tout leur temps à la sécurité opérationnelle. Ils sont affectés à cette tâche le plus souvent à temps partiel, et pour partie, de manière mutualisée au bénéfice de plusieurs établissements. Par ailleurs, ils doivent mener des travaux dans le domaine de la conformité ou des opérations de sensibilisation du personnel. En outre, les tensions, en termes de recrutement, dans le secteur de la cybersécurité, engendrent un fort turn-over.

Détecter le plus tôt possible

C'est pourquoi des solutions de type SOC (Security Operation Center) sont apparues sur le marché. Destinés au départ aux grandes entreprises type CAC 40, ces outils de surveillance, qui ont recours à de l'intelligence artificielle, sont déployés sur l'ensemble du SI (grâce à des composants installés sur les serveurs et les terminaux). Ils ont deux rôles. À l'image des antivirus, ils bloquent les menaces informatiques répertoriées. Mais ils vont aussi déclencher des alertes en cas de comportements étranges (connexions avec le compte administrateur tôt le matin un dimanche, augmentations des sessions, terminal connecté à un serveur qu'il n'utilise jamais d'habitude...). Ces anomalies sont alors traitées par un expert, en général dans la journée.

Les SOC ont aussi l'atout de se placer dans une démarche d'amélioration continue. Les systèmes conservent les historiques des évènements pendant plusieurs mois, analysent les attaques et ajoutent éventuellement des règles de sécurité supplémentaires. Chaque cas traité contribue à la sécurité collective. Le coût d'un SOC oscille entre 20 et 30 euros TTC par machine et par an pour une surveillance 24/24.



UN ACHETEUR AVERTI EN VAUT DEUX

Il faut le répéter : la sécurité informatique est l'affaire de tous. Les acheteurs ont donc aussi leur rôle à jouer. D'abord en intégrant ce sujet lors de leurs choix de matériel (DM, équipements biomédicaux, télécoms, équipements en réseau, objets connectés...) et en associant le référent SSI à la réflexion, en évaluant le risque éventuel, notamment lors de l'acquisition de nouvelles solutions. Ensuite en établissant clairement dans les cahiers des charges des exigences en matière de cybersécurité qui serviront à la sélection des fournisseurs. Enfin en prévoyant dans les contrats des clauses de maintien en condition de sécurité avec des délais de mise à jour rapides, et la possibilité de mener des audits sur l'état de vulnérabilité de ces solutions.

Sensibiliser l'ensemble du personnel

Les comportements évitables d'agents et de partenaires des établissements sont à l'origine de nombreuses attaques comme l'ouverture d'un document contenant un programme malveillant.... Il est donc impératif d'indiquer à l'ensemble des acteurs et des métiers (administratifs, soignants, techniques...) quelles pratiques adopter pour limiter le risque d'une cyber-intrusion et, entre autres, apprendre comment repérer les messages pernicieux et avoir le bon réflexe de signaler un incident de sécurité aux référents appropriés. Ces opérations de sensibilisation doivent être menées à intervalles répétés en raison de la rotation des effectifs. Les formations standards ne sont pas forcément les plus adaptées aux utilisateurs finaux et, pour frapper les esprits, mieux vaut recourir à des techniques plus modernes comme le webinaire, la diffusion de vidéos, ou même un « escape game »...

Se faire tester

Pour mieux identifier ses talons d'Achille, la solution la plus simple est de procéder à des tests. Il en existe de plusieurs sortes.

Le « pentest » (test d'intrusion) va évaluer la possibilité de s'immiscer dans le SI. L'investissement est plus que raisonnable. Les ta-

SE METTRE DANS LA PEAU D'UN HACKER PENDANT 45 MN

Depuis 2018, le GCS e-santé Pays de la Loire met à disposition des établissements de sa région un « escape game » sur le thème de la sécurité numérique. Les participants doivent en 45 minutes chrono endosser le rôle de journalistes d'un magazine people peu scrupuleux qui doivent s'emparer de données sur l'état de santé d'une star hospitalisée. De quoi vérifier d'une façon ludique si les bonnes pratiques numériques sont correctement appliquées dans la structure. L'initiative a été récompensée par le prix Sécurité aux Talents de la e-santé 2020, organisés par la Délégation ministérielle au Numérique en Santé.

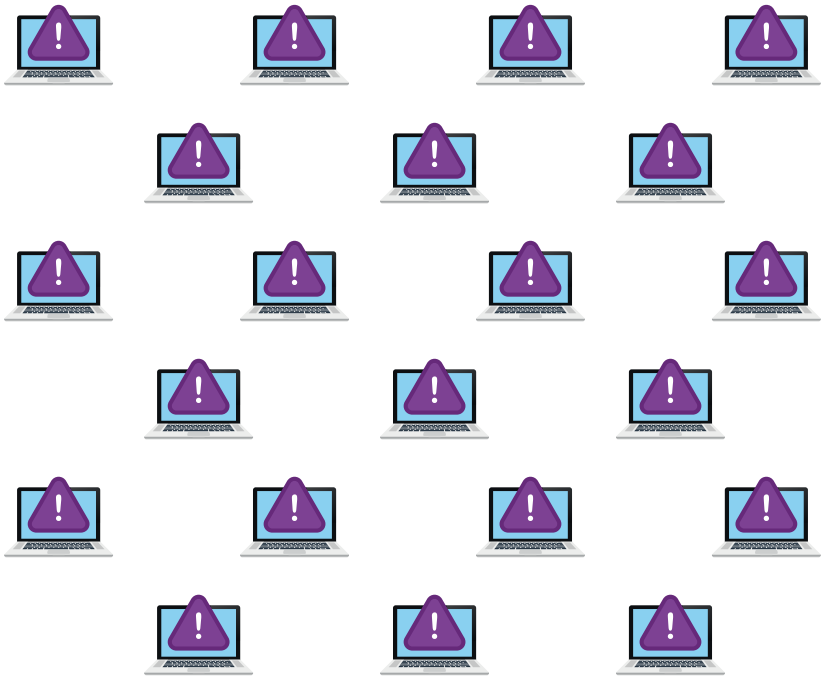
rifs peuvent osciller entre 3 000 et 6 000 euros en fonction de la configuration de la tentative d'intrusion, débriefing compris.
La campagne de simulation de phishing, avec l'envoi d'un mél comportant une pièce jointe ou un lien censé héberger un programme malveillant, permet de mieux se rendre compte du comportement des équipes. Elle s'accompagne généralement d'un module de e-learning qui explique à quoi s'exposent les personnes qui sont tombées dans le panneau. Une intervention comportant une campagne de « phishing », des sessions de formation, puis une seconde campagne de « hameçonnage » afin d'évaluer le changement d'attitude, peut revenir à 20 000 euros pour 500 utilisateurs.

MIEUX VAUT PRÉVENIR QUE GUÉRIR

Pour éviter de se retrouver devant un écran affichant une demande de rançon, l'une des solutions est de se faire diagnostiquer et accompagner par des experts avant tout incident : analyse des risques SSI, enquêtes effectuées par des prestataires d'audit de la sécurité des systèmes d'information (PASSI) qualifiés, définition de schémas directeur SSI avec plans d'action, audit de conformité, scan de vulnérabilité, test de pénétration des équipements...

À RETENIR

S'il n'existe aucune assurance tous risques contre une cyber-attaque, l'instauration d'une politique et d'un système de management dédiés permettent de réduire les probabilités. Il s'agit d'une démarche d'amélioration continue qui ne doit jamais s'interrompre afin d'augmenter la maturité SSI de l'établissement. La cybersécurité n'est pas seulement l'apanage de la DSI car le sujet dépend de la compréhension des dangers par l'ensemble des équipes et de comportements plus vertueux.



4

QUE FAIRE EN CAS DE CYBER-ATTAQUE ?

En raison des répercussions sur le bon fonctionnement de l'établissement, une cyber-attaque est une importante source de stress et de déstabilisation pour la DSI, la DG et l'ensemble des services (soins, administratifs, techniques). Comme dans les autres situations de crise, il s'agit de se préparer à une possible intrusion informatique. Savoir réagir à un évènement de ce type fait d'ailleurs partie des processus d'un SMSI (voir chapitre 3).

Prévoir une gouvernance particulière

L'établissement ou le GHT a tout intérêt à imaginer une gouvernance particulière à actionner en cas de besoin, avec un processus clairement formalisé :

- création d'une cellule de crise dédiée,
- recensement des ressources internes et externes (prestataires/experts) à mobiliser,
- inventaire des actions à mener,
- établissement d'un plan B pour les canaux de communication dans le cas où le téléphone et la messagerie seraient hors service,
- protocole de fonctionnement des services en « mode dégradé » en cas de dysfonctionnement ou d'arrêt des applications métier,
- définition d'un plan de communication en fonction des cibles (personnel, patients et leurs familles, fournisseurs et partenaires, journalistes...),
- définition d'un plan de reprise progressif de l'activité informatique (restauration des systèmes et des applications) en fonction des priorités stratégiques de la structure.

Des gestes barrières

La première mesure à prendre, en cas de cyber-attaque, est la déconnexion globale des machines, en bloquant les communications depuis et vers Internet, afin d'empêcher le pirate d'agir à distance, de contrôler son programme malveillant, de poursuivre le cryptage de données ou leur vol.

Là encore, l'établissement aura tout intérêt à se préparer à cette éventualité, en recensant précisément tous les points d'accès pour n'en oublier aucun, et en imaginant des solutions pour s'adapter à la situation (messagerie interrompue, impossibilité d'accéder à des bases de données externes ou des solutions SaaS). La connexion sera ensuite rétablie au fur et à mesure lorsque la DSI aura la certitude que la situation s'assainit.

LE CYBER-RISQUE NE JOUE PAS L'ARLÉSIENNE

Le 1er août 2021, le centre hospitalier d'Arles est la cible d'un cryptovirus. Dès le lendemain, l'hôpital met en place une cellule de crise, coupe tous les accès à Internet et passe en mode dégradé. Le CH avait anticipé avec une documentation sur la conduite à adopter en cas de perturbation de son système d'information. Il obtient l'aide de l'ANSSI et de prestataires spécialisés pour repérer la genèse de l'attaque puis renforcer sa sécurité informatique. Une quinzaine de jours plus tard, une organisation de cybercriminels revendique être à l'origine de l'attaque.

Il s'agit aussi de constituer une équipe spéciale chargée d'investiguer pour identifier les postes de travail corrompus ou suspectés de l'être afin de les isoler du reste du SI. Il ne faut pas hésiter à procéder à un confinement du matériel.

En revanche, il n'est pas recommandé d'éteindre le parc déconnecté pour faciliter les investigations qui permettront de faire la lumière sur la porte d'entrée utilisée par le cyber-pirate. Il est dans la même logique conseillé d'externaliser les logs en ne permettant pas à l'attaquant de détruire ses traces de passage.

À noter que la pratique d'externalisation des logs devrait être systématique bien avant qu'une attaque ne se produise.

L'autre automatisme est de protéger les sauvegardes, nerf de la guerre, de s'assurer qu'elles ne sont pas infectées et de les placer sur un serveur distinct et autonome.

Tracer tout ce qui se passe

Geste réflexe, l'ouverture d'une « main courante » servira à lister tous les évènements et actions concernant l'intrusion (chronologie des faits, matériels corrompus, échanges éventuels avec le rançonneur…).

Cette « boîte noire » sera utile pour l'enquête de police et permettra de tirer les leçons de la crise en définissant des actions correctrices.

Alerter et s'entourer

Dans ce genre de scenario catastrophe, l'établissement aura besoin de l'aide de tous. Très sollicitée dans le cas d'une attaque, la DSI doit pouvoir se mobiliser mais aussi savoir s'entourer pour affronter plus sereinement l'épreuve. Il est nécessaire de prévenir l'équipe de réponse aux incidents de sécurité de l'ANSSI pour les administrations et opérateurs d'importance vitale et de services essentiels (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques : **https://cert.ssi.gouv.fr/contact/**, et de recourir à l'expertise de prestataires spécialisés dans la réponse aux cyber-attaques.

Il ne faut pas omettre de contacter le(s) fournisseur(s) des équipements ou programmes infectés afin qu'ils puissent apporter son aide, prévenir d'autres établissements utilisant les mêmes machines, et corriger l'éventuelle vulnérabilité informatique à l'origine de l'attaque.

LE CERT SANTÉ VEILLE AU GRAIN

Antenne de l'Agence du numérique en santé (ANS), le CERT Santé (Computer Emergency Response Team), ex-cellule d'accompagnement cybersécurité des structures santé (ACSS), a pour mission de réaliser une veille sur les menaces pour mener des actions préventives, de mener des audits, mais aussi d'apporter son aide en cas de besoin : en 2020, un signalement sur 4 a bénéficié d'un accompagnement. Contact : cyberveille@esante.gouv.fr

Communiquer de manière appropriée

Lors d'une cyber-attaque, la politique de communication se révèle cruciale. Mieux vaut jouer la carte de la transparence, spécialement dans le cas d'un rançongiciel. Il est indispensable d'expliquer la situation et de donner des consignes au personnel, mais aussi d'informer les patients et leurs familles qui ne manqueront pas de se faire écho de la situation, entre autres sur les réseaux sociaux. Il en va de même pour les média, en choisissant soigneusement les éléments de langage pour éviter d'être contredit par des commentateurs experts. Choisir la politique de l'autruche n'est pas la bonne option. Car elle risque d'envenimer la situation, en irritant le pirate informatique qui pourra, lors d'un vol de données, en publier une partie en ligne dans le but de prouver à tous le succès de son entreprise.

Avertir les autorités et porter plainte

Les établissements de santé, les hôpitaux des armées, les centres de radiothérapie, les laboratoires de biologie médicale et les établissements médico-sociaux doivent déclarer à l'Agence régionale de santé (ARS) les incidents « graves » de sécurité (article L. 1111-8-2 du code de la santé publique).

En cas de vols de données personnelles, l'établissement doit prévenir la Commission nationale de l'informatique et des libertés (CNIL) dans un délai de 72 heures au plus tard (nature des données, volume, conséquences et mesures envisagées). Le règlement général sur la protection des données (RGPD) impose en outre d'aviser les personnes concernées, en cas de « risque élevé » pour leurs droits et libertés.

Il est préconisé à la structure victime d'un vol de données ou d'un rançongiciel de déposer une plainte, laquelle déclenchera une enquête et servira aussi auprès des assurances lors de la constitution d'un dépôt de sinistre. En général, l'affaire pourra être confiée au profit de la section cybercriminalité du parquet de Paris, qui a compétence nationale en la matière.

Relancer l'activité par étapes

Indispensable au bon fonctionnement de la structure, la reconstruction du SI doit être entamée, parallèlement aux investigations numériques qui peuvent être très longues. Pendant des semaines, voire des mois, l'établissement sanitaire ou médico-social peut vivre avec une épée de Damoclès, faute d'être certain à 100% que le SI est intégralement intègre et que le cyber-forban n'a pas laissé des bombes à retardement derrière lui. Car des répliques d'attaque peuvent avoir lieu.

Réinstaller des milliers de poste de travail de manière simultanée demeure ardu. La meilleure approche est de relancer progressivement l'activité, en donnant la priorité à certaines applications métiers, et en menant une surveillance constante.

Et après ?

Une fois la tempête passée, il s'avère nécessaire de décortiquer à la fois comment la crise a été surmontée, et aussi de quelle façon le malfaiteur est parvenu à s'introduire dans le SI pour réfléchir aux actions à mener.

À RETENIR

En cas d'intrusion, il est primordial de couper les accès à Internet, de confiner les machines suspectées d'être corrompues et de penser immédiatement à protéger ses sauvegardes, socle de la restauration du système d'information. Les établissements doivent impérativement se préparer à ce type de crise pour avoir immédiatement les bons réflexes et limiter les dommages.

RETOUR
D'EXPÉRIENCE

Sylvain François
Directeur du Système d'Information,
CHU de Rouen

COMMENT AVEZ-VOUS DÉCOUVERT QU'UN PIRATE INFORMATIQUE AVAIT RÉUSSI À S'INTRODUIRE DANS VOTRE SI EN 2019 ? DE QUELLE MANIÈRE AVEZ-VOUS RÉUSSI À RETROUVER UNE ACTIVITÉ NORMALE ET COMBIEN DE TEMPS CELA VOUS A-T-IL PRIS ?

"La découverte de notre cyberattaque s'est effectuée par l'intermédiaire de notre astreinte informatique. En effet, l'attaque ayant été déclenchée le vendredi dans la soirée, plusieurs utilisateurs ont successivement appelé le support d'astreinte pour indiquer une incapacité à se connecter au système d'information. Notre technicien a rapidement déterminé une impossibilité bien plus large à accéder à nos serveurs, et nous en avons déduit un chiffrement assez large de nos infrastructures.

Le retour à la normale a été travaillé dans un mode collaboratif avec l'ANSSI, que nous avons alertée dès ce vendredi soir. En la matière, nous avons pu répartir les missions entre l'ANSSI (analyse de la cyberattaque et travail sur la sécurisation de la situation) et le CHU (travail focalisé sur la remédiation). Le fait d'avoir nos sauvegardes totalement saines a permis la restauration successive des applications affectées par ordre de priorité (cette priorité étant guidée par la criticité de celles-ci au regard de la prise en charge des patients). Dans ce cadre, nous avions remis en service la quasi-totalité de nos applications critiques le dimanche soir, et nous avons remis en service progressivement le reste du système d'information sur la semaine suivante."

LE CHU A-T-IL ESTIMÉ LE COÛT QUE CETTE ATTAQUE A ENGENDRÉ ?

“Nous avons essayé d'estimer le coût, mais cet exercice est assez complexe du fait de notre secteur d'activités corrélé à la production de soins et non à la génération de revenus. Le principal est bien sûr qu'aucun impact sur nos patients a été à signaler lors de cet évènement. Sans pouvoir en avoir une certitude profonde, il ne semble pas que l'établissement ait eu à déplorer une perte d'activités, car nous n'avons pas eu à annuler des interventions programmées (consultations, blocs opératoires notamment) et très peu de patients ont annulé leur rendez-vous.

Le surcoût financier est donc essentiellement lié aux ressources humaines nécessaires à la gestion de la crise (heures supplémentaires ou renfort dans les services) ainsi que la commande de certaines prestations informatiques auprès de nos partenaires pour accélérer et fiabiliser la remédiation informatique.”

QUELLES LEÇONS L'ÉTABLISSEMENT A-T-IL TIRÉ ? LE CHU A-T-IL MODIFIÉ SA POLITIQUE DE SÉCURITÉ INFORMATIQUE ? ET LE CAS ÉCHÉANT, QUELLES MESURES OU PRÉCAUTIONS ONT ÉTÉ PRISES ?

“Tout d'abord, cette cyberattaque a démontré logiquement l'aspect central du système d'information dans la prise en charge des patients, mais a aussi mis en lumière l'importance de l'existence de procédures dégradées (et leur maîtrise par les utilisateurs) pour pallier les dysfonctionnements informatiques. Nous avons d'ailleurs pu déterminer certains secteurs d'activités pour lesquels ces procédures étaient inefficaces.

Cela a permis aussi de définir des axes d'améliorations dans la construction de notre architecture informatique mais aussi concernant les mésusages des utilisateurs (ex : sauvegarde de données sur leur poste de travail).

Concernant notre politique de sécurité, celle-ci était déjà en pleine construction avant la cyberattaque, cela nous a permis d'axer les travaux sur certaines priorités (ex : active directory). Enfin, cet évènement a permis de renforcer nos liens avec l'ANSSI, et de mettre en place des audits réguliers de nos infrastructures (i.e., détection de vulnérabilités ou points de faiblesse) à travers leurs outils mis à disposition (ex : ORADAD).”

FAITES-VOUS UNE ANALYSE DE RISQUE PARTICULIÈRE LORSQUE LE CHU ACQUIERT OU INSTALLE DES ÉQUIPEMENTS BIOMÉDICAUX CONNECTÉS ?

“Nous sommes en train de travailler avec les équipes du service biomédical pour intégrer systématiquement l'aspect sécurité dans leurs achats, notamment à travers l'inclusion de clauses dans les cahiers des charges. Par ailleurs, nous accompagnons les mises en œuvre des outils biomédicaux en termes de connexion au réseau, afin d'assurer une conformité à l'état de l'art. Nous appliquons également des stratégies de segmentation réseau pour éviter toute propagation généralisée.

Dans un avenir proche, nous souhaitons mettre en place des audits de sécurité axés sur le biomédical, car il serait illusoire de penser que l'intégralité des dispositifs historiquement mis en service ont donné lieu à une qualification d'impact en termes de sécurité.”

COMMENT SENSIBILISEZ-VOUS LE PERSONNEL DE L'HÔPITAL AUX CYBER-RISQUES ?

“Nous mettons en place des communications régulières à travers les outils internes au CHU (magazine, intranet), et nous envoyons des mails d'information. Très prochainement, nous allons mettre à disposition de l'intégralité des agents du CHU de ROUEN (et même plus largement du GHT Rouen Cœur de Seine) un accès à une plate-forme de sensibilisation en ligne et d'e-learning, ce qui permettra à chacun(e) d'évaluer son niveau de maturité sur le sujet et bien sûr de se former à travers des cas concrets.

Enfin, nous avons créé une adresse mail dédiée à disposition de tout le personnel du CHU pour leur permettre de nous poser les questions éventuelles ou de nous signaler le moindre évènement en cas de doute (ex : mail avec un lien ou une pièce jointe, mais dont l'expéditeur n'est pas connu).”

QUELS CONSEILS DONNERIEZ-VOUS À UN HÔPITAL OU UN ÉTABLISSEMENT MÉDICO-SOCIAL CONFRONTÉ À UNE INTRUSION INFORMATIQUE, NOTAMMENT POUR MIEUX GÉRER UNE CRISE DE CE TYPE ?

“ Plusieurs conseils peuvent être donnés :
La notion d'existence de sauvegarde du système d'information, par ailleurs isolée du réseau informatique pour éviter qu'elles soient elles-mêmes infectées, est primordiale. C'est ce point précis qui va définir la remédiation rapide ou non du système d'information, ainsi que son niveau d'exhaustivité ; en cas de détection d'une attaque, un signalement sans délai aux services de l'ANSSI et « cyberveille » permet d'être accompagné par des vrais spécialistes du domaine et d'obtenir des conseils sur la manière de gérer la crise ; la mise en place d'une cellule de crise en complément des équipes techniques permet d'une part de pouvoir gérer les priorités et construire les consignes à donner aux équipes opérationnelles, mais d'autre part de pouvoir traiter les questions autour de la prise en charge des patients (informations des équipes de soins, organisation potentielle de déport d'activités, échanges auprès des tutelles...).

Chaque établissement doit avoir notion du niveau de criticité de chacun des pans de son système d'information, afin de vérifier pour les plus importantes l'existence des procédures dégradées. Il ne faut pas négliger les activités connexes aux soins (ex : logistique) car leur incapacité à réaliser leurs missions a de vrais impacts (ex : stérilisation, restauration).

Enfin, il faut avoir conscience que la gestion d'une cyberattaque s'apparente plus à une course de fond qu'à un sprint, ce qui veut dire qu'il faut avoir en tête de ménager les équipes (informatique, direction, soignants) afin d'assurer leur rotation sur potentiellement plusieurs jours et ne pas être tenté de mettre la totalité des ressources en parallèle sur des cycles longs (i.e., supérieurs à 24 heures). ”

POUR
EN SAVOIR PLUS

- *La sécurité du système d'information des établissements de santé,* Cédric Cartau, Presses de l'EHESP, 2018
- *Cyber résilience, les cyberattaques,* guide de l'Association pour la sécurité des systèmes d'Information de santé (APSSIS)
- *Attaques par rançongiciels : comment les anticiper et réagir en cas d'incident,* guide de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), 2020
- *Guide de passation des marchés publics pour la cybersécurité des hôpitaux,* Agence européenne pour la cybersécurité des hôpitaux (ENISA), 2020
- *Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé,* rapport public 2020, ministère des Solidarités et de la Santé
- *Etat de la menace rançongiciel à l'encontre des entreprises et institutions,* rapport ANSSI, mars 2021
- *Cybersécurité, nouveau défi des établissements de santé et médico-sociaux,* Livre blanc du SHAM, 2021
- *Fuite de données, l'attrait des cybercriminels pour les données médicales,* Livre blanc Orange Cyberdéfense, 2021

DÉJÀ PARUS

1. *Comment réussir une opération de* ***déménagement*** *à l'hôpital ?* - 2019
2. *Comment mettre en place une* ***plateforme territoriale*** *de* ***téléradiologie*** *?* - 2019
3. *Améliorer le parcours des patients avec* ***les nouveaux outils de téléphonie*** - 2019
4. *Comment réduire sa* ***consommation énergétique*** *?* - 2019
5. *Maîtriser* ***le Value Based Procurement****, nouvelle technique d'achat* - 2020
6. *Garantir les soins de proximité grâce à la* ***télémédecine*** - 2020
7. *Comment optimiser et gérer la* ***maintenance de ses équipements biomédicaux*** *?* – 2020
8. *Comment transformer sa* ***logistique*** *pour assurer la qualité des soins ?* - 2021
9. *Améliorer* ***le bien-être au travail*** *à l'hôpital* - 2021
10. *Comment repenser* ***l'alimentation*** *dans le secteur de la santé ?* - 2021
11. *Comment se prémunir des* ***cyberattaques*** *? - 2021*

À PARAÎTRE

12. *Les grands enjeux* ***RSE*** *du secteur de la santé - 2022*

La cybermenace est réelle. Et elle aussi de plus en plus banale. Les actes de cybermalveillance dans le secteur de la santé ne cessent d'augmenter : 41% des incidents informatiques signalés en 2018, 60% deux ans plus tard. Début 2021, plusieurs hôpitaux ont été victimes d'intrusion informatique et de chiffrement de leur système d'information. Vols de données, d'identités, racket, demandes de rançons sont aujourd'hui monnaie courante.

En raison de la numérisation grandissante des activités et de la prise en charge des patients et résidents, aucun établissement sanitaire ou médico-social n'est à l'abri. Le secteur est d'ailleurs une priorité du volet cybersécurité de France Relance. Se protéger passe naturellement par le déploiement d'équipements boucliers, mais également par l'achat de prestations (audits, tests, accompagnement) afin de définir une politique de sécurité informatique pérenne, basée sur une démarche d'amélioration continue, et le respect d'une hygiène numérique de tous les instants.

Rédigé avec l'aide d'experts du sujet, ce guide fait le tour de la question, inventorie les dangers et les recettes utilisées par les hackers, et indique aux décideurs quelles sont les voies à suivre pour parer aux principaux risques.

resah
Réseau des Acheteurs Hospitaliers

Appuyons la transformation du système de santé par les achats