E-Santé

CYBER SÉCURITÉ

DARK WEB

100 % des hôpitaux français sont susceptibles d'être hackés

Dossier réalisé par Arnaud Janin

LE RISQUE D'INTRUSION DE HACKERS ET DONC DE VOL DE DONNÉES DE SANTÉ CROÎT AVEC L'INFORMATISATION DES HÔPITAUX ET L'INTERCONNEXION GALOPANTE AVEC LES ACTEURS DU SECTEUR. POUR AUTANT, MÊME SI LA SANTÉ EST EN RETARD DANS SA POLITIQUE DE SÉCURITÉ, DES VIGIES, LES RSSI SONT CHARGÉS D'ÉDUQUER LE PERSONNEL EN MATIÈRE DE PROTECTION ET D'ÉTEINDRE LE FEU EN CAS D'ATTAQUES RÉELLES. ENQUÊTE.

Panique à l'hôpital Charles-Nicolle de Rouen le 16 novembre dernier. Le CHU de la préfecture de Seine-Maritime a été victime ce samedi matin d'une grosse panne informatique. *« Il y a eu une attaque informatique hier à 19H45. Dès que nous avons vu que nous étions attaqués, nous avons décidé d'arrêter à 20 heures notre système d'information pour éviter que l'attaque ne se propage »*, a déclaré Rémi Heym, directeur de la communication du CHU, ajoutant que l'établissement avait dû *« repasser à la bonne vieille méthode du papier et du crayon »*. Ce fut le cas aussi pour le groupe Ramsay santé le week-end du 10 et 11 août 2019, premier pôle de cliniques privées en France. Il a fallu une semaine entière pour le groupe pour revenir à la normale. Depuis 2014, l'explosion des *ransomware* avec des très grosses campagnes de hacking a eu un impact important sur les systèmes d'information de certaines structures de santé. Philippe Loudenot, Fonctionnaire de sécurité des systèmes d'information et de sécurité de défense, a été l'un des premiers à avoir rapporté l'existence de ce type de virus.

LA VALEUR DE LA DONNÉE MÉDICALE

Pourquoi les données de santé des établissements de santé intéressent particulièrement les hackers ? Selon Vincent Trely, consultant en stratégies numériques de santé, *« la donnée médicale a de la valeur.* On trouve sur le dark net *des bases de don-*

nées d'hôpitaux vendues plusieurs centaines de milliers d'euros, voire plusieurs millions. » Et au fur et à mesure que la base de données grandit, son prix prend aussi de la valeur. Les acheteurs potentiels de ces masses d'informations de santé sont des États, voire des grandes entreprises dans le cadre de la guerre économique qui utilisent ces données stratégiques sur les populations, la recherche, etc. D'où l'intérêt par exemple de dérober des dossiers en masse, afin de constituer des bases de données pour la recherche. Difficile en fait de savoir qui est intéressé par l'achat de ces dossiers médicaux, car il n'y a pas de preuve, le *dark web* étant par définition anonyme. Toutefois, à défaut de désigner des personnes, plusieurs motifs sont évoqués par les experts. Premièrement, posséder le plus d'informations possible sur quelqu'un permet d'usurper plus facilement son identité. En témoigne le nombre grandissant d'usurpations d'identités de personnes décédées, qui ne porteront pas plainte ! Autre avantage de l'usurpation, il devient plus facile de travailler dans certains pays, voire de se faire prendre en charge ses soins en l'absence de mutuelle. Un autre objectif de se faire passer pour un autre, c'est d'obtenir des médicaments uniquement disponibles sur ordonnance. Ou bien avec des grandes quantités d'adresses de messageries, les hackers peuvent ainsi cibler des campagnes marketing afin de vendre des médicaments (et des contrefaçons) pour une pathologie particulière. Enfin, les hôpitaux sont aussi des cibles de choix des *hackers* pour leur faire du chantage, ce qui met aussi la pression sur les patients. Ces établissements en effet, constate Cédric Cartau, sont plus vulnérables : « *il y existe moins de culture de sécurité que dans les grosses organisations comme les banques* ». Particulièrement dans les hôpitaux stratégiques comme les CHU où tout est interconnecté. « *Si vous y arrêtez l'informatique, tout deviendra impossible. Les personnels n'auront plus accès ni aux examens de biologie, ni à l'imagerie, ni à Internet* », s'alarme Cédric Cartau. Pis, cumulé à une panne informatique, un arrêt de la téléphonie deviendrait une apocalypse. Facteur aggravant pour Auriane Lemesle, référente régionale sécurité des SI en charge de l'animation de la démarche sécurité numérique en santé pour les acteurs de santé des Pays de la Loire, au niveau de GCS e-santé, non seulement les structures ne sont pas assez protégées, mais elles sont de plus en plus interconnectées, ce qui accroît le nombre de « *portes ouvertes sur l'extérieur* ».

FAILLES

Quelles sont ces failles qui font rentrer le loup dans la bergerie ? Première porte d'entrée souvent citée par les experts, le mot de passe des messageries. Selon Damien Bancal (site Zataz), journaliste en cybersécurité, « *les professionnels utilisent le même mot de passe, ce qui est désastreux. Pourtant on a bien une clef pour chaque objet (voiture, maison…). Pourquoi ne fait-on pas pareil pour le web ?* »

> **Les gens ne voient pas le mal à se refiler les mots de passe**

Deuxième faille, le monde des objets connectés, domaine sur lequel Cédric Cartau attire en particulier l'attention : « *C'est une des pires vacheries qu'on ait inventées en termes de sécurité informatique. Mais nous avons beau alerter, nous prêchons dans le désert. On va sans doute se prendre quelques sinistres et on ne commencera à sécuriser ce bazar qu'après ces incidents.* »

Selon l'Asip (mai 2019), près de **500** incidents de cybersécurité depuis la mise en place de la cellule d'accompagnement cybersécurité des structures de santé (ACSS) en octobre 2017.

88 % des déclarations d'incidents proviennent des établissements de santé, 6 % d'autres structures de type Ehpad, 4 % des laboratoires de biologie médicale et 2 % des centres de radiothérapie.

Enfin, l'éducation au sein du secteur de la santé, même si elle commence tout doucement à prendre forme, est encore un chantier à défricher. Raison principale, on aurait manqué de pédagogie au début de l'installation des ordinateurs dans les hôpitaux, selon Vincent Trely : « *Dix ans après le début de l'informatisation, on est revenu expliquer aux hospitaliers les cartes à puces, les logins, les mots de passe. Mais c'était trop tard.* » Sur le terrain, le résultat est catastrophique : « *Les gens ne voient pas le mal à se refiler les mots de passe. De plus, contrairement à l'industrie, la santé n'est pas un environnement très obéissant. Une partie des opérateurs de soins disent ne pas avoir le temps de s'en occuper.* » Cédric Cartau modère ces propos. Soulignant le phénomène du cordonnier mal chaussé, la moitié des incidents informatiques seraient dus au non-respect des règles de base par les informaticiens. Quant à Damien Bancal, il en attribue la responsabilité à tous : « *Absolument tout le monde est responsable de ses actes et devrait être éduqué en termes de vigilance informatique.* » Il cible particulièrement « *les médecins qui croient souvent tout savoir, mais oublient de mettre à jour leurs logiciels et leur antivirus.* »

ÉQUIPEMENTS BIOMÉDICAUX

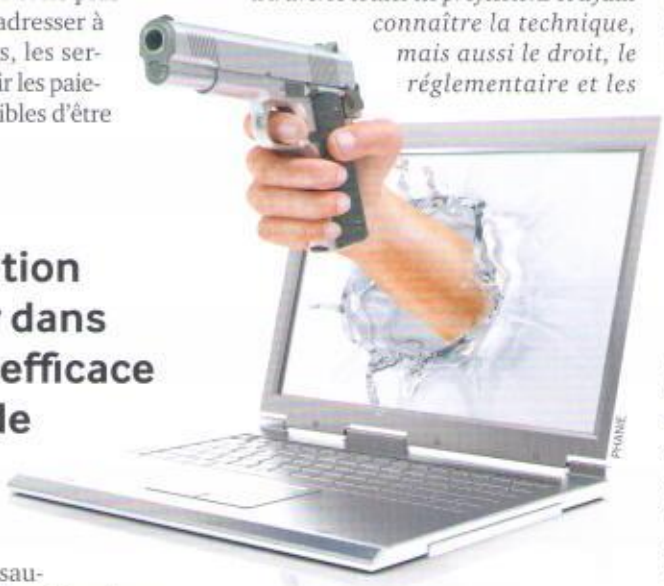
Après les comportements individuels, d'autres failles structurelles cette fois-ci sont aussi pointées du doigt par les experts. Selon Auriane Lemesle, « *les systèmes numériques des équipements biomédicaux, qui sont déjà pour la plupart obsolètes en matière de cybersécurité, sont, selon le ministère, à l'origine de la plupart des incidents dans le secteur de la santé ces derniers mois* ». Alors que leurs fournisseurs avaient l'habitude de se déplacer pour la maintenance, désormais ils ont tendance à connecter leur équipement à distance à partir du *web*. « *Déjà contraints par le marquage CE, ils refusent souvent d'installer des antivirus sur leur équipement et d'appliquer les mises à jour de sécurité* », argumente Auriane Lemesle. Plus incroyable encore, le système d'exploitation (mais toujours utilisé sur certains ordinateurs) comme Windows XP est devenu obsolète depuis plusieurs années en raison de la fin des mises à jour et donc de la maintenance du fabricant. Et ce n'est pas tout. « *Windows 7 [installé sur nombre d'ordina-*

teurs des hôpitaux] va stopper son support en janvier 2020 et donc par là même ses mises à jour. Donc potentiellement, si des failles sont identifiées, elles ne seront plus corrigées », déplore la RSSI.

NE JAMAIS PAYER LA RANÇON

Quand un établissement est victime d'un *ransomware*, doit-il payer la rançon ? Certainement pas. Selon Damien Bancal, il n'y a aucune certitude de récupérer ces données. Le pirate qui a agi peut même se faire pirater lui-même et ne plus avoir la possibilité de s'adresser à l'établissement. De plus, les serveurs dédiés pour recevoir les paiements sont aussi susceptibles d'être hackés. La seule solution est d'investir dans un dispositif efficace de sauvegarde. Et si cette dernière a lieu chaque nuit, il faut que la direction accepte de perdre toutes les données chiffrées par le hacker et qui ont été générées après la dernière sauvegarde.

> **La seule solution est d'investir dans un dispositif efficace de sauvegarde**



Ensuite, côté prévention pour mettre l'accent sur la sensibilisation du personnel, les RSSI passent par des affiches de sensibilisation, des vidéos courtes sur la confidentialité et la protection des mots de passe, etc. Un *escape game* co-construit avec des structures de santé a même été mis en place par l'ARS et le GCS e-santé Pays de Loire, afin de mettre en situation les hospitaliers, témoigne Auriane Lemesle, secrétaire générale de l'APSSIS.

RSSI, LE PIVOT

Pour mettre en œuvre cette politique d'information, les RSSI ont un rôle central. Leur profil ? Ce sont soit des experts très techniques mais qui sont plutôt considérés comme des responsables informatiques, soit des « *profils multicompétents* » très expérimentés et capables de réaliser l'interface entre les processus, les métiers, la technique et la réglementation. Recruté en 2009 et précurseur dans cette fonction, Cédric Cartau appartient à la deuxième catégorie. Alors qu'il était l'un des rares RSSI présents sur le marché de la santé, tous les autres secteurs industriels avaient déjà recruté de tels profils. Le manque de RSSI compétents dans les hôpitaux (6 000 en Île-de-France, 30 000 sur tout le territoire) est déploré par Vincent Trely : « *Ce n'est pas un métier simple, il est transversal, il traverse toutes les professions et il faut connaître la technique, mais aussi le droit, le réglementaire et les référentiels.* » Les directeurs d'hôpitaux qui sont aussi en général les mieux payés ont du mal à recruter des profils rémunérés à 80 000 ou 100 000 euros par an (salaires des RSSI des grands groupes industriels ou des banques). « *Ils recherchent des RSSI qui savent tout faire mais à des salaires deux fois moins importants.* » Une fois le RSSI recruté, le directeur de l'établissement est aussi confronté à un autre problème, le manque de moyens financiers. Dans une période de disette budgétaire, alors que le ministère n'a pas mis d'argent sur la table, quelle part accorder à la sécurité et à la prévention informatique alors que bien d'autres investissements plus rentables à long terme comme des matériels médicaux innovants seraient nécessaires ? Le RSSI est-il bien identifié ? La réponse est positive dans les CHU, mais bien moins évidente dans les plus petites structures. « *C'est assez hétérogène en fonction des établissements*, témoigne Auriane Lemesle. *On lui donne plus ou moins de poids, de rôle, de missions.* » Vincent Trely abonde dans ce sens : « *Même si les enjeux pour les hackers sont différents pour le médico-social qui est bien moins informatisé que le sanitaire, plus la structure est petite, plus elle est limitée en matière de personnel informatique* versus *les gros CHU qui disposent de grosses équipes d'informaticiens.* » Pour autant, avec la réforme des GHT, ces petits établissements vont peu à peu bénéficier d'une superstructure de sécurité au niveau du GHT. Mais il faudra encore un délai de cinq à dix ans pour que la convergence soit effective et acceptée par tous les acteurs.

DÉCLARATION DES INCIDENTS

En même temps que la réforme des GHT, les obligations imposées par le réglementaire sont toujours plus nombreuses : en effet, les autorités publiques ont imposé aux établissements de santé de déclarer les incidents de sécurité auprès du ministère depuis le 1er octobre 2017. Cette déclaration n'est pas passible de sanctions, mais est fortement recommandée aux établissements qui peuvent être poursuivis en justice s'ils manquent à leurs obligations de signalement. Le dispositif d'accompagnement a été étendu en 2019 à tous les autres établissements de santé dont les Ehpad.

Pourquoi les établissements renâclent-ils à communiquer sur leurs incidents, notamment à la presse ? Selon Vincent Trely, « *les RSSI n'ont pas toujours la liberté de parler, même s'ils ont au moins ce rôle de former le directeur général de l'établissement à communiquer sur l'incident auprès des journalistes. 100 % des hôpitaux peuvent se faire plomber. Il faut savoir coopérer et surtout déculpabiliser.* » Même si le directeur est bien formé pour gérer toutes les crises (sanitaire, sociale), il ne dispose pas encore des éléments de langage pour administrer les crises numériques. Là aussi, le RSSI doit les former. C'est pourquoi les établissements hormis quelques RSSI chevronnés refusent souvent de parler à la presse. Est-ce la peur de l'affichage médiatique et du détournement d'information ? Des témoignages sont donnés au compte-gouttes dans des colloques de spécialistes de la sécurité. À l'heure des *big data*, à quand le passage à une *big* sécurité dans les hôpitaux français ? •