Retour d'expérience, CHU de Rouen confronté à une attaque en 2019

Cédric Hamelin

Institut Droit et Santé
Université de Paris
Inserm UMRS 1145

Les cyberattaques dans les établissements de santé : enjeux et protection

Actes du colloque en ligne en date du 17 mai 2021

Cédric Hamelin
Responsable Adjoint à la Sécurité du Système d'Information au CHU de Rouen, établissement support du GHT Rouen Coeur de Seine

Retour d'expérience, CHU de Rouen confronté à une attaque en 2019

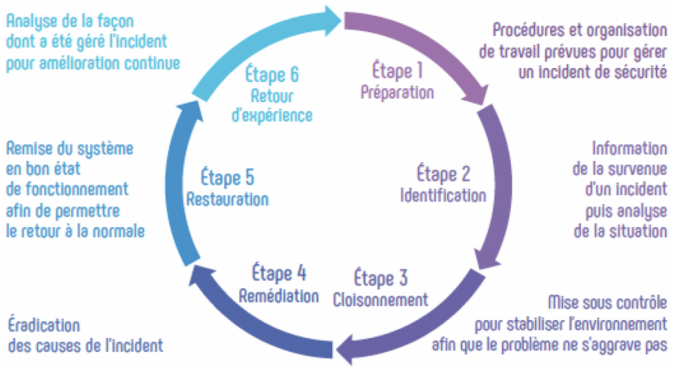
Afin de comprendre l'environnement dans lequel la cyberattaque du Centre Hospitalier Universitaire (CHU) de Rouen s'est produite, il est judicieux d'apporter quelques éléments de contexte. Au dernier classement établi par un grand quotidien national, le CHU de Rouen est le 12ème établissement de santé français. En prenant en compte uniquement les indicateurs autour des outils numériques (nombre de postes de travail, serveurs, applications, etc.), il se situe même aux alentours de la 8ème place des établissements de santé français, avec un budget de 750 millions d'euros et environ 12 000 agents, que ce soit du personnel administratif, médical ou des soignants. Le CHU est un établissement multi-sites qui est réparti sur 13 sites avec à la fois des sites qui concernent des magasins (matériel, médicaments), des distributions de repas que ce soit pour les patients ou le personnel à l'intérieur mais aussi à l'extérieur de l'établissement. Enfin, d'autres sites sont rattachés au CHU de Rouen et concernent le *Medical training center*, un service de formation proposé à l'extérieur.

2 500 lits sont répartis sur 5 sites. Il y a dix blocs opératoires pour une moyenne de 130 interventions chirurgicales programmées par jour, 400 passages par les urgences par jour et jusqu'à 2 000 consultations par jour ouvré soit un total de 512 000 par an.

Aujourd'hui les systèmes d'information sont utilisés par tous les agents ou presque de l'établissement au travers des différentes activités professionnelles, les agents sont amenés à utiliser des postes de travail, des tablettes, des smartphones… Il y a donc une dépendance du numérique qui s'est créée et qui va tendre à exploser dans les prochaines années.

Les SI permettent de traiter un nombre important de données qui vont à la fois de la gestion des données RH liées aux agents de l'établissement à la gestion des données administratives pour l'accueil des patients dans l'établissement.

Il y a aujourd'hui environ 300 applications métiers hébergées au sein de l'établissement qui sont accessibles sur l'un des 6 500 postes de travail et qui sont basées sur 900 serveurs sur le réseau interne. Un établissement de santé est nécessairement ouvert vers l'extérieur, le CHU de Rouen est l'établissement support d'un Groupement Hospitalier de Territoire (GHT) qui comprend 9 établissements. Enfin, il y a également 270 conventions actives qui renvoient à des échanges extérieurs avec 200 établissements externes, qu'ils soient des partenaires publics ou privés.



Le 15 novembre 2019, en quelques minutes, une cyberattaque a tenté de mettre à l'arrêt total le CHU.

La gestion d'une cyberattaque est basée sur six grandes phases. La première phase est la préparation de la gestion de la crise comprise entre le moment du premier appel sur l'indisponibilité d'une application et la fin de la constitution de la cellule de crise comprenant « l'escalade de la gestion d'incident». Durant cette période, une trentaine de personnes ont été rappelées en moins de deux heures après le premier appel sur le site avec pour chacun une action définie pour basculer sur la suite des étapes. Le CHU n'a ici pas eu la crainte de faire appel à une aide extérieure, en l'occurrence celle de l'ANSSI et du HFDS (ministère) pour compléter le dispositif de la cellule de crise.

Ensuite, il faut identifier la cause de l'incident en faisant état des lieux de la menace et en investiguant pour comprendre le type d'attaque subi.

Puis, a lieu le cloisonnement afin de mettre en place le plan d'action. Le CHU a souhaité s'attacher à ce que tout ce qui n'a pas été impacté ne le soit pas par répercussion. L'idée était d'éviter que l'attaquant puisse continuer à propager le rancongiciel sur d'autres postes de travail ou sur d'autres serveurs. En ce sens, le choix a été fait d'isoler les sauvegardes pour les préserver et anticiper la reconstruction future mais aussi de couper l'ensemble des flux internes. En

effet, un poste sain ne doit pas être infecté ou être utilisé par rebond.

Au CHU de Rouen les étapes deux et trois ont été réalisées en parallèle. Le souhait général était que l'attaque n'ait pas d'impact sur l'extérieur ; ainsi une décision forte a été prise de fermer l'accès à l'extérieur.

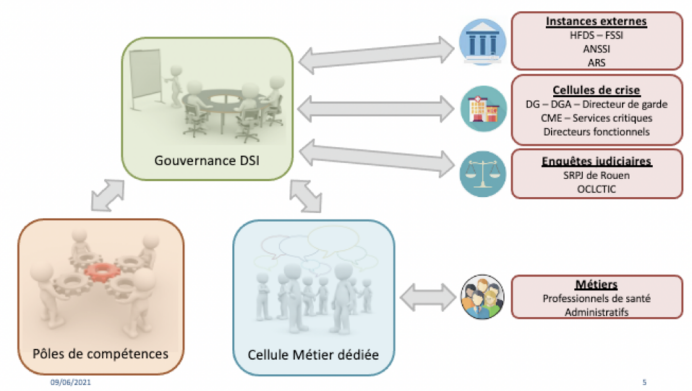
Après cela, il y a l'étape de la remédiation dans laquelle l'objectif est de voir comment bloquer puis éradiquer la menace en se basant sur les informations collectées lors de la phase d'identification.

L'étape de restauration arrive ensuite et n'est possible que dès lors que la menace ne se propage pas et n'est plus active. Elle représente la remise du système en bon état de fonctionnement pour permettre le retour à la normale. Le CHU s'est servi du système de sauvegarde prévu à cet effet. En l'espèce, il y a eu une reconstruction en moins de 48h des applications les plus critiques (stérilisation, blocs opératoires, urgences, dossiers patients, etc.). 95 % des applications métier étaient à nouveau disponibles sous une quinzaine de jours ainsi que le rétablissement des accès au réseau internet.

La dernière étape est le retour d'expérience afin de constater, en interne, ce qui a très bien fonctionné et identifier les axes d'amélioration et les anomalies dans le traitement de la crise afin de pouvoir s'améliorer. Ensuite, il y a eu les retours d'expérience à froid dont l'idée est de partager avec les instances externes pour partager en prévision d'autres cyberattaques et être en capacité de se préparer.

L'organisation de la cellule de crise est particulière, elle doit être adaptée à chaque établissement, celle dans le schéma ci-dessous étant propre au Centre Hospitalier Universitaire de Rouen, elle dépend de la façon dont chaque établissement fonctionne, le positionnement du DSI et du RSSI, etc. L'idée était, comme déjà précisé, qu'en moins de deux heures une trentaine de personnes soient disponibles sur le site pour répondre à l'incident. La cellule de crise a commencé par la mise en place de la gouvernance de DSI. L'idée est qu'il y avait quatre personnes permanentes qui devaient être présentes pour le pilotage au niveau du service informatique de la crise dans le but d'être en interaction avec les instances externes (HFDS, ANSSI, ARS). Elle est aussi en lien avec la cellule de crise qui devait informer régulièrement par des points toutes les trois à six heures avec la direction générale, avec la CME et les directeurs fonctionnels. On s'est attaché à ce qu'en interne l'information soit suffisamment relayée pour que les métiers puissent comprendre que l'on est dans la situation la plus maîtrisée possible mais également pour que l'on puisse avoir des remontées de terrain pour comprendre les éventuelles corrections à apporter au plan d'action dans la gestion de crise. Enfin, elle est en lien avec les enquêtes judiciaires avec des échanges réguliers avec le service de police par rapport à la situation en l'espèce.

Sur les premières 6/12h, la problématique était l'impossibilité de communiquer auprès des métiers car les messageries professionnelles internes n'étaient plus fonctionnelles. Ce qui a très bien fonctionné, c'est l'apport d'une cellule métier dédiée, équipe rattachée à la DSI et composée de ressources comme par exemple des anciens infirmiers, qui ont été déployés sur le terrain dans le but d'expliquer ce qu'il se passait et d'accompagner les équipes dans l'utilisation des modes dégradés.



Du point de vue des conséquences d'une cyberattaque, il y a un volet technique d'une part mais également d'autres impacts constatés par le CHU.

Tout d'abord, il y a les impacts organisationnels qui tiennent. En premier il y a eu un déport d'activité auprès d'établissements extérieurs sur le premier week-end qui a notamment touché le service de stérilisation. A aussi été constatée une adaptation des procédés de prise en charge et de suivi des patients par les services, du fait de l'absence d'accès aux systèmes d'information et de la mise en œuvre des procédures dégradées. À cet égard, on s'est aperçu que ces modes dégradés étaient très pratiques pour des utilisations de très court terme mais que lorsque cela dure entre 24 et 48 heures cela devient très compliqué. De plus, des problématiques ont été corrélées à d'éventuels enjeux réglementaires. Les activités de la Direction du SI sont restées perturbées pendant plusieurs semaines.

Puis, on retrouve les impacts en termes d'image. Aujourd'hui, les cyberattaques sont de plus en plus médiatisées, mais Rouen a été la première cyberattaque importante à l'encontre d'un CHU. Globalement, ce qui a été noté c'est que la communication était plutôt maîtrisée par l'établissement pour répondre aux attentes, au regard des préconisations des instances ministérielles ou judiciaires (ANSSI, HFDS, SRPJ). Cependant, cela n'a pas empêché les nombreux articles sur l'évènement ainsi que les commentaires au niveau de ces articles ou sur les réseaux sociaux. De plus, le CHU a rencontré une perte de confiance au niveau de certains partenaires et éditeurs qui demandaient de justifier si la situation était optimale ou si elle allait entraîner une dévalorisation de la sécurisation de leurs systèmes. Dans certains cas de figure, il a fallu faire intervenir le ministère avec certains des éditeurs pour pouvoir rouvrir certains accès. Enfin il y a eu beaucoup de retours négatifs par d'autres établissements sur l'absence de communication par les instances ministérielles sur l'origine de l'évènement, sur les aspects techniques, sur la mise en

œuvre d'un RETEX…

D'un point de vue règlementaire, les établissements de santé ont tout d'abord l'obligation de déclarer sur le portail dédié au signalement des événements sanitaires indésirables tout ce qui peut se passer en termes de cyberattaques[1]. Le Règlement général sur la protection des données (RGPD) énonce également des obligations. En effet, l'article 32 énonce l'obligation de sécurité du traitement à caractère personnel et sensible. L'article 33 du RGPD formule l'obligation de notification obligatoire sous 72 heures auprès de la Commission nationale d'informatique et des libertés (CNIL). Enfin, l'article 34 du RGPD exige la communication à la personne concernée d'une violation de données à caractère personnel.

Ensuite, il y a l'obligation d'un signalement auprès de la Direction des Archives départementales rattachée à la Préfecture[2], que ce soit à propos d'archives papiers ou numériques.

En outre, un dépôt de plainte contre X auprès du SRPJ ou du commissariat le plus proche doit être réalisé pour « Accès frauduleux dans un système de traitement automatisé de données » et/ou « Tentative d'extorsion ».

Enfin, il y a une déclaration obligatoire des événements indésirables associés aux soins.

Pour conclure, quelques mesures simples sont à préconiser, en premier lieu la mise en place des mesures techniques. Puis faire en sorte que les décideurs soient au fait de tous les risques qui pèsent sur les systèmes d'information. Enfin, il faut également mettre en place des phases de sensibilisation et de formation des agents aux risques liés aux outils numériques pour anticiper la survenue d'une cyberattaque voire les préparer.

Cédric Hamelin

Propos retranscrits par Sonia Cordon, juriste de l'Institut Droit et Santé

1 - Article 110 de la Loi de modernisation du système de santé du 26 janvier 2016

2 - Articles L211-1 et L211-4 du Code du Patrimoine des archives publiques