Cyberwal
by digital
wallonia

Les défis et les meilleures pratiques

de la cybersécurité dans le secteur de la santé

Wallonie Relance

Agence du Numérique

Table des matières

E.R.: Agence du Numérique | **Programme:** *"Cyberwal by Digital Wallonia"* | **Experts:** Jeremy Grandclaudon & Nina Hasratyan | **Rédaction:** Garance Wauthier | **Mise en page:** Hungry Minds

Les défis et les meilleures pratiques

de la cybersécurité dans le secteur de la santé

Avant-propos

Chers lecteurs,

Avec la multiplication et la sophistication des cyberattaques, la cybersécurité s'est imposée comme un enjeu fondamental pour nos sociétés, revêtant une importance critique tant pour les entreprises que pour les organisations publiques. Dans le secteur de la santé, cet enjeu acquiert une dimension encore plus essentielle, car il touche directement à la vie et au bien-être des citoyens. Ce livre blanc rassemble des témoignages révélateurs d'hôpitaux wallons qui ont subi des cyber-attaques. Leurs récits illustrent cette importance des enjeux de la cybersécurité pour le secteur. La protection des systèmes informatiques n'est plus une simple question technique, mais une responsabilité sociétale majeure.

*En Wallonie, cette priorité est au cœur de la politique numérique du Gouvernement, et l'Agence du Numérique joue un rôle clé en déployant le programme **Cyberwal**, qui s'inscrit dans la stratégie numérique du Gouvernement wallon, **Digital Wallonia**.*

***Cyberwal**, fer de lance de la cybersécurité en Wallonie, vise à renforcer la résilience des écosystèmes, notamment dans le secteur de la santé au travers de deux actions phares :*

- *La **Cyber Response Team (CRT)** est une équipe spécialisée, dédiée à l'intervention en urgence en cas d'incident de cybersécurité, réduisant ainsi les impacts sur les hôpitaux et autres établissements de santé. Ce dispositif, qui a déjà fait ses preuves dans d'autres régions, joue également un rôle préventif en offrant des conseils et des recommandations pour éviter de futures attaques.*

- *Le **simulateur numérique** est un outil innovant qui permet aux établissements de santé d'adopter une approche unique pour se préparer aux cyberattaques. En recréant des scénarios d'agression dans un environnement contrôlé, le simulateur offre au personnel l'occasion de développer ses compétences, d'affiner ses protocoles de sécurité et d'améliorer sa capacité à anticiper les menaces.*

*Ces actions ne représentent qu'un aperçu des nombreuses initiatives mises en œuvre en Wallonie par une multitude d'acteurs, illustrant ainsi un engagement collectif face aux défis de la cybersécurité. En unissant la recherche, la formation et l'accompagnement des entreprises autour du programme **Cyberwal by Digital Wallonia**, la Wallonie a réussi à créer une synergie forte et innovante.*

Je vous souhaite une lecture enrichissante et inspirante.

Cordialement,

Cassandre Laurent
Directeur Général, Agence du Numérique

Introduction

La menace grandissante des cyber-attaques dans le secteur des soins de santé : une réalité incontournable

par SANTHEA et UNESSA

Le paysage numérique des soins de santé, autrefois vu comme un catalyseur pour améliorer la qualité et l'accessibilité des soins, est désormais confronté à la cybermenace en constante évolution. Jusqu'ici, ces attaques ont ciblé des secteurs jugés plus vulnérables. Aujourd'hui, l'ensemble du secteur des soins de santé, des hôpitaux aux maisons de repos, en passant par les cliniques spécialisées et les centres de soins à domicile est devenu une cible de choix. Ce contexte impose une réflexion approfondie sur la gestion des incidents de sécurité dans ces structures, où la technologie de pointe et la gestion des données de santé jouent un rôle de plus en plus central.

La **gestion d'incidents** n'est plus un simple volet technique, mais **un enjeu stratégique essentiel** pour la survie des établissements de soins de santé devenus des entités critiques, qu'ils soient grands ou petits, complexes ou modestes. La capacité de ces structures à se prémunir, à répondre rapidement et efficacement aux crises numériques est devenue un facteur clé de résilience et de continuité des services de soins. La question n'est plus de savoir si mais quand une structure de santé sera visée par une cyberattaque.

UN SECTEUR VULNÉRABLE ET DES CONSÉQUENCES MAJEURS

Les cybercriminels exploitent les failles des systèmes numériques pour provoquer des perturbations massives, allant du vol de données sensibles à l'interruption des services critiques, avec des conséquences directes sur la sécurité des patients, l'organisation interne, la communication externe, la gestion des ressources humaines et la viabilité des établissements.

LES DÉFIS SPÉCIFIQUES DE LA GESTION D'INCIDENTS DANS LE SECTEUR DES SOINS DE SANTÉ

La gestion d'incidents dans les soins de santé présente des défis qui vont bien au-delà de ceux rencontrés dans d'autres secteurs. Chaque établissement doit faire face à des enjeux spécifiques liés à la nature de ses services. Pour les hôpitaux, il s'agit de maintenir la continuité des soins critiques, où la moindre panne peut mettre en danger la vie des patients et engendrer de sérieux dysfonctionnements organisationnels sur le long terme. Pour les maisons de repos et les cliniques, la gestion des incidents se concentre souvent sur la protection des données sensibles des résidents et la garantie de la sécurité des systèmes de support.

Les ressources limitées de certains établissements rendent la tâche encore plus ardue. Tandis que les grands hôpitaux peuvent se permettre tant bien que mal d'investir dans des équipes de sécurité informatique dédiées et des technologies de pointe, les plus petites structures doivent souvent jongler avec des moyens restreints tout en garantissant un niveau de sécurité suffisant pour protéger leurs systèmes et leurs patients. Cette disparité dans les ressources ajoute une couche supplémentaire de complexité à la gestion des incidents, nécessitant des approches adaptées et souvent très créatives.

STRATÉGIES POUR UNE GESTION D'INCIDENTS EFFICACE: PRÉPARATION, RÉACTION ET RÉCUPÉRATION

Pour tous les établissements de soins de santé, la clé réside dans la **préparation**. Un **plan d'action** robuste et bien conçu est **indispensable pour anticiper les incidents et y répondre de manière coordonnée**. Ces plans de continuité et de rétablissement doivent être adaptés aux ressources disponibles et régulièrement mis à jour pour faire face aux nouvelles menaces. Pour les plus petites structures, cela peut inclure des partenariats avec des services de sécurité externe ou l'adhésion à des réseaux de soutien régionaux ou nationaux.

La **réactivité** est également **cruciale**. Dès qu'une attaque est détectée, il est vital de réagir rapidement pour limiter les dégâts. Les premières actions, telles que l'identification de la menace, la contention du problème, et la protection des données sensibles, doivent être exécutées avec précision et rapidité. Ce processus est souvent plus délicat pour les petites structures, où la disponibilité des compétences techniques, peuvent être limitées, mais il n'en est pas moins crucial.

La **phase de récupération** est tout aussi importante. Une fois la menace écartée, il faut restaurer les systèmes, récupérer les données et s'assurer que les services reprennent leur cours normal. Pour cela, des procédures claires doivent être en place, adaptées à la taille et à la complexité de chaque établissement. L'objectif est de minimiser les perturbations pour les patients et de revenir à un fonctionnement normal le plus rapidement possible. Un aspect important à ne pas négliger est l'impact humain au niveau du personnel : sensation d'intrusion, culpabilité, stress organisationnel…

LEÇONS TIRÉES ET RENFORCEMENT DE LA RÉSILIENCE: VERS UNE AMÉLIORATION CONTINUE

Chaque incident est une occasion d'apprendre et de renforcer les défenses. L'**analyse post-incident** est cruciale pour identifier les failles et améliorer les processus de gestion des incidents. Ces leçons doivent être partagées au sein du secteur, permettant à tous les établissements, quelle que soit leur taille, de bénéficier des expériences des autres.

L'**innovation** et l'**adaptation** doivent être **au cœur de la stratégie de gestion des incidents**. Pour les petites structures, cela peut signifier l'adoption de solutions plus légères mais efficaces, ou la formation continue du personnel pour qu'il puisse réagir rapidement en cas de crise. De même, il est essentiel de promouvoir une culture de la résilience, où chaque membre du personnel, qu'il soit administratif ou clinique, est conscient des risques et connaît les protocoles à suivre en cas d'incident.

CONCLUSION: UN APPEL À L'ACTION POUR TOUS LES ACTEURS DES SOINS DE SANTÉ

Dans ce contexte de menaces croissantes, la gestion des incidents de sécurité ne doit plus être considérée comme une simple obligation réglementaire, mais comme un impératif stratégique pour l'ensemble du secteur des soins de santé. Cette deuxième édition du livre blanc se veut un guide précieux pour les dirigeants, qu'ils soient à la tête de grands hôpitaux ou de petites structures, les incitant à prendre conscience de l'importance de la gestion des incidents et à investir dans des stratégies adaptées à leurs réalités.

L'avenir des soins de santé dépend de notre capacité à anticiper, réagir et nous relever face aux menaces numériques. Chaque établissement a un rôle à jouer en tant que partie prenante pour garantir la sécurité des soins. En faisant de la gestion des incidents une priorité, nous pouvons non seulement protéger nos institutions, les données de santé à caractère personnel mais aussi assurer la continuité des soins pour ceux qui en dépendent le plus. **Ensemble, bâtissons un secteur des soins de santé où la résilience face aux cyberattaques n'est pas seulement un objectif, mais une réalité partagée.**

Philippe Costard
Conseiller en Sécurité de l'Information, **SANTHEA asbl**

Fabian Céréssia
Responsible ICT & BI, **UNESSA asbl**

Le Centre pour la Cybersécurité Belgique (CCB), un partenaire clé pour accompagner les hôpitaux face aux cyberattaques

Le secteur hospitalier est particulièrement vulnérable aux cyberattaques en raison de la nature sensible des données concernées et de l'importance des services en jeu. Face à l'augmentation des cyberattaques, les hôpitaux sont souvent mal préparés pour gérer les incidents et rétablir leurs systèmes rapidement. Face à ces défis, la résilience, c'est-à-dire la capacité à anticiper, résister et se remettre rapidement des incidents, est devenue essentielle.

Dans ce contexte, le **Centre pour la Cybersécurité Belgique (CCB)** et ses différents services opérationnels - en particulier le **CERT (Cyber Emergency Response Team)** - jouent un rôle déterminant dans l'accompagnement des hôpitaux. Le CERT, notamment, peut intervenir en première ligne de défense dans la gestion des cyberincidents, avec pour mission principale d'analyser, contenir et éradiquer les menaces ciblant les infrastructures critiques, y compris celles des établissements de santé. Cet article illustre comment les services du CCB soutiennent les hôpitaux à travers chaque étape cruciale de la gestion des cyberincidents, de la détection à la récupération.

VULNÉRABILITÉS PROPRES AUX HÔPITAUX : LE DIAGNOSTIC DU CCB

Les hôpitaux font face à des défis importants en matière de cybersécurité, souvent aggravés par des infrastructures vieillissantes et complexes. Le manque de plans de réponse aux incidents et de plans de reprise après sinistre est fréquent. En conséquence, ces institutions sont mal préparées pour gérer les cyberattaques et rétablir leurs systèmes critiques rapidement.

L'un des points faibles récurrents est l'absence de la double authentification : les mots de passe demeurent souvent le principal moyen d'accès, ce qui augmente considérablement les risques d'intrusion. Par ailleurs, la gestion des correctifs (patch management) pose souvent problème : les dispositifs réseau et les VPN ne sont pas mis à jour assez rapidement, ce qui expose les systèmes hospitaliers aux menaces. Ce délai entre la disponibilité d'un correctif et son installation effective est une fenêtre d'opportunité pour les attaquants.

Les équipements médicaux connectés constituent une autre faiblesse. Ces machines, souvent non segmentées au sein des réseaux, facilitent une propagation rapide de l'attaque à tout le système. Souvent sous la gestion de fournisseurs externes, elles sont fréquemment **connectées en permanence** aux réseaux du fournisseur pour des raisons de support, créant ainsi une **voie d'accès potentielle** vers l'intérieur du réseau de l'hôpital en cas d'attaque ciblant la chaîne d'approvisionnement (supply chain attack). Pire encore, certaines d'entre elles sont « impatchables » et ne peuvent ainsi pas recevoir de mises à jour de sécurité, ce qui augmente leur vulnérabilité face aux cybercriminels. **Pour réduire cette exposition au risque, il est fortement recommandé d'isoler ces machines du reste du réseau hospitalier** afin de limiter leur impact en cas de compromission.

La gestion des accès à distance est aussi un point d'attention. Le vol d'identifiants, et le commerce de ceux-ci à bas prix sur le Dark Web, constituent souvent le point de départ pour l'accès aux réseaux hospitaliers, ce qui accroît davantage l'exposition de ces infrastructures critiques.

Enfin, **la gestion des sauvegardes (backups)** des systèmes hospitaliers n'est **pas toujours optimale**. Trop souvent, ces sauvegardes sont connectées aux systèmes principaux et peuvent ainsi être la cible d'attaques, notamment par ransomwares. Pour renforcer la sécurité, il est fortement recommandé de **conserver des copies de sauvegarde hors ligne** et de veiller à ce que les systèmes de backup ne soient pas connectés avec des utilisateurs du domaine (**Active Directory**) pour limiter le déplacement depuis un domaine compromis vers les backups. Pour les hô-

pitaux, le non-respect de ce principe de sauvegarde déconnectée aggrave la situation et peut conduire à la parte de l'ensemble de leurs données en cas de compromission. Le CCB note que cette faille est particulièrement critique dans un environnement où la professionnalisation des hackers leur permet de mener des attaques de plus en plus rapides, parfois en l'espace de quelques heures seulement.

TYPOLOGIE DES ATTAQUES SUBIES PAR LES HÔPITAUX

Les hôpitaux, comme d'autres organisations, sont exposés à un large éventail de cyberattaques, mais certaines menaces reviennent plus fréquemment et avec une intensité particulière. Parmi les attaques les plus courantes identifiées par le CCB figurent :

1. Les ransomwares et l'exfiltration de données

Les **ransomwares** représentent l'une des attaques les plus courantes et destructrices dans le secteur hospitalier. Ces attaques commencent généralement par l'infiltration des systèmes, suivie du **chiffrement des données critiques**, procédés qui rendent les informations inaccessibles et paralysent les opérations de l'hôpital. Cependant, les cybercriminels ne s'arrêtent souvent pas là. Une nouvelle tendance identifiée par le CCB montre que les **hackers utilisent un double moyen de pression**. En plus de demander une rançon pour décrypter les données, ils menacent **de divulguer des informations sensibles** exfiltrées si leurs demandes ne sont pas satisfaites. Cette menace supplémentaire est particulièrement redoutée par les hôpitaux, étant donné la nature hautement confidentielle des données en question, notamment celles relatives aux patients et aux traitements.

2. L'accès non autorisé via des identifiants compromis

L'utilisation d'identifiants volés, souvent récupérés sur le Dark Web, est une autre méthode courante pour infiltrer les systèmes hospitaliers. Ces informations, fréquemment vendues à bas prix, permettent aux attaquants d'accéder aux réseaux et de compromettre les systèmes rapidement. Le CCB souligne que cette vulnérabilité est souvent exacerbée par l'absence de mécanismes de **double authentification**, rendant l'accès à distance encore plus simple pour les cybercriminels.

3. Les attaques DDoS

Bien que moins fréquentes, les **attaques par déni de service distribué (DDoS)** sont parfois **utilisées pour surcharger les systèmes hospitaliers**, rendant inaccessibles les services en ligne ou les infrastructures critiques. En comparaison avec d'autres secteurs, les hôpitaux semblent cependant moins ciblés par ce type d'attaques, même si elles restent une menace.

Le CCB constate également une évolution rapide des tactiques utilisées par les cybercriminels. Si auparavant les intrusions prenaient plusieurs jours, voire des semaines, les dernières attaques observées montrent une réduction drastique du temps d'action. Dans certains cas, seules quelques heures séparent l'intrusion du verrouillage complet des systèmes.

En raison de la nature sensible de leurs données et de la criticité de leurs opérations, les hôpitaux sont devenus des cibles de choix pour ce type d'attaques. La vitesse et la complexité des incidents soulignent l'importance d'une préparation rigoureuse et d'une réponse rapide.

LA RÉPONSE DU CCB : ASSISTANCE, COORDINATION ET CONSEILS

Face à l'ampleur des cybermenaces qui pèsent sur les hôpitaux, le rôle du CCB est fondamental pour les aider à répondre efficacement aux attaques. LeCCB intervient à plusieurs niveaux : il offre une assistance proactive, coordonne les réponses aux incidents et fournit des conseils techniques pour restaurer les systèmes compromis. Cependant, l'accompagnement offert a des limites précises et se concentre essentiellement sur l'analyse et la gestion des incidents, plutôt que sur la reconstruction complète des infrastructures.

1. Assistance proactive et systèmes d'alerte

L'**Early Warning System (EWS)** proposé par le **CCB**, via la plateforme **Safeonweb@work**, fournit une alerte précoce sur les menaces au sein des réseaux des organisations enregistrées. Le système envoie des notifications spécifiques lorsqu'une vulnérabilité ou une infection est signalée par les partenaires du CCB spécialisés en matière de veille. Les informations sont recueillies à partir de sources commerciales et ouvertes. Les organisations sont averties si une menace est détectée sur les adresses IP ou domaines qu'elles ont enregistrés.

Pour bénéficier pleinement de ce service, il est recommandé que l'hôpital enregistre, entre autres, ses adresses IP, noms de domaine, ainsi que des informations sur les technologies utilisées sur la plateforme. Bien que le **CCB** puisse envoyer des alertes de sécurité dès qu'il le juge nécessaire, indépendamment de l'inscription sur la plateforme, s'enregistrer permet de s'assurer que ces alertes sont envoyées directement aux bonnes personnes au sein de l'organisation. Le CCB recommande d'utiliser ces notifications pour agir rapidement et atténuer les risques avant qu'une attaque ne se produise.

Cependant, il est important de noter que Safeonweb@work ne fournit pas de support opérationnel sur les actions à entreprendre après la réception de ces alertes, cette tâche incombe aux équipes internes de l'organisation. Ce service est entièrement gratuit et vise à offrir une couche supplémentaire de surveillance proactive aux hôpitaux, qui peuvent ainsi bénéficier d'une vigilance accrue face aux cybermenaces.

2. Réponse à l'incident

Lorsqu'un cyberincident survient dans un hôpital, le CCB peut intervenir de manière flexible pour s'adapter aux besoins spécifiques de chaque situation. Son rôle principal est d'apporter des **conseils techniques** et de **coordonner la réponse** afin que les actions soient menées dans le bon ordre.

Tout d'abord, le CCB évalue le type d'assistance requis. Dans certains cas, il s'agit de **conseils proactifs** pour s'assurer que les bonnes pratiques sont respectées, par exemple le fait d'éviter de réinstaller immédiatement les systèmes infectés sans avoir au préalable identifié la porte d'entrée des hackers. Parfois, leur rôle se limite à la **coordination**, c'est-à-dire à s'assurer que les actions critiques sont effectuées de manière méthodique pour limiter les dégâts.

Si l'incident le justifie, le CCB peut également intervenir sur site pour mener une analyse technique approfondie. Les experts aident à identifier la source de l'intrusion, à comprendre comment les cybercriminels ont pénétré dans le système, et donnent des recommandations sur la **récupération** après l'attaque. Toutefois, leur implication a des limites : leur rôle est comparable à celui de **pompiers** qui éteignent l'incendie, mais ils ne participent pas à la reconstruction complète des systèmes après l'incident. Leur principale mission est de contenir la menace et de formuler des recommandations concernant les vulnérabilités identifiées.

En plus de la gestion technique, le **CCB** peut jouer un rôle dans la **communication de crise**. Son équipe de communication peut aider l'hôpital à communiquer efficacement avec le personnel, le public, voire, dans certains cas, avec les groupes de hackers eux-mêmes. Cependant, il est important de noter que le CCB ne communique jamais publiquement sur les victimes des cyberattaques, respectant ainsi la confidentialité des organisations touchées.

PLAN DE GESTION DES INCIDENTS ET OUTILS POUR RENFORCER LA RÉSILIENCE

Pour se préparer efficacement aux cyberattaques, il est essentiel que les hôpitaux disposent d'un plan de gestion des incidents clair, permettant une réponse rapide et organisée. Ce plan doit non seulement prévoir des procédures pour la gestion des attaques, mais aussi des solutions pour assurer la continuité des services critiques durant et après l'incident. Le CCB rappelle que les cyberattaques sont inévitables, et qu'il est impératif d'anticiper différents scénarios d'attaques en établissant des étapes de réponse précises. Cela inclut la détection précoce des menaces et la capacité à isoler rapidement les systèmes infectés.

Le CCB recommande de constituer une équipe de gestion des incidents regroupant les responsables IT, la direction et les équipes opérationnelles. Une bonne coordination entre les services permet de limiter les dégâts. En cas d'indisponibilité des systèmes, des solutions de communication alternatives doivent être prévues pour maintenir les opérations.

Par ailleurs, la gestion des sauvegardes est cruciale. Le CCB souligne que celles-ci doivent être déconnectées des systèmes principaux pour éviter qu'elles ne soient compromises. Une fois l'attaque contenue, une analyse approfondie est nécessaire avant de restaurer les systèmes, afin de s'assurer que la vulnérabilité exploitée a été correctement corrigée.

Pour accompagner les hôpitaux, le CCB propose plusieurs outils essentiels :

- Le **CyberFundamentals Framework**, un ensemble de mesures pratiques pour renforcer la sécurité des infrastructures hospitalières, notamment en matière de gestion des accès, de segmentation des réseaux et de correctifs. Ce référentiel aide à structurer la défense contre les cybermenaces et est accessible à toutes les organisations.

- Le **Cyber Security Incident Management Guide**, qui fournit une feuille de route détaillée pour naviguer à travers une crise cyber. Ce guide offre des recommandations pour identifier, contenir et résoudre les attaques tout en minimisant les nuisances. Il permet également de s'assurer que les hôpitaux prennent les bonnes décisions et se retrouvent un fonctionnement normal rapidement après un incident.

En s'appuyant sur ces ressources, les hôpitaux peuvent renforcer leur résilience face aux cybermenaces, anticiper les attaques et garantir la continuité de leurs services critiques.

PROTÉGER LES SYSTÈMES POUR PROTÉGER LES VIES

Les cyberattaques ne sont pas une menace abstraite, mais une réalité à laquelle les hôpitaux sont confrontés au quotidien. Chaque intrusion, chaque vulnérabilité, met en péril non seulement la **confidentialité des données** des patients, mais aussi la **continuité des soins**, un enjeu vital pour les hôpitaux.

C'est dans ce contexte que les hôpitaux doivent comprendre qu'au-delà de la réaction aux incidents, il est impératif d'intégrer la résilience au cœur de leurs stratégies. Cette résilience ne se construit pas du jour au lendemain, mais grâce à des outils, des procédures, et un accompagnement, tous adaptés à cette fin. Les ressources offertes par le **CCB** sont là pour soutenir cette démarche proactive.

S'il est évident que les défis sont nombreux — infrastructures vieillissantes, manque de ressources techniques et humaines, manque de formations spécialisées, vulnérabilités non corrigées — les **solutions existent**. La vraie question n'est pas de savoir si une attaque surviendra, mais **quand**. C'est pourquoi il est essentiel que chaque hôpital prenne le temps d'évaluer ses vulnérabilités, de se préparer en conséquence et, surtout, de s'appuyer sur les ressources disponibles pour renforcer ses défenses.

Le CCB ne se contente pas d'intervenir en urgence ; il agit en **partenaire stratégique**, fournissant les conseils et l'assistance nécessaires pour aider les hôpitaux, non seulement à se relever après une attaque, mais aussi à devenir plus résistants. Cette collaboration doit être perçue comme un atout majeur dans la lutte contre les cybermenaces. La résilience ne consiste pas uniquement à réagir à l'incident, mais à bâtir des systèmes capables de **prévenir** les attaques, **répondre** efficacement et **récupérer** rapidement.

Ensemble, grâce aux outils mis à disposition par le CCB, et avec le soutien du CERT, les hôpitaux peuvent relever ce défi et garantir que leur mission première — les soins — ne sera jamais compromise par une cyberattaque.

Le CHRSM face à la cyberattaque : malgré la crise, les patients ont pu compter sur une communication proactive et continue

par Bastien Ducarme

Le 26 mai 2023, le Centre Hospitalier Régional Sambre et Meuse (CHRSM) a été frappé de plein fouet par une cyberattaque majeure. En quelques heures, les deux sites de l'hôpital ont vu leurs systèmes informatiques paralysés par un ransomware, interrompant brutalement la plupart des activités de l'établissement, à l'exception des urgences vitales. Cette crise a forcé l'hôpital à activer immédiatement son plan d'urgence et à s'appuyer sur des méthodes de communication et de travail manuelles pour continuer à fournir des soins aux patients.

LA NATURE ET L'ÉTENDUE DE LA CYBERATTAQUE

L'attaque, orchestrée par le groupe derrière le **ransomware « NoEscape »**, a frappé le CHRSM aux premières heures du 26 mai 2023. Ce logiciel malveillant a ciblé spécifiquement les machines sous Windows, chiffrant la majorité des serveurs et postes de travail de l'hôpital. Rapidement, l'attaque a interrompu l'accès à des systèmes essentiels, dont l'annuaire Windows (Active Directory) et les systèmes de téléphonie en VoIP. Grâce à une intervention rapide, le personnel a pu stopper la propagation avant que tous les systèmes ne soient affectés, épargnant ainsi certaines sauvegardes critiques hébergées sur des serveurs Linux.

DÉTECTION ET PREMIÈRES RÉPONSES

C'est une infirmière qui, en tentant de se connecter au dossier patient informatisé (DPI) vers 3 heures du matin, a détecté le problème pour la première fois. Devant l'impossibilité d'accéder au système, elle a immédiatement alerté un technicien informatique. Ce dernier, en constatant un comportement anormal des systèmes, a pris la décision cruciale de contacter le directeur informatique, qui a rapidement compris la gravité de la situation. Le plan d'urgence a été activé sans délai, ordonnant la coupure complète du réseau pour empêcher la propagation du ransomware.

Peu après, le **CCB** (Centre pour la CyberSécurité Belgique) et le **CERT** (Cyber Emergency Response Team) ont été contactés pour intervenir. Les équipes du CERT sont arrivées sur place en début de matinée. Elles ont travaillé en étroite collaboration avec l'équipe informatique de l'hôpital pour contenir l'attaque, en se concentrant d'abord sur l'identification du vecteur de l'attaque et en lançant une enquête forensique approfondie.

Le CERT a également conseillé l'hôpital sur les meilleures pratiques pour sécuriser les systèmes restants et éviter toute nouvelle propagation du malware. Leur présence a été essentielle dans les premiers jours de la crise, jouant un rôle clé dans le retour progressif à la normale, bien que leur mission principale ait été d'éteindre le feu et d'assurer la stabilité initiale des systèmes avant de partir.

En dépit des efforts pour contenir l'attaque, le CHRSM a dû faire face à une autre conséquence grave : le vol et la publication de données sensibles. Les attaquants ont réussi à s'emparer de fichiers de sauvegarde qui contenaient des informations sur les patients et le personnel de l'hôpital. Conformément à leur mode opératoire habituel, les hackers ont laissé un fichier texte sur chaque bureau d'ordinateur affecté, expliquant la marche à suivre pour entrer en contact avec eux et négocier une rançon. Cependant, la direction du CHRSM a maintenu une position ferme dès le début, refusant toute négociation. En réponse à ce refus, les hackers ont mis à exécution leur menace et ont publié les données sur le Dark Web après l'expiration de leur ultimatum.

COMMUNICATION EN INTERNE ET EN EXTERNE

Face à la crise, la communication est devenue une priorité pour le CHRSM. Avec les systèmes numériques indisponibles, l'hôpital a dû rapidement s'adapter en revenant aux méthodes traditionnelles pour maintenir le lien avec ses équipes. Des **notes papier** ont été distribuées pour transmettre les informations essentielles, et des points de rassemblement ont été mis en place pour coordonner les actions sur le terrain. Les directions ont été incitées à se déplacer physiquement au sein des services pour s'assurer que le personnel était bien informé et soutenu.

En ce qui concerne la **communication externe**, le CHRSM a immédiatement informé le public **via les médias et les réseaux sociaux**. Malgré l'ampleur de l'attaque, l'hôpital a réussi à maintenir une communication claire et proactive. Le **site internet de l'hôpital, hébergé par un fournisseur externe et non impacté par l'attaque, a été utilisé pour diffuser des informations critiques**. Une fenêtre pop-up et une page évolutive ont été mises en place pour centraliser les demandes et fournir des mises à jour régulières.

L'hôpital a également instauré une veille active sur ses réseaux sociaux, notamment sur **Facebook**, **LinkedIn**, et **Twitter**, pour répondre aux questions et préoccupations des patients et du public. En parallèle, des canaux de communication spécifiques ont été créés pour gérer les relations avec la presse, avec une stratégie visant à anticiper les questions et à dicter le rythme de l'information, plutôt que de simplement réagir aux événements.

IMPACTS OPÉRATIONNELS ET FINANCIERS

L'attaque a eu des répercussions profondes sur le fonctionnement du CHRSM. Immédiatement après l'incident, l'hôpital a dû adapter toute son activité. Chaque patient a été contacté personnellement pour être informé de la tenue ou du report de son examen, intervention ou consultation. Certains services critiques, comme le Centre de Prise en Charge des Violences Sexuelles (CPVS) et le Service de Procréation Médicalement Assistée (PMA), ont pu maintenir leurs activités essentielles. Les urgences vitales et les accouchements ont également été pris en charge, mais l'hôpital a conseillé aux patients d'éviter de se présenter aux urgences pour des cas non vitaux.

La perturbation des systèmes a également entraîné des interruptions prolongées dans certains services. Par exemple, les mammotests, un examen clé pour la détection précoce du cancer du sein, ont été suspendus pendant plus d'un an. Cette suspension a été causée par l'impossibilité de sécuriser les connexions vers les centres de relecture externes. Ce n'est qu'en septembre 2024 que ces examens ont enfin pu reprendre normalement.

Côté financier, l'attaque a engendré des pertes importantes, qui se sont répercutées directement sur le compte de résultat de l'année. Les coûts immédiats liés à la réponse à l'incident, incluant les dépenses en consultance informatique et les investissements urgents pour renforcer la sécurité, ont lourdement pesé sur les finances de l'hôpital. Ces dépenses inattendues ont été suivies par une série de répercussions en cascade.

Parmi celles-ci, les retards de facturation ont perturbé la trésorerie de l'hôpital, engendrant des coûts financiers liés aux lignes de crédit. De plus, certaines surcharges de travail, dues à la désorganisation causée par l'attaque, ont été difficiles à quantifier. Par exemple, une forme de chômage technique a touché certains employés bloqués dans leurs tâches habituelles en raison de l'indisponibilité des systèmes informatiques. Ces pertes indirectes, bien que réelles, n'ont pas pu être calculées jusqu'au dernier centime, rendant l'évaluation du coût total de l'attaque encore plus complexe.

RÉVISION DE LA STRATÉGIE DE CYBERSÉCURITÉ

Suite à l'attaque, le CHRSM a entrepris une **révision complète de sa stratégie de cybersécurité** pour renforcer sa résilience face aux menaces futures. L'une des premières mesures prises a été la **mise en place de l'authentification multifactorielle (MFA)** pour tous les utilisateurs, une initiative qui était déjà en préparation avant l'incident, mais qui a été accélérée à la suite de l'attaque. Cette mesure a permis de sécuriser davantage les accès aux systèmes critiques.

Par ailleurs, l'hôpital a établi un **Centre des opérations de sécurité (SOC)** et déployé une **solution EDR (Endpoint Detection and Response)**. Contrairement aux antivirus traditionnels, l'EDR analyse les comportements suspects au sein des systèmes et déclenche des alertes en cas d'activité anormale, offrant ainsi une défense proactive contre les cybermenaces. La segmentation du réseau a également été revue et ren-

forcée, une nécessité mise en lumière par la découverte de failles lors de l'attaque.

La **sécurisation de l'Active Directory (AD) et des backups** a été une autre priorité. Les audits réalisés avant l'attaque avaient déjà souligné la nécessité de ces renforcements, mais les événements ont catalysé leur mise en œuvre. De plus, l'hôpital a migré certaines applications et services vers le cloud, reconnaissant les avantages de cette approche en matière de sécurité et de continuité des services.

Toutefois, la révision de la stratégie ne s'est pas limitée à l'aspect technique. Le CHRSM a également intensifié la **sensibilisation à la cybersécurité parmi son personnel**. Des campagnes de phishing interne ainsi que des séances d'e-learning obligatoires ont été lancées pour former les employés aux bonnes pratiques.

« La mise en place de mesures de sécurité robustes avant une attaque est indispensable pour minimiser l'impact potentiel. »

LEÇONS TIRÉES ET RECOMMANDATIONS POUR LE SECTEUR

L'attaque subie par le CHRSM a servi de leçon cruciale pour l'établissement, mais elle offre également des enseignements précieux pour l'ensemble du secteur de la santé. L'un des principaux constats est que **la prévention est bien moins coûteuse que la réaction à une cyberattaque**. Le CHRSM reconnaît qu'il avait sous-estimé certains risques avant l'incident, une erreur qui s'est révélée coûteuse tant sur le plan financier qu'opérationnel. La mise en place de mesures de sécurité robustes avant une attaque est indispensable pour minimiser l'impact potentiel.

Le CHRSM recommande vivement à d'autres entités du secteur de la santé de **définir une organisation de crise adaptée aux incidents de cybersécurité**. Cela inclut la mise en place de plans d'urgence spécifiques pour sécuriser les systèmes d'information et une stratégie de reprise priorisée. L'expérience du CHRSM a montré que même si des plans existaient, ils ne sont jamais parfaitement adaptés à la réalité d'une attaque de cette ampleur.

Une autre leçon clé concerne la continuité des opérations en cas de défaillance des systèmes informatiques. Le CHRSM recommande de **prévoir des plans B pour les activités essentielles**, y compris des solutions alternatives pour la téléphonie, particulièrement si elle est basée sur la VoIP. La crise a révélé l'importance de pouvoir fonctionner sans accès aux systèmes numériques, une situation à laquelle beaucoup d'organisations ne sont pas préparées.

L'hôpital insiste également sur l'importance d'**avoir des contrats de soutien en place pour les premières heures critiques après une attaque**. En ayant des partenaires prêts à intervenir immédiatement, les établissements peuvent gagner un temps précieux dans la gestion de la crise. Le soutien d'experts en cybersécurité, comme ceux du CERT, s'est avéré crucial pour le CHRSM, et leur intervention rapide a été déterminante pour limiter les dégâts.

Trois jours pour restaurer la normalité : témoignage d'un hôpital victime d'un ransomware

Le secteur de la santé est devenu une cible de choix pour les cybercriminels en raison de la dépendance croissante aux systèmes informatiques et de la sensibilité des données médicales. Récemment, un hôpital, qui souhaite garder l'anonymat, a fait face à cette réalité lorsque ses systèmes informatiques ont été frappés par une attaque. En dépit de la gravité de l'attaque, l'équipe informatique a su réagir avec rapidité et efficacité pour limiter l'impact sur les opérations et les patients. L'histoire de cet hôpital met en lumière l'importance cruciale d'une préparation rigoureuse et d'une gestion de crise bien coordonnée.

LA NATURE DE L'ATTAQUE CYBERNÉTIQUE

L'attaque subie par cet hôpital s'est manifestée sous la forme d'un **ransomware**, un type de cyberattaque de plus en plus courant dans le secteur de la santé. Les attaquants ont réussi à pénétrer le réseau interne de l'institution, et à partir de là, ils ont progressivement chiffré environ 80 % des serveurs de l'hôpital. Cela a rapidement paralysé la majorité des services.

L'incident a été détecté grâce à une alerte progressive des utilisateurs qui ont commencé à remarquer des dysfonctionnements dans les services. Ces interruptions de service ont conduit le personnel à contacter le service de garde informatique. C'est à ce moment-là que l'équipe a pris conscience de l'ampleur du problème.

Une fois connectée à distance à l'institution, l'équipe IT a confirmé qu'il s'agissait d'une attaque par ransomware. Un message demandait de contacter les pirates par e-mail, avec un appel direct à verser une rançon en échange des clés de décryptage. Cependant, conformément à la politique de l'hôpital, aucune tentative de contact n'a été faite, et aucune rançon n'a été payée. L'équipe a immédiatement concentré ses efforts sur la gestion de la situation et la récupération des données.

RÉPONSE IMMÉDIATE : ACTIVATION DU PLAN D'URGENCE ET GESTION DES OPÉRATIONS

Lorsque l'équipe informatique de garde a confirmé l'attaque, l'hôpital a rapidement activé son plan d'urgence hospitalier afin de gérer la crise. Ce plan comprenait **plusieurs actions clés : la sécurisation des services critiques, la coordination des équipes sur le terrain, et l'activation de procédures de continuité des soins**. Les équipes soignantes ont dû rapidement basculer vers des méthodes manuelles, utilisant des dossiers papier pour assurer la continuité des soins aux patients hospitalisés. En parallèle, les chefs de service ont été mobilisés pour prendre les premières décisions cruciales et organiser la gestion de la crise.

IMPACT OPÉRATIONNEL ET REPRISE DES ACTIVITÉS

L'attaque par ransomware a eu des conséquences significatives sur le fonctionnement de l'hôpital, forçant l'établissement à passer en « mode dégradé ». Les patients critiques ne pouvaient plus être admis, et l'hôpital a dû suspendre certaines consultations, en particulier celles nécessitant un matériel spécifique devenu inopérant à cause de l'attaque.

Malgré ces difficultés, l'hôpital a réussi à maintenir les soins pour les patients déjà hospitalisés. Les équipes soignantes ont adopté des **procédures en mode dégradé, utilisant des méthodes manuelles comme la gestion des dossiers papier** pour compenser l'indisponibilité des systèmes numériques. Cette capacité à opérer sans accès aux systèmes informatiques a été rendue **possible grâce à une planification préalable** qui prévoyait ce type de scénario d'urgence.

La reprise des activités a été une priorité immédiate après avoir stabilisé la situation. En l'espace de trois jours, l'hôpital a pu remettre en service l'ensemble

des systèmes critiques nécessaires à la gestion quotidienne des opérations. Cependant, la restauration complète des données, bien qu'elle n'ait entraîné aucune perte ou exfiltration, a pris beaucoup plus de temps en raison du volume considérable d'informations stockées. Cette période prolongée de récupération des données a nécessité une gestion minutieuse pour s'assurer que les nouvelles informations pouvaient être enregistrées correctement pendant que les anciennes données étaient restaurées.

Le défi opérationnel le plus important a été la nécessité de **coordonner la reprise des services dans un ordre de priorité** soigneusement déterminé. Par exemple, la réouverture du service des urgences ne pouvait pas se faire sans que les services de laboratoire et d'imagerie médicale soient pleinement opérationnels. Cette coordination complexe a mis en évidence l'**importance d'une planification rigoureuse et flexible**, capable de s'adapter aux imprévus selon les besoins immédiats de l'hôpital.

Bien que l'hôpital ait subi un coup dur, la mise en place rapide de procédures de crise et la reprise progressive des activités ont permis de limiter l'impact de l'attaque sur les soins aux patients. Cette expérience a également renforcé la **nécessité d'avoir des plans de continuité et de reprise d'activité robustes**, adaptés aux réalités opérationnelles d'un environnement hospitalier.

COMMUNICATION INTERNE ET EXTERNE: COORDINATION ET TRANSPARENCE

- **Communication interne**
  Dans un contexte où les systèmes informatiques étaient inaccessibles, la communication interne a dû être réorganisée rapidement. La téléphonie étant encore fonctionnelle, elle a servi de principal canal de communication entre les différents services. Les chefs de service ont relayé les instructions depuis la cellule de crise vers leurs équipes respectives, garantissant que chaque département recevait des directives claires et cohérentes. Des réunions en personne et des messages affichés sur des tableaux d'information ont également été utilisés pour maintenir la communication.

- **Communication externe**
  La communication externe a été indirecte dans un premier temps. Lorsque l'hôpital a basculé en mode dégradé, la première action a été de fermer les urgences, ce qui a marqué le début de la communication externe. Cette décision a été prise après une analyse initiale de la situation pour évaluer l'impact de l'attaque et déterminer les mesures nécessaires. La fermeture des urgences et le passage en mode dégradé ont été les premières actions visibles à l'extérieur, signalant aux patients et au public qu'une situation critique était en cours. Cette fermeture a naturellement conduit à une prise de conscience de la crise par l'extérieur, avant même toute communication officielle. Ce n'est qu'après cette première mesure que l'hôpital a commencé à communiquer plus formellement avec les parties externes. Les rapports obligatoires ont été transmis aux autorités compétentes, telles que le CERT ou le régulateur de la protection des données. En parallèle, lorsque les médias ont commencé à s'intéresser à la situation, le service de communication de l'hôpital a pris en charge la diffusion des informations publiques. L'objectif était de fournir des messages clairs et mesurés pour éviter toute panique tout en assurant la transparence sur les actions prises par l'hôpital.

LEÇONS APPRISES ET CHANGEMENTS STRATÉGIQUES

L'attaque par ransomware a été une épreuve difficile pour l'hôpital, mais elle a également servi de catalyseur pour renforcer et affiner sa stratégie de cybersécurité.

Cette expérience a mis en lumière plusieurs leçons essentielles, qui ont conduit à des changements significatifs dans la manière dont l'établissement aborde la sécurité informatique et la gestion des crises.

- **Préparation à l'indisponibilité des systèmes**
  L'une des principales leçons retenues est que, bien que la protection contre les attaques soit essentielle, il est encore plus crucial de se préparer à gérer l'indisponibilité des systèmes informatiques. L'hôpital a réalisé que **disposer de solutions de repli et de procédures claires** pour remettre en route les systèmes informatiques est primordial pour surmonter une telle crise. En effet, bien que la restauration complète des systèmes ait pris du temps, la capacité à reprendre les opérations essentielles en trois jours a montré l'importance de cette préparation.

- **Importance d'un plan de reprise**
  L'attaque a également souligné la nécessité de disposer non seulement d'un plan de continuité des activités, mais aussi d'un **plan de reprise robuste**. Ce plan doit être **flexible** et **capable de s'adapter aux circonstances spécifiques**, comme le moment du mois où l'incident se produit (par exemple, la priorité accordée au service RH pour le paiement des salaires en fin de mois). La coordination entre les différents services lors de la reprise des activités a été un défi, nécessitant une organisation rigoureuse pour rétablir les services dans le bon ordre de priorité.

- **Renforcement des mesures de sécurité**
  Suite à l'incident, l'hôpital a renforcé ses mesures de cybersécurité autant que possible dans les limites de son budget et des ressources humaines disponibles. De nouvelles procédures ont été mises en place pour améliorer la détection précoce des incidents, notamment par la **mise en place d'un service manager externe, capable de réagir 24h/24 et 7j/7** en cas d'incident majeur. Cette évolution continue permet à l'hôpital d'ajuster ses politiques de sécurité et d'intégrer de nouveaux outils au fur et à mesure que cela est possible.

- **Amélioration continue des pratiques internes**
  L'hôpital révise constamment ses pratiques de cybersécurité, en ajoutant progressivement de nouveaux outils et en affinant les procédures existantes. L'accent est mis sur la **prévention des incidents et sur la capacité à réagir rapidement et efficacement lorsqu'un incident survient**.

- **Formation et sensibilisation accrue du personnel**
  L'hôpital a poursuivi ses efforts de formation et de sensibilisation. Des **sessions d'information** et des **campagnes de sensibilisation avec du matériel didactique** sont **régulièrement organisées** pour **maintenir un haut niveau de vigilance parmi le personnel**. En effet, si la vigilance est toujours bien présente juste après un incident, il est nécessaire de continuer la sensibilisation pour que chacun et chacune reste sur ses gardes et soit également informé des nouveaux risques.

Ces ajustements illustrent l'engagement de l'hôpital à non seulement protéger ses systèmes informatiques, mais aussi à assurer une reprise rapide en cas de crise. L'expérience a montré que, même dans une situation critique, une planification adéquate et une réponse coordonnée sont essentielles pour limiter les impacts sur les opérations hospitalières.

DE LA CRISE À LA RÉCUPÉRATION RAPIDE

Cette attaque par ransomware a été une expérience difficile pour l'hôpital, mais elle a également été riche en enseignements. L'établissement a pu démontrer l'importance d'une préparation rigoureuse, d'une gestion de crise réactive, et d'une communication efficace. Bien que l'attaque ait gravement perturbé ses opérations, l'hôpital a su remettre en route ses services essentiels en un temps record et a tiré parti de cette crise pour renforcer sa stratégie de cybersécurité.

Les leçons apprises de cette attaque sont claires : il est crucial de se préparer non seulement à se protéger contre les cyberattaques, mais aussi à réagir de manière efficace lorsqu'elles surviennent. La mise en place de plans de continuité et de reprise d'activité robustes, adaptés aux spécificités opérationnelles de l'hôpital, s'est révélée être un facteur clé de résilience.

Ce témoignage montre que même face à une attaque majeure, une préparation minutieuse et une réponse bien coordonnée peuvent permettre de surmonter cette épreuve rapidement et de continuer à offrir des soins de qualité.

La force du facteur humain : comment la Clinique Saint-Luc Bouge a surmonté une cyberattaque grâce à l'engagement de ses équipes

par Adrien Dufour et Pierre-Stéphane Baton

Le 8 octobre 2021, à l'aube d'un week-end, la Clinique Saint-Luc Bouge a été frappée par une cyberattaque de type ransomware qui a presque entièrement paralysé son infrastructure informatique. Grâce à l'engagement intense de l'ensemble des équipes de l'hôpital et à l'aide précieuse du **CERT** (Cyber Emergency Response Team), l'établissement a pu reprendre ses activités en un temps record, limitant ainsi les impacts négatifs de cette crise.

DÉTECTION DE L'ATTAQUE ET PREMIÈRE RÉACTION

Tout a commencé vers 4 heures du matin, lorsque les systèmes de l'hôpital ont progressivement cessé de fonctionner. Il a fallu quelques heures avant que le problème soit détecté par le personnel d'accueil qui, à 7 heures, a constaté des anomalies sur les ordinateurs : des icônes étranges apparaissaient sur les bureaux des machines. C'était le signe d'une attaque de type **ransomware**, qui a rapidement été confirmée. L'attaque était globale, touchant environ 90 % des postes de travail, épargnant seulement les machines qui n'étaient pas sous Windows.

La gravité de la situation est vite apparue, et un technicien de garde a immédiatement alerté l'équipe informatique. En l'espace de quelques dizaines de minutes, tout le personnel concerné avait été mobilisé pour entamer l'analyse de l'incident. Les premières heures ont été cruciales pour évaluer l'étendue des dégâts et comprendre l'impact sur les soins aux patients, les opérations hospitalières, et la continuité des services critiques.

Il est important de noter que l'attaque s'est produite pendant un week-end, ce qui a posé des défis supplémentaires en termes de disponibilité du personnel. Toutefois, l'absence de consultations et une activité légèrement réduite ont permis de limiter l'impact immédiat sur les patients. Malgré cela, l'hôpital, qui compte 303 lits agréés, devait continuer à prendre en charge les nombreux patients présents, tout en naviguant dans un environnement informatique fortement compromis.

Face à l'urgence, l'hôpital a rapidement contacté le **CERT** qui **a joué un rôle central dans l'analyse de l'attaque et l'accompagnement des équipes dans la mise en place des premières mesures de réponse**. Cette collaboration s'est révélée essentielle pour reprendre le contrôle de la situation.

Ce n'était pas la première fois que l'hôpital activait son plan d'urgence hospitalier cette année-là. En pleine crise COVID, l'établissement avait déjà acquis une certaine pratique dans la gestion des urgences. Cela a grandement aidé l'équipe à réagir rapidement : déclencher le plan d'urgence, contacter les personnes concernées, organiser le travail en mode réduit, et en mode dégradé, tout en continuant à prendre en charge les patients présents dans l'hôpital.

GESTION DE LA CRISE : STRATÉGIES ET COMMUNICATION

Deux constats ont été faits dès l'attaque détectée. Le premier est qu'il y a toujours un choc initial lorsqu'une cyberattaque survient. Il est donc essentiel de réduire au maximum cette période de choc et de surprise. Dans ce cas-ci, la Clinique Saint-Luc Bouge ne disposait pas de plan de cybersécurité spécifique pour faire face à une telle attaque. C'est l'équipe IT qui a rapidement pris l'initiative de contacter les bonnes personnes, et une fois les équipes mobilisées, elles ont réagi avec efficacité. Le **premier enseignement** est donc l'importance d'avoir un **plan bien structuré, avec les contacts utiles clairement définis dès le départ**.

Le **deuxième point crucial** est que **vous ne pouvez pas compromettre la sécurité** de vos collaborateurs

et de vos patients. Il est donc essentiel de s'assurer que les décisions prises soient les bonnes. La question à se poser est : **avons-nous encore la capacité d'accueillir de nouveaux patients ?** Dans ce cas précis, l'équipe dirigeante a choisi de **fermer le 112 temporairement**. Toutefois, les patients pouvaient toujours se rendre directement à l'hôpital si nécessaire. Ensuite, il s'agissait de se préparer pour le lundi, en s'assurant que les équipes IT avaient les moyens de restaurer les systèmes.

Adrien Dufour, le directeur général, a communiqué très rapidement en externe, suivant les conseils du CERT. L'objectif principal était de rassurer le public, car la fermeture des urgences et l'annulation des consultations touchent rapidement des centaines de personnes. Le message clé à faire passer était clair : des mesures de sécurité ont été prises, aucune donnée sensible n'a été exfiltrée ou exposée, et la situation était en cours d'analyse. Il était crucial de protéger la réputation de l'hôpital tout en assurant que les informations partagées étaient transparentes et rassurantes.

En interne, la communication s'est concentrée sur les grandes étapes à venir : comment organiser le travail, quelles mesures de sécurité appliquer, et quelles seraient les prochaines étapes pour la reprise des activités.

PLAN DE REPRISE ET RÉINSTALLATION DES SYSTÈMES

Une fois l'urgence immédiate maîtrisée, la Clinique Saint-Luc Bouge a rapidement initié un **plan de reconstruction** pour rétablir ses systèmes informatiques. Dès le lundi suivant l'attaque, l'objectif était clair : revenir à un état opérationnel normal d'ici la fin de la semaine. Ce plan ambitieux reposait sur plusieurs étapes critiques. Tout d'abord, les équipes informatiques ont dû identifier avec précision la date et la méthode de l'incursion initiale des cyberattaquants pour s'assurer que toutes les traces de l'attaque étaient éliminées avant de restaurer les systèmes. Cela a impliqué un travail intensif pour analyser les logs, remonter dans les sauvegardes, et déterminer à quel point exact revenir pour restaurer les données.

L'une des principales difficultés rencontrées a été la perte partielle des sauvegardes initiales, certaines ayant été compromises par l'attaque. Heureusement, l'hôpital disposait de **plusieurs couches de sauvegarde**, y compris des **enregistrements sur bande**, qui n'étaient **pas connectés au réseau** et ont donc été épargnés. Ces sauvegardes ont joué un **rôle crucial dans la restauration des systèmes**.

La réinstallation des systèmes ne s'est pas limitée aux équipes informatiques. Conscients de l'ampleur de la tâche, les responsables ont décidé de déléguer certaines opérations aux équipes soignantes et administratives. Ces équipes ont été rapidement formées pour effectuer des tâches techniques de base, telles que le reformatage des ordinateurs, libérant ainsi les informaticiens pour se concentrer sur les aspects plus complexes de la récupération.

Pendant les deux jours du week-end suivant, tout le personnel s'est mobilisé pour effectuer ces tâches en temps record. Finalement, grâce à cette **mobilisation collective** et à une **coordination exemplaire**, l'hôpital a réussi à remettre en service l'ensemble de ses systèmes, permettant ainsi une reprise rapide des opérations normales dès la semaine suivante. **Ce succès repose sur une stratégie bien pensée, un travail acharné et l'utilisation judicieuse de plusieurs types de sauvegardes, qui ont permis de minimiser les pertes de données et de restaurer la confiance dans les infrastructures informatiques de l'hôpital**.

RENFORCEMENT DE LA SÉCURITÉ ET CONSÉQUENCES FINANCIÈRES

La cyberattaque subie par la Clinique Saint-Luc Bouge a conduit à un renforcement de sa stratégie de cybersécurité. L'une des premières priorités a été de **renforcer tout ce qui concernait le stockage et les sauvegardes**, étant donné que les cybercriminels avaient réussi à atteindre la première couche de sauvegarde. L'établissement a donc réinvesti dans un **système de sauvegarde plus sécurisé, avec une plus grande déconnexion entre les différents environnements** pour prévenir toute future intrusion.

En parallèle, l'accent a été mis sur l'**amélioration des systèmes de détection des comportements anormaux**. Alors que précédemment la sécurité se concentrait principalement sur la périphérie de l'infrastructure, l'approche a évolué pour inclure une surveillance plus approfondie à l'intérieur des systèmes, à l'image d'une ville médiévale où des murs de protection internes viennent renforcer la sécurité au-delà des seules portes d'entrée.

Cependant, même avec des systèmes renforcés, la clinique reconnaît qu'elle ne peut jamais être

complètement à l'abri des failles dites « zero-day », c'est-à-dire des vulnérabilités qui sont connues des cyberattaquants mais pas encore des éditeurs de logiciels. Alors que la majorité des cyberattaques exploitent des failles connues ou des équipements non mis à jour, il est crucial de maintenir des systèmes à jour tout en se préparant à l'imprévisible.

Les impacts financiers de cette crise ont été significatifs. Dans un premier temps, il a fallu engager des dépenses importantes pour permettre la continuité des services et la remise en ordre de la situation initiale, notamment en recrutant des consultants et en achetant des logiciels en urgence. En outre, l'arrêt temporaire des activités a entraîné des pertes financières substantielles, car chaque jour d'inactivité se traduit par une perte de revenus et des coûts additionnels dus au personnel inactif. L'impact financier a été évalué en millions d'euros, soulignant que **la sécurisation proactive est toujours moins coûteuse que de gérer les conséquences d'une cyberattaque**.

Pour répondre à ces défis, la clinique a non seulement amélioré ses sauvegardes et ses systèmes de détection, mais a également réalisé un audit de sa posture actuelle afin de se préparer à la conformité avec la directive NIS2. Cet effort s'est également traduit par la création d'un **Security Operations Center (SOC)** externalisé, fonctionnant 24/7.

Enfin, la clinique a intégré ces efforts dans une stratégie de gouvernance renforcée, visant à assurer que les outils de cybersécurité ne dictent pas les procédures, mais qu'ils s'intègrent plutôt dans un cadre stratégique cohérent. Cette approche a également inclus des **sessions de sensibilisation** lors de soirées stratégiques, où les principaux décideurs de l'institution ont été informés des enjeux liés à la cybersécurité et des défis à venir.

CONSEILS POUR LA GESTION DES CYBERATTAQUES DANS LE SECTEUR HOSPITALIER

Face à l'expérience vécue, la Clinique Saint-Luc Bouge recommande vivement aux établissements de santé de prendre contact avec le **CERT** ou un partenaire spécialisé en cybersécurité dès les premiers signes d'une attaque. Le temps est un facteur critique, et disposer de contacts ou de contrats de support en amont peut faire toute la différence. En effet, sans ces accords préétablis, il est possible que l'assistance nécessaire ne soit pas disponible en temps voulu, comme cela a été le cas pour l'hôpital sur certains aspects.

Un autre point crucial est de **ne jamais éteindre les machines touchées par une cyberattaque**. Au contraire, il est recommandé de les isoler du réseau sans les couper, pour permettre aux experts de suivre la trace des cyberattaquants. Cette procédure est essentielle pour remonter jusqu'au point d'entrée initial, identifier le premier contact avec le système et déterminer la date exacte de l'intrusion. Sans ces informations, il est impossible d'être certain qu'il n'y a pas d'autres compromissions encore présentes dans l'infrastructure, comme un cheval de Troie caché.

Enfin, il est primordial de mettre en place des **sauvegardes régulières**, et surtout de s'assurer que ces sauvegardes sont **déconnectées du réseau principal**. Cette mesure simple peut se révéler cruciale pour la récupération rapide des systèmes après une attaque.

En résumé, la **préparation**, la **réactivité**, et la **rigueur** dans la gestion des sauvegardes et des analyses post-incident sont les clés pour limiter les impacts d'une cyberattaque dans le secteur de la santé.

LA COORDINATION DES ÉQUIPES : LA CLÉ DE LA RÉSILIENCE FACE À UNE CYBERATTAQUE

Bien que la clinique ait réussi à surmonter cette crise grâce à la mobilisation rapide de ses équipes et au soutien crucial du CERT, les impacts financiers et opérationnels ont été significatifs. L'engagement sans faille et l'expertise des équipes ont permis à l'hôpital de retrouver rapidement une situation normale.

En fin de compte, la cybersécurité n'est pas seulement une question de technologie, mais aussi de coordination humaine, de gouvernance efficace, et d'une culture de sécurité partagée à tous les niveaux de l'organisation. La Clinique Saint-Luc Bouge en est ressortie plus forte et mieux préparée pour faire face aux défis de demain, assurant ainsi la protection de ses patients, de son personnel, et de ses infrastructures.

Cyberattaques dans le secteur hospitalier : stratégies et réflexes pour gérer la crise

La cybersécurité dans le secteur de la santé est un sujet de plus en plus préoccupant. Les hôpitaux, en tant que détenteurs d'informations sensibles et opérateurs vitaux, sont des cibles privilégiées de cyberattaques. Catalina Al Hok, Senior Manager chez Sia Partners et experte en cyberrésilience partage son expertise sur la manière de gérer efficacement une crise cyber dans ce secteur. Cet article détaillé vise à fournir aux hôpitaux une feuille de route claire et pratique pour se préparer et réagir face à de telles crises.

LES RÉFLEXES À ADOPTER

Lors d'un incident cyber majeur, les premières minutes sont cruciales, car c'est durant cette période que se prennent les décisions les plus déterminantes. **Catalina Al Hok** insiste sur plusieurs réflexes essentiels à adopter pour assurer une gestion efficace de la crise.

1. Anticipation et préparation

La gestion d'un incident cyber ne doit jamais être improvisée. La **préparation** est le premier et le plus important des réflexes à avoir. Cela implique une **anticipation des imprévus**, nécessitant une préparation pour prendre des décisions dans un contexte où règne une grande incertitude. Pour cela, il est essentiel de bien connaître le panorama des **risques cyber de l'organisation et les scénarios de crise** auxquels l'organisation pourrait être confrontée. La mise en place de mesures pour mitiger ces risques identifiés et anticiper ces scénarios est une étape clé. Il s'agit de définir des dispositifs de **gestion d'incident et de crise**, incluant des processus et des procédures clairs, ainsi que d'identifier les parties prenantes, tant internes qu'externes avec une matrice RACI claire et partagée. Cette préparation permet de développer les bons réflexes pour le jour J. Grâce à des exercices et des tests réguliers, les équipes peuvent affiner leur capacité à réagir efficacement, connaître leurs périmètres de délégation, et prendre des décisions adaptées sans devoir consulter des processus complexes.

2. Maîtrise de soi et respect des processus

Un autre réflexe indispensable, toujours en lien avec la préparation, mais davantage axé sur l'aspect humain, est de faire preuve de maîtrise de soi et de confiance dans le dispositif et les processus mis en place. Il est crucial de maintenir les différentes cellules de crise distinctes. En fonction des structures, on identifie plusieurs typologies de cellules de crise, mais il est essentiel d'avoir au minimum une **cellule de crise décisionnelle** et une **cellule de crise opérationnelle**. Ces cellules doivent rester bien séparées pour éviter tout chevauchement des rôles et des responsabilités. En effet, regrouper toutes les parties prenantes autour de la même table risque de paralyser la prise de décision, car chacun traite une dimension différente. L'équipe doit savoir dans quelle mesure elle peut agir en urgence, et cette capacité d'action dépend directement de la préparation en amont. **Garder son sang-froid, se baser sur les faits, et respecter scrupuleusement les processus de détection, d'alerte et de réaction sont des impératifs pour gérer efficacement la crise**.

3. Prendre des décisions sans précipitation

Il est également vital de ne pas céder à la précipitation lors de la prise de décisions en situation d'incertitude, même si l'on doit réagir rapidement. Les **décisions** doivent être **mûrement réfléchies**, et pour cela, il est recommandé de **préparer des fiches de décision en amont**, basées sur les grandes décisions que l'organisation pourrait être amenée à arbitrer. Ces fiches aident à guider les actions de manière structurée et à éviter les erreurs dues à une réaction trop rapide.

4. Partager une vision commune de la crise

Trop souvent, lors de la gestion de crise, les informations sont dispersées, et les équipes manquent de direction. Catalina Al Hok souligne l'importance de **prendre le temps**, même si cela signifie interrompre d'autres activités pendant quelques minutes, **pour aligner tous les membres sur une compréhension claire de la crise** : quel est exactement l'événement en cours, quel est son impact sur l'organisation, et où veut-on aboutir ? Cet alignement garantit que toutes les actions sont coordonnées et orientées vers un objectif commun, ce qui est essentiel pour une gestion de crise réussie.

5. Communication interne et externe

Communication interne

Communiquer en interne est indispensable pour limiter les conséquences d'une crise. Cette communication est décisive pour obtenir l'adhésion des collaborateurs et des utilisateurs et pour les impliquer activement dans la résorption de la crise.

Communication externe

Une cyberattaque est un événement fâcheux vis-à-vis des parties externes, comme les clients, partenaires, prestataires et régulateurs. Communiquer vers l'extérieur permet d'instaurer la confiance en montrant que l'événement est maîtrisé et que les équipes travaillent à résoudre le problème. Cette communication est d'autant plus importante que les cyberattaquants eux-mêmes peuvent communiquer en temps réel sur la crise, d'où la nécessité d'avoir une stratégie de communication validée en amont, construite autour de différents scénarios d'attaque et adaptée aux différents publics cibles (clients, régulateurs, médias, etc.). La temporalité de la communication est également critique ; il est important de tenir les parties prenantes informées de l'évolution de la situation pour maintenir leur confiance.

6. Ne pas se précipiter, mais être proactif

Il ne faut pas se contenter d'être réactif, mais il est essentiel d'être proactif. Cela signifie anticiper les actions qui pourraient avoir lieu sur le système d'information lors de la résolution de l'attaque, en fonction du profil de l'attaquant, car c'est une grande partie d'échecs qui est alors engagée. Les modes opératoires des attaquants permettent d'établir leur portrait-robot, et la **préparation de scénarios en amont**, selon ces profils, permet d'anticiper leurs éventuelles réactions, et donc d'agir de manière plus efficace pour contrer leurs stratégies.

RÉFLEXES TECHNIQUES : ISOLER, NEUTRALISER ET RESTAURER

Après avoir exploré les réflexes essentiels à adopter sur le plan organisationnel et humain, il est crucial de se pencher sur les **aspects techniques** de la gestion d'une crise cyber. La réponse technique doit être **coordonnée**, **précise** et **méthodique** pour garantir la sécurité et la reprise d'activité de manière sûre et fiable.

1. Isolement immédiat du système

La première action technique à entreprendre lors d'une cyberattaque est l'**isolement du système d'information affecté**. Cette étape vise à **limiter la propagation latérale** de la menace à l'intérieur du SI. La segmentation du réseau devient alors essentielle pour confiner l'incident et empêcher l'attaquant d'accéder à d'autres systèmes critiques.

2. Opérations de réponse à l'incident

Une fois l'isolation effectuée, il est temps de conduire globalement les opérations de réponse à l'incident. Cela implique une série d'interventions visant à stabiliser la situation et à prévenir toute escalade. Ces opérations couvrent plusieurs actions techniques et organisationnelles pour s'assurer que l'incident est contenu et que les systèmes sont sous contrôle.

3. Neutralisation de la menace et rétablissement de la confiance dans le SI

Après avoir lancé les actions de réponse, l'étape suivante consiste à **neutraliser la menace**, qu'il s'agisse de l'attaquant ou du malware, qui se propage sur le système d'information. Cette étape est souvent réalisée de manière incomplète, laissant des vulnérabilités persistantes. Catalina Al Hok souligne qu'il est essentiel de ne pas se limiter à traiter uniquement le problème identifié, mais de **vérifier que l'attaquant ne pourra pas se propager à nouveau** ou réintégrer le SI en corrigeant toutes les failles qui ont pu être exploitées pour mener la cyberattaque initiale.

4. Opérations de Threat Hunting

Avant de redémarrer les activités, il est crucial de s'assurer que le système d'information est totalement exempt de toute présence malveillante. Le **Threat Hunting** est une phase cruciale où l'équipe technique s'assure qu'il ne reste aucune trace du malware ou de l'attaquant dans le SI. Cette étape consiste à examiner en profondeur chaque compo-

sant du système pour détecter et éradiquer toute persistance de la menace. Cela prend du temps, mais cette démarche est indispensable pour éviter des répercussions ultérieures plus graves. La confiance dans le SI doit être restaurée à un niveau qui permette de reprendre les activités en toute sécurité, en fonction du degré de confiance exigé.

5. Analyse des causes racines (Root Cause Analysis)
Enfin, un **Root Cause Analysis** doit être réalisé pour comprendre les causes profondes de l'incident ayant conduit à une crise. Cela permet non seulement d'évaluer les dégâts, mais aussi de s'inscrire dans un cycle d'amélioration continue. Catalina Al Hok souligne que cette analyse ne doit pas être la priorité lors d'une gestion de crise ; elle vient après les mesures d'urgence. Certaines structures commettent l'erreur de vouloir immédiatement imputer des responsabilités ou désigner des coupables, alors que l'urgence est d'abord de contenir et d'éradiquer la menace. Cette recherche approfondie peut être menée des semaines, voire des mois après la crise, lorsque la situation est pleinement maîtrisée.

LES ERREURS À NE PAS COMMETTRE

Même si la gestion de crise implique une part d'incertitude et d'erreurs, l'essentiel est de savoir rebondir et d'apprendre de ses erreurs. Lorsqu'une structure vit une attaque cyber, elle ne reviendra jamais à son état antérieur, mais évoluera pour devenir plus résiliente. L'approche doit être de considérer chaque crise comme une opportunité d'amélioration : ce qui a été mis en place en mode dégradé peut être réutilisé pour renforcer la posture cyber de l'organisation.

1. Ne pas être préparé
La première et la plus grave erreur est de ne pas être préparé. Attendre le jour J pour improviser n'est plus acceptable. La préparation, comme mentionnée précédemment, est cruciale pour anticiper les actions à entreprendre lors d'une cyberattaque.

2. Réduire la crise cyber à un simple problème technique
Une crise cyber n'est jamais uniquement technique. Catalina Al Hok rappelle qu'il est crucial d'analyser les impacts sur les différents piliers de l'entreprise pour prendre des décisions éclairées. Parmi ces piliers, on peut citer les aspects **financiers**, **juridiques**, la **réputation**, la **production**... Ne pas considérer ces impacts de manière globale peut transformer une crise cyber mineure en une crise systémique, particulièrement dans un environnement comme celui des hôpitaux, où une perturbation peut rapidement évoluer en crise sanitaire.

3. Ne pas communiquer
La communication est essentielle dans la gestion de crise. Cependant, il est important de trouver le juste équilibre entre transparence et discrétion, pour ne pas fournir d'informations qui pourraient être exploitées par les attaquants. La communication doit inclure différents acteurs de l'organisation (IT, juridique, communication, direction) pour **assurer une réponse coordonnée**. Il faut également être préparé à répondre en cas de contact direct avec les cyberattaquants.

4. Se focaliser uniquement sur les outils technologiques
Une erreur fréquente est de croire qu'un incident cyber peut être résolu uniquement avec des équipements et des logiciels. L'utilisateur reste au centre du dispositif de sécurité. Un logiciel, même sophistiqué, est inefficace s'il est mal paramétré ou si les bons scénarios et points de contrôle n'ont pas été développés. Il est important de ne pas se reposer à 100 % sur les logiciels de sécurité et de **s'assurer que les utilisateurs sont bien formés et vigilants**.

5. Négliger le risque tiers
Il est crucial d'intégrer le **risque tiers** dans la gestion de la cybersécurité. Une organisation peut être robuste, mais elle reste vulnérable si ses partenaires ou prestataires n'ont pas le même niveau d'exigence en matière de sécurité. De plus en plus d'attaques proviennent de tiers, rendant ce point particulièrement critique.

6. Négliger la gestion de l'après-crise
Enfin, il ne faut pas négliger la gestion de l'après-crise. Il est essentiel de maintenir une veille et un monitoring actifs pour identifier les signaux faibles et prévenir toute résurgence. Cependant, il est également important de ne pas prolonger indéfiniment l'état de crise, ce qui pourrait épuiser les ressources humaines. La rotation des équipes en crise est indispensable pour maintenir le dispositif sur la durée

et assurer une transmission efficace et fiable des informations.

La vision de la crise doit s'appuyer sur un fil d'Ariane tout au long de l'événement, c'est-à-dire qu'elle doit être claire, maintenue jusqu'à la résolution complète de la crise, et accessible à toute personne intégrée dans le dispositif. Ce fil d'Ariane permet à chacun de savoir précisément où en est l'organisation et d'agir en conséquence, garantissant ainsi la continuité et la cohérence des actions jusqu'à la fin de la crise.

LA CYBERSÉCURITÉ, UN CENTRE DE VALEUR ESSENTIEL

Autrefois perçue comme un centre de coûts, la cybersécurité était souvent négligée par les structures moins matures, considérant la probabilité d'occurrence d'une attaque comme faible. Aujourd'hui, cette perspective est obsolète. Ce qu'on constate c'est que tous les secteurs se régulent, d'autant que les grandes entreprises sont clientes et partenaires des secteurs critiques. Les hôpitaux ne fonctionnent plus isolément ; ils collaborent avec un large éventail d'entreprises privées et publiques, créant des **interconnexions complexes**. Avec l'évolution des cadres réglementaires, la cybersécurité est devenue une affaire commune à toutes les organisations, peu importe leur taille ou leur secteur d'activité.

Dans ce contexte, la cybersécurité passe d'un centre de coûts à un **centre de valeur**. Elle protège le patrimoine informationnel et la propriété intellectuelle des hôpitaux, notamment ceux impliqués dans la recherche médicale. Ces recherches de pointe ne doivent pas tomber entre de mauvaises mains, pouvant servir des intérêts peu louables.

La cybersécurité devient ainsi un **accélérateur de business**. Ce qui était auparavant un simple « nice to have » est aujourd'hui indispensable pour rassurer ses partenaires, ses utilisateurs, et renforcer la confiance dans ses capacités à protéger des données critiques. En définitive, investir dans la cybersécurité, c'est investir dans la pérennité et la crédibilité de l'organisation.

Sia Partners est un acteur majeur du conseil en stratégie et management, avec une forte expertise en cybersécurité et protection de données, opérant en Europe, au Moyen-Orient et en Amérique du Nord. Le cabinet propose une offre structurée en plusieurs axes :

- **Gouvernance, risque et conformité cyber**
  Accompagnement des clients sur les problématiques de gouvernance, conformité et maîtrise des risques.

- **Ingénierie cybersécurité**
  Sécurisation technique des différentes couches du Système d'Information (SI), incluant la sécurité réseau, des systèmes d'exploitation, des applications et du cloud, avec une composante forte sur la Cloud Security.

- **War Gaming**
  Sensibilisation à la cybersécurité à travers des exercices de gestion d'incident et de crise, tant pour un public opérationnel que décisionnel.

- **Protection des données**
  Du cadre juridique à la mise en place de solutions techniques telles que le chiffrement des données et la prévention des pertes de données (DLP).

Deux offres en plein essor chez Sia Partners sont la **sécurité de l'intelligence artificielle** et l'**accompagnement à la mise en conformité DORA et NIS2**.

Nous remercions l'ensemble des contributeurs,
des entreprises et des partenaires pour leur temps et leur expertise.

Cyberwal
by digital
wallonia

digitalwallonia.be/cyberwal

Wallonie
Relance

Agence
du Numérique