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

Avant-propos par Benoit Hucq, Directeur Général, Agence du Numérique . **4**

À propos de *Cyberwal by Digital Wallonia* **6**

Préface par le Centre for Cyber security Belgium (CCB) **8**

1. **Approach Cyber**
   par Jorien Decroos *« La cybersécurité dans le secteur de la santé : la nécessité d'un approche personnalisée »* **10**
2. **Ataya Partners**
   par Anthony van der Maren *« Protéger des vies et des données : les défis de la cybersécurité en milieu hospitalier »* **13**
3. **AVIQ**
   par Françoise Lannoy et Séverine Ovyn
   « L'AVIQ : à la confluence de l'innovation numérique, de la protection des données et de la stratégie d'entreprise » **15**
4. **Groupe santé CHC**
   par Philippe Olivier, Alain Coudijzer, Laurence Delcomminette et Frédéric Pampalone *« Sécurité informatique au CHC : leçons d'une attaque majeure et perspectives »* **18**
5. **Microsoft**
   par Bart Asnot *« Protéger le futur : l'alliance de la cybersécurité et de l'innovation dans le monde médical »* **21**
6. **Proximus**
   par Antonio Paci *« Cybersécurité, le SOCle indispensable »* **23**
7. **RHEA Group**
   par Matteo Merialdo *« Sans une gouvernance des risques, investir dans des outils revient à gaspiller le budget »* **25**
8. **Solvay Business School**
   par Georges Ataya *« Comment bien gérer la cybersécurité des hôpitaux »* **27**
9. **Thales**
   par Johann Alessandroni *« Les trois piliers de la cybersécurité médicale : les recommandations de Thales pour un secteur en évolution. »* **29**
10. **Université Catholique de Louvain (UCL)**
    par le Professeur Axel Legay *« Transformer la cybersécurité médicale en opportunité économique pour la Wallonie »* **31**

Éditeur responsable : 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

La prospérité de notre région est intrinsèquement liée au bien-être de ses citoyens. Le secteur de la santé en est l'une des principales fondations . C'est pourquoi, je suis particulièrement heureux de préfacer ce livre blanc abordant cette question stratégique de la cybersécurité au sein du secteur de la santé en Wallonie.

Le paysage de la santé connaît une transformation profonde, caractérisée par un usage croissant des technologies numériques et par la génération d'énormes quantités de données sensibles. Bien que ces avancées offrent d'incroyables opportunités, elles suscitent également des défis sans précédent en matière de cybersécurité, défis qui exigent notre attention immédiate.

La résilience de notre secteur de la santé est de plus en plus mise en cause par la cyber-criminalité !

Ces dernières années, la Wallonie a en effet connu des cyberattaques visant les établissements de santé, nous rappelant avec force les menaces croissantes auxquelles nous sommes confrontées. Ces incidents compromettent la vie privée des patients, perturbent les services de santé et même entravent l'innovation médicale. Nous ne pouvons pas rester passifs face à de tels évènements et menaces futurs.

Au-delà de souligner l'urgence de ces questions, ce livre blanc propose une stratégie globale visant à renforcer les défenses en cybersécurité de nos établissements de santé. Il appelle à l'allocation de ressources, à la collaboration entre les professionnels de la santé et les experts en cybersécurité, ainsi qu'à la diffusion des meilleures pratiques pour protéger l'intégrité de notre système de santé.

Notre engagement envers la sécurisation du secteur de la santé ne relève pas uniquement de l'intérêt économique. Il s'agit d'un devoir fondamental visant à protéger la santé et le bien-être de nos concitoyens. En investissant collectivement et en mettant en œuvre ces recommandations, nous pouvons renforcer considérablement la capacité du secteur wallon de la santé à resister aux menaces de cybersécurité.

J'adresse mes remerciements aux personnes, experts et organisations qui ont contribué à la conception et la réalisation de ce livre blanc. Leurs idées et expertises ont joué un rôle essentiel dans la définition de notre approche face à cette question stratégique.

Renforcer la cybersécurité du secteur de la santé, c'est aussi contribuer à l'objectif majeur de préservation de la réputation de la Wallonie en tant que territoire soucieux de sa résilience au profit de ses habitants et de son système de santé.

Cet objectif est, entre autres, poursuivi par le programme régional *« Cyberwal By Digital Wallonia »*. Ensemble, nous pouvons y contribuer par nos pratiques au quotidien : cet ouvrage est en cela une source importante d'inspirations. Je vous en souhaite une bonne lecture !

Benoit Hucq
Directeur Général,
Agence du Numérique

À propos de *Cyberwal by Digital Wallonia*

La problématique de la cybersécurité est reconnue comme vitale pour la Wallonie. En l'intégrant dans le Plan de Relance Wallon (PRW), la Wallonie s'aligne sur la stratégie européenne d'investissement et de relance.

Pour atteindre cette ambition, l'Agence du Numérique a mis en place le programme *« Cyberwal by Digital Wallonia »* dont le but est d'augmenter la résilience en matière de cybersécurité des entreprises, citoyens et services publics via 4 objectifs principaux :

- Préserver la souveraineté numérique du territoire ;
- Soutenir et protéger les citoyens, les entreprises et organismes publics ;
- Valoriser le potentiel de la recherche et développer des cursus de formation adéquats ;
- Développer des outils et services stratégiques à destination de tous.

L'atteinte de ces objectifs cités requiert des actions fortes et concertées, mobilisant les entreprises et les organisations tant publiques que privées, impliquant les acteurs de l'écosystème (entreprises de l'offre du secteur du numérique, acteurs de la recherche, de l'innovation, de la formation et de l'animation économique).

Dès lors, les activités et actions de *Cyberwal by Digital Wallonia* reposent sur 4 piliers de développement complémentaires. :

- **Sensibilisation & Accompagnement** du territoire et de l'écosystème wallon aux enjeux, outils et opportunités de la cybersécurité ;
- **Formation** couvrant à la fois la pénurie de talents pour les entreprises et leur accompagnement mais aussi pour nourrir l'axe Recherche ;
- **Recherche & Innovation** mobilisant les acteurs de la recherche autour de thématiques d'excellence et porteuses d'innovation pour les entreprises, en particulier dans le cadre de la S3 ;
- **Internationalisation** couvrant la valorisation des entreprises wallonnes mais aussi de la recherche et de l'innovation *« Made in Wallonia »* vers le reste du monde, incluant une présence dans les projets européens ainsi que dans des salons ou événements majeurs de la cybersécurité.

Afin de mieux atteindre ses objectifs et servir à son plus haut potentiel les intérêts numériques de la Wallonie, *Cyberwal by Digital Wallonia* a décidé de donner un focus particulier aux secteurs suivants en 2023 et 2024 :

- Industrie 4.0
- Secteur public
- Secteur de la santé

Ainsi, alliant les activités du pilier 1 « Sensibilisation et accompagnement » avec la priorisation du secteur de la santé, ce livre blanc est le premier jalon d'une série d'actions qui seront publiées et mises à disposition de l'écosystème.

La cybersécurité est l'affaire de tous, et *Cyberwal by Digital Wallonia* prend à cœur les intérêts sécuritaires des acteurs wallons.

Préface par le Centre pour la Cybersécurité Belgique (CCB)

Le monde est en pleine mutation numérique. Les nombreux services et technologies numériques offrent à la population et aux organisations belges une multitude d'opportunités de développement et cela devrait encore s'amplifier à l'avenir.

Cette croissance de l'utilisation des nouvelles technologies s'accompagne toutefois d'une augmentation de nouvelles menaces (avancées) dans le champ cyber, susceptibles de mettre à mal les possibilités offertes par les services numériques. À l'ère du numérique, les menaces qui pèsent sur l'intégrité des données et la stabilité des systèmes sont omniprésentes. La cybersécurité est donc d'une importance capitale, notamment pour protéger les informations sensibles et les activités critiques.

Dans le domaine des soins de santé, cette sécurité revêt une importance encore plus grande. L'augmentation constante, ces dernières années, des cyberattaques visant des établissements de santé et secteurs connexes – comme ce fut le cas dans notre pays – met en péril l'offre ininterrompue des services de santé ainsi que la confidentialité des données des patients. La pandémie de Covid-19 a démontré à bien des égards à quel point, dans un monde de plus en plus interconnecté, il n'a jamais été aussi important d'investir dans de solides mesures de sécurité. Ces mesures doivent garantir la confiance du public, l'intégrité des soins de santé et la protection des données sensibles.

LE CCB

En tant qu'autorité nationale pour la cybersécurité en Belgique, le Centre pour la cybersécurité en Belgique (CCB) joue un rôle de premier plan dans ce domaine et vise à aider les organisations à protéger leurs systèmes et leurs données au mieux de leurs capacités.

Le CCB – qui est directement sous l'autorité du Premier ministre – supervise, coordonne et contrôle la mise en œuvre de la stratégie de cybersécurité 2.0 de la Belgique (2021-2025), s'efforçant de faire de la Belgique l'un des pays les moins cybervulnérables d'Europe, tout en coopérant avec de nombreux acteurs fédéraux et régionaux. L'échange optimal d'informations entre les entreprises, les gouvernements et le public doit permettre de mener à une protection appropriée. Même si, en fin de compte, chaque organisation reste responsable de la protection de ses propres systèmes.

C'est pourquoi le CCB a développé plusieurs initiatives, notamment Safeonweb, pour protéger les citoyens. Il peut en outre compter sur la Computer Emergency Response Team (CERT.be), les cyberpompiers auxquels chaque organisation peut signaler des incidents, recevoir des conseils et éventuellement demander une assistance technique. Le CCB a également mis en place un système d'alerte rapide (*Early Warning System*), auquel les organisations d'importance vitale – y compris celles du secteur de la santé – peuvent avoir recours afin de recevoir des alertes précoces en cas d'incident. Enfin, le CCB publie de nombreux guides de conseils pratiques et des lignes directrices pour aider les organisations à mieux se protéger.

Dans les mois à venir, le CCB lancera un portail sur lequel toutes les organisations belges pourront s'inscrire afin de recevoir des alertes précoces et de mesurer et d'améliorer leur maturité en matière de cybersécurité. Ce portail sera également accessible aux organisations du secteur médical.

CYFUN

Dans cette optique, et afin d'aider les organisations à réduire de manière significative le risque de cyberattaques les plus courantes et de les aider à augmenter leur niveau de cyber-résilience, le CCB a développé **le framework des cyberfundamentals**. Ce dernier prévoit **3 niveaux d'assurance** (Basic, Important et Essentiel) afin d'adapter la proportionnalité des mesures aux risques auxquels chaque organisation est exposée.

Le contenu et les mesures de chaque niveau de ce framework sont définis sur la base de nos données historiques des incidents et ce, en conformité avec d'autres normes internationales. De ce point de vue, les mesures clés qui y sont identifiées permettent de hiérarchiser les mesures de protection.

Ce framework est disponible sur le site web du CCB et est accompagné d'un outil permettant de définir le niveau d'assurance approprié pour chaque organisation, donc aussi dans le secteur de la santé. Un outil facilitant l'auto-évaluation est également mis à disposition. La finalisation des éléments pour l'obtention d'une attestation de conformité sous ce framework est en cours auprès d'un organisme accrédité.

INCIDENTS & CCB/CERT.BE

Ces dernières années, le secteur médical s'est révélé être une cible privilégiée des cyberattaques, en raison de l'urgence de la disponibilité et de la sensibilité des données. La Belgique a connu, elle aussi, plusieurs incidents majeurs qui ont fortement perturbé le fonctionnement d'hôpitaux et d'autres organisations liées aux soins de santé.

Nous recommandons donc à toutes les organisations du secteur médical de prendre les précautions minimales suivantes :

- Disposer de sauvegardes hors ligne non connectées au réseau ;
- Limiter les accès au strict minimum nécessaire pour le bon fonctionnement. Cela s'applique à la fois aux droits des utilisateurs et à l'accès aux serveurs/dispositifs spécifiques ;
- Garantir les capacités de détection. Au-delà des logiciels et du matériel (système de détection d'intrusion, pare-feu, EDR, antivirus, etc.), il s'agit également de veiller à ce que les alertes générées par ces produits soient transmises et analysées en temps utile par les bonnes personnes ;
- Planifier et tester les procédures à suivre en cas d'incident ou de détection. La communication interne, avec les collègues, les partenaires extérieurs, etc. est à inclure dans cette démarche.

En cas d'incident, outre les notifications potentiellement requises par le GDPR auprès, entre autres, de l'Autorité de protection des données, nous recommandons également de contacter le *CERT.be*. Pour plus d'informations, consultez le site *https://cert.be/fr/signaler-un-incident*.

Récemment, la Belgique a également mis en place un cadre juridique pour le **piratage éthique**. Ce cadre permet à des tiers, à condition qu'ils respectent les règles, de trouver des vulnérabilités dans les services et de les signaler. Cela peut aider les organisations à renforcer leur protection. Vous trouverez plus d'informations sur les procédures et les réglementations en la matière sur le site du CCB.

NIS2

En janvier 2023, la directive européenne dite NIS2 est entrée en vigueur (directive UE 2022/2555). Cette directive remplace la directive NIS1 de 2016 (transposée en Belgique dans la loi de 7 avril 2019), et elle exige que les États membres imposent des mesures minimales de cybersécurité et des obligations de notification des incidents aux organisations de 17 secteurs critiques, dont la santé.

Il s'agit non seulement des hôpitaux, mais aussi des laboratoires, de la R&D et des entités fabriquant des produits pharmaceutiques de base ou des dispositifs médicaux. Toutes les grandes et moyennes organisations du secteur devront se conformer aux obligations de NIS2. Il s'agit donc de toutes les organisations employant plus de 50 personnes ou dont le chiffre d'affaires annuel est supérieur à 10 millions d'euros.

Les services du gouvernement belge travaillent actuellement d'arrache-pied pour transposer cette directive européenne dans la législation belge afin de donner un contenu concret à ces obligations. La loi sera en place d'ici octobre 2024, suite à quoi les opérateurs disposeront d'une période de transposition. Il va de soi que les organisations ont tout intérêt à commencer à renforcer leur propre cybersécurité dès que possible.

Il est clair que la cybersécurité est une question cruciale, dans tous les secteurs, mais plus particulièrement dans le secteur de la santé. Nous devons garantir la résilience et la continuité des services de santé essentiels pour nos citoyens et la société. Cependant, nous sommes convaincus qu'en travaillant ensemble, nous pouvons faire de la Belgique, aussi dans le secteur de santé, l'un des pays les moins cybervulnérables d'Europe.

Ce livre blanc initié par *Cyberwal by Digital Wallonia* et l'Agence du Numérique contribuera sans aucun doute à cet objectif et nous vous en souhaitons une bonne lecture.

Miguel De Bruycker
Directeur général du CCB

Approach Cyber

La cybersécurité dans le secteur de la santé : la nécessité d'un approche personnalisée

par Jorien Decroos

Approach Cyber est une entreprise spécialisée dans le domaine de la cybersécurité et de la protection des données personnelles. L'équipe d'Approach Cyber, composée d'environ cent personnes, est répartie entre plusieurs bureaux en Belgique et en Suisse. Approach Cyber met à la disposition de ses clients une gamme complète de solutions qui couvrent l'ensemble du spectre de la cybersécurité, leur permettant ainsi d'anticiper, prévenir, protéger, détecter, réagir et récupérer face aux menaces numériques. Ces solutions comprennent des prestations de conseil et d'audit, des programmes de formation et de sensibilisation, la mise en place de solutions technologiques de pointe en matière de sécurité, ainsi que le développement de logiciels sur mesure pour répondre aux besoins spécifiques de ses clients. De plus, Approach Cyber agit en tant que prestataire de services de sécurité managés (MSSP) via leur Centre d'Opérations de Sécurité (SOC) partagé, opérant en français, néerlandais, et anglais, à proximité de leurs clients tant en Belgique qu'à l'étranger.

Approach Cyber accompagne divers acteurs du secteur de la santé. Les besoins en matière de cybersécurité sont aussi variés que les organisations elles-mêmes. Deux groupes qui illustrent parfaitement cette diversité sont les acteurs du secteur médical, tels que les HealthTech et les MedTech, d'une part, et les hôpitaux, d'autre part. Pour Jorien Decroos, Director - Head of Information Security Governance chez Approach Cyber, ces deux groupes demandent des approches très différentes.

LA GOUVERNANCE ET LA CONFORMITÉ POUR LES HEALTHTECH ET MEDTECH

Dans le domaine des entreprises axées sur la santé, telles que les HealthTech et les MedTech, il est devenu impératif d'accorder une attention accrue à la gouvernance et à la conformité en matière de cybersécurité. Cette exigence s'est parfois transformée en un impératif commercial, car les clients de ces entreprises s'attendent désormais à avoir la garantie d'une gestion adéquate de la cybersécurité.

Mais pourquoi cet accent sur la gouvernance ? Parce que c'est à travers elle que les contrôles techniques nécessaires à la sécurité informatique sont mis en place. En ayant une gouvernance solide en place, on peut raisonnablement supposer que les aspects techniques de la sécurité sont également pris en compte. L'utilisation de certains cadres de référence, comme ISO 27001, s'avère être l'un des moyens efficaces pour se conformer à des réglementations telles que NIS 2. Pour les acteurs opérant aux États-Unis, la réglementation HIPAA joue un rôle essentiel et tous ces cadres de référence s'avèrent compatibles, simplifiant ainsi la conformité.

Les entreprises médicales, en particulier les start-ups, ont souvent des budgets dédiés à ces questions, car la sécurité informatique est devenue un élément essentiel de leurs activités commerciales. De plus, elles ont généralement une conscience aiguë des enjeux liés à la cybersécurité, comprenant l'impact direct sur leurs activités commerciales. En conséquence, nombre d'entre elles ont déjà nommé un responsable de la sécurité de l'information (CISO) ou au moins une personne chargée de cette responsabilité au sein de leur organisation.

LES DÉFIS PLUS COMPLEXES DES HÔPITAUX

La situation est très différente dans les hôpitaux, et plusieurs facteurs compliquent considérablement la gestion de la cybersécurité. En ce qui concerne la sensibilisation à la cybersécurité, on remarque qu'elle est nettement moins présente, principalement en raison du pouvoir décisionnaire qui repose souvent entre les mains des professionnels de la santé, qui ne sont pas nécessairement experts en cybersécurité. De ce fait, la conscience des enjeux cybernétiques est souvent moins développée.

Une particularité courante dans les hôpitaux est l'existence de deux réseaux distincts : l'infrastructure informatique (IT) et l'infrastructure opérationnelle (OT). Ces deux réseaux sont souvent gérés de manière séparée, voire indépendante. De plus, les équipes IT dans les hôpitaux sont généralement de taille réduite, ce qui peut constituer un défi supplémentaire pour la gestion de la cybersécurité dans un environnement aussi complexe.

Il convient également de prendre en compte la nature publique des hôpitaux, où un flux constant de personnes entre et sort, ce qui les différencie considérablement des autres types d'organisations. Cette caractéristique rend plus facile l'accès à des zones potentiellement confidentielles, d'autant plus que le roulement du personnel y est considérable. Les médecins, qui sont souvent indépendants et apportent leur propre matériel, les employés, les stagiaires et les étudiants contribuent à la complexité du contexte de sécurité. En outre, les contraintes budgétaires qui pèsent sur les hôpitaux constituent un défi supplémentaire, car les ressources sont limitées. Dans l'ensemble, cela représente un défi de sécurité majeur difficile à surmonter.

LES RISQUES DANS LE SECTEUR HOSPITALIER

En ce qui concerne les risques dans le secteur hospitalier, Jorien Decroos identifie plusieurs aspects cruciaux :

- **Confidentialité :** Les hôpitaux traitent des données extrêmement sensibles et personnelles. La préservation de la confidentialité revêt une importance capitale. Il arrive parfois que des données médicales soient accessibles sans qu'un processus rigoureux de vérification de l'identité soit suivi, même en l'absence de cyberattaques. Le facteur humain représente un risque majeur, d'autant plus dans un environnement où la charge de travail est extrêmement élevée. La sensibilisation et la conscientisation des employés sont essentielles pour contrer ce type de risque.

- **Intégrité :** La possibilité qu'une personne puisse altérer des données médicales soulève des préoccupations majeures. De telles altérations pourraient avoir des conséquences graves sur la vie des patients.

- **Disponibilité :** Récemment, il a été observé plusieurs cas où le dossier patient informatisé (DPI) est devenu indisponible, perturbant ainsi gravement la continuité des opérations pour les hôpitaux et les services d'urgence.

AUGMENTER LA SÉCURITÉ : LA SENSIBILISATION ET LA SEGMENTATION COMME LEVIERS

Quelles sont les mesures les plus efficaces pour obtenir des résultats optimaux en matière de cybersécurité ? Le fonctionnement complexe des hôpitaux signifie que certains réflexes essentiels pour renforcer la sécurité ne sont pas toujours applicables. Par exemple, l'authentification multifacteur (MFA) peut être difficile à mettre en place en raison de la présence de comptes partagés dans certains services.

L'accent doit être mis en premier lieu sur la sensibilisation, tant au sein du personnel médical que de la direction. Deux axes d'approche sont recommandés.

Dans de nombreux hôpitaux, des tests de pénétration sont régulièrement effectués sous différents scénarios. Ces tests comprennent une évaluation classique où un hacker tente de se connecter au réseau à distance, ainsi que des simulations de présence malveillante à l'intérieur de l'hôpital. Dans ce dernier cas, un individu s'introduit physiquement dans l'hôpital et essaie d'accéder à des zones confidentielles ou au réseau. Ces simulations mettent souvent en lumière un manque de segmentation du réseau, ce qui signifie que débrancher une télévision dans une chambre et y brancher un ordinateur portable peut permettre un accès à de vastes parties du réseau. Des techniques d'ingénierie sociale (technique de manipulation utilisée par les cybercriminels pour inciter les gens à partager des informations confidentielles] et de tailgating (une attaque physique d'ingénierie sociale au cours de laquelle une personne cherche à pénétrer dans une zone d'accès restreint où elle n'a pas le droit de se trouver) sont également utilisées pour illustrer les vulnérabilités liées au facteur humain. Jorien Decroos : *« Ce qui est dommage c'est que lorsqu'on travaille en cybersécurité, on n'apprécie plus quand quelqu'un est sympa et nous ouvre la porte. »*.

Une autre menace à prendre en compte est celle de la menace interne, qui peut être le résultat d'un médecin ou d'un membre du personnel hospitalier avec un ordinateur portable infecté qui se connecte au réseau, entraînant une infection du réseau. Une fois de plus, cela souligne l'importance de la segmentation du réseau, qui est cruciale dans les hôpitaux en raison de l'utilisation d'appareils médicaux obsolètes et de technologies en fin de vie, y compris des imprimantes et des caméras de surveillance.

La segmentation du réseau — encore et toujours — se révèle être un aspect fondamental.

Enfin, il est essentiel de considérer la cybersécurité comme un programme avec une stratégie claire et une gouvernance appropriée : savoir quelle est la situation actuelle, là où vous voulez/devez être, comment y aller et impliquer toutes les parties prenantes. Les ressources à investir ne se limitent pas au budget, mais comprennent également le temps et la motivation des personnes impliquées. Souvent, la cybersécurité, en particulier dans le secteur de la santé, est perçue comme une complication. Comprendre le contexte et mettre en place des contrôles conviviaux est crucial pour éviter les contournements des mesures de sécurité : le personnel médical doit pouvoir agir et avoir accès à l'information rapidement afin de faire son travail et de sauver des vies.

PARER À TOUTE ÉVENTUALITÉ

La préparation est d'une importance capitale lorsqu'il s'agit de garantir la sécurité des hôpitaux. Alors que les plans d'urgence hospitaliers initiaux étaient principalement axés sur les urgences physiques, telles que les incendies, une évolution significative a été observée, incorporant de plus en plus une composante liée à la sécurité. Ces plans ont ainsi évolué pour devenir des plans de continuité d'activité, englobant non seulement les aspects physiques, mais aussi la sécurité. Cette transformation est perçue comme une étape essentielle pour la préparation, car elle répond à la nécessité de savoir comment agir en cas de pire scénario possible : qui prendra quelles mesures, qui contacter en cas de crise. Cette préparation exige une compréhension approfondie de l'architecture de l'organisation, de ses ressources, de ses processus, et de ses interdépendances entre les différents systèmes.

La détection précoce des menaces est également d'une importance primordiale, car les hackers ont souvent une présence silencieuse au sein du réseau pendant un certain temps avant de passer à l'action, poursuivant des objectifs variés. Avant de réagir, il est essentiel de savoir où en est actuellement la sécurité du système.

Pour atteindre ces objectifs, il est crucial de réaliser une évaluation de la maturité, différente d'un audit classique. Cette évaluation sert à déterminer ce qui existe déjà et comment cela fonctionne. Elle se penche généralement sur deux aspects complémentaires : la maturité de conception, englobant les procédures et les processus documentés, et la maturité de mise en œuvre, portant sur la manière dont ces éléments sont réellement appliqués, y compris les aspects techniques. La différence entre les deux réside dans le fait que, parfois, tout peut être correctement documenté sans que personne ne soit informé ou consulte ces documents. À l'inverse, il arrive que peu de choses soient documentées, mais que cela n'affecte pas significativement le fonctionnement. Ces deux dimensions sont explorées de manière simultanée lors de l'évaluation, permettant ainsi d'identifier les priorités, d'estimer les budgets et de définir les ressources nécessaires. Il s'agit d'un travail continu d'amélioration de la maturité de la sécurité, adapté à un contexte en constante évolution en raison des exigences réglementaires en constante évolution. Dans ce contexte, NIS 2 offre une opportunité exceptionnelle pour établir une gouvernance solide et une stratégie de cybersécurité.

Parallèlement aux défis internes, les besoins des patients évoluent également. La conscience de la vie privée et de la sécurité des données médicales est en constante augmentation. De plus, le spectre des menaces informatiques s'élargit constamment.

Jorien Decroos souligne l'importance d'impliquer l'ensemble de l'organisation, y compris la direction, dans la gestion des risques de sécurité, car cela ne concerne pas seulement les technologies de l'information, mais l'ensemble de l'entreprise. Il s'agit de gérer les risques commerciaux autant que les risques en cybersécurité.

Ataya Partners

Protéger des vies et des données : les défis de la cybersécurité en milieu hospitalier

par Anthony van der Maren

La cybersécurité est devenue une préoccupation majeure pour les hôpitaux du monde entier, mais les défis qu'ils rencontrent varient en fonction de leurs tailles, de leurs ressources et de leurs priorités. Dans cet article, nous explorons comment Ataya Partners, avec son expertise en cybersécurité, se positionne comme un allié essentiel pour les établissements de santé. Découvrez comment Anthony van der Maren, expert en la matière, accompagne les hôpitaux dans leur quête de certification ISO 27001, tout en soulignant l'importance cruciale de la sensibilisation, de la formation, et des simulations pour préparer ces institutions à l'inévitable : les attaques informatiques. La protection des vies et des données médicales est au cœur de ces enjeux complexes, où la vigilance et la préparation sont devenues la norme pour faire face aux menaces numériques croissantes.

L'ÉPÉE ET LE BOUCLIER DE LA CERTIFICATION ISO 27001

Au sein d'Ataya Partners, Anthony van der Maren, Managing Partner, met son expertise au service des centres hospitaliers et les accompagne dans leur cybersécurité, jusqu'à l'obtention de la certification ISO 27001. L'obtention de la certification ISO 27001 est un jalon important pour les hôpitaux dans leur quête de cybersécurité. Cette certification repose sur un ensemble de bonnes pratiques qui permettent de gérer un système de sécurité de l'information de manière efficace. Anthony van der Maren nous révèle que ce n'est pas tant une quête de perfection que d'amélioration constante, de mesures et de changements pour s'adapter aux risques émergents. Pour insuffler ces changements, la norme ISO 27001 propose une liste de 93 contrôles de sécurité à passer en revue. Lorsque ces contrôles ont été traités, soit parce que le risque mentionné est sous contrôle ou parce qu'il ne s'applique pas à l'établissement en question, un organisme de contrôle pourra auditer et délivrer, ou non, cette certification.

Notons que la directive européenne NIS 2, qui vise à harmoniser et à renforcer la cybersécurité du marché européen et votée en décembre 2022, a ajouté la santé dans la catégorie des secteurs hautement critiques. Ce secteur de la santé ne concerne pas seulement les hôpitaux, mais aussi des laboratoires de référence, les fabricants de dispositifs médicaux ou de préparations pharmaceutiques et autres. Et à ce titre, la certification ISO 27001 est une base essentielle pour la mise en conformité à la directive NIS 2.

Bien que la certification ISO 27001 soit une base solide pour la gestion de la cybersécurité, Anthony van der Maren nuance : *« Une certification de sécurité n'empêche pas d'avoir un acte de piratage. Mais c'est une meilleure garantie sur le fait que l'établissement pourra probablement mieux résister et mieux redémarrer son activité. »*

> *Aux hôpitaux je ne dis jamais*
> ***"si vous êtes attaqués",***
> *je dis toujours*
> ***"quand vous serez attaqués***
>
> ***Anthony van der Maren***

LES DÉFIS DE LA CYBERSÉCURITÉ HOSPITALIÈRE : UNE QUESTION DE TAILLE, DE PRIORITÉ ET DE BUDGET

L'approche des hôpitaux en matière de cybersécurité est un délicat équilibre entre leurs tailles, leurs ressources financières et leur sens des priorités. Les petites structures hospitalières, souvent démunies et disposant de moyens financiers limités, sont confrontées à des défis particulièrement ardus pour renforcer leur cybersécurité. Les contraintes budgétaires sont une réalité incontournable, rendant difficile l'allocation de ressources spécifiques à la protection des systèmes informatiques.

Même pour les hôpitaux de plus grande envergure, la question de la cybersécurité demeure un enjeu de priorité. Cependant, il est courant de constater que l'intérêt pour la cybersécurité ne se manifeste qu'en réaction à des incidents survenus dans des hôpitaux voisins. Les attaques numériques subies par d'autres établissements de santé agissent comme un catalyseur, poussant les hôpitaux à reconsidérer leur propre préparation à de telles menaces.

Un autre défi réside dans l'absence de budgets spécifiques dédiés à la cybersécurité dans de nombreux hôpitaux. Les budgets informatiques sont souvent « saupoudrés », regroupant toutes les demandes informatiques au sein d'une même enveloppe. Cette approche peut rendre difficile l'attribution de fonds suffisants pour mettre en place des mesures de cybersécurité robustes et adaptées aux besoins spécifiques de chaque établissement.

En somme, la cybersécurité dans le milieu hospitalier est un domaine en constante évolution, où les hôpitaux, petits ou grands, doivent jongler avec des ressources limitées tout en se montrant de plus en plus réactifs face aux menaces croissantes.

AU-DELÀ DE L'ANALYSE DES RISQUES, L'HUMAIN AU CŒUR DES ENJEUX

Les hôpitaux, confrontés à la complexité croissante des enjeux de cybersécurité, expriment fréquemment le besoin de réaliser des analyses de risques exhaustives. Cependant, Anthony van der Maren souligne l'importance de ne pas s'arrêter à cette étape initiale. La simple identification des risques ne suffit pas à garantir une cybersécurité efficace. Souvent, les établissements de santé se retrouvent face à une longue liste de menaces potentielles, ce qui peut rapidement sembler écrasant.

Ce qui est crucial à comprendre, c'est que tous les aspects de la cybersécurité ne relèvent pas uniquement du département informatique. La sensibilisation et la formation des employés, ainsi que la prise en compte du facteur humain, sont des éléments clés pour prévenir les erreurs humaines, qui peuvent se produire à tout moment. Le facteur humain est souvent un maillon faible dans la chaîne de la sécurité informatique, et c'est pourquoi la sensibilisation à la cybersécurité au sein de l'ensemble du personnel hospitalier revêt une importance cruciale.

Si l'analyse de risques est une étape essentielle, la cybersécurité dans les hôpitaux ne peut pas se limiter à cette seule phase. La sensibilisation, la formation et la vigilance constante vis-à-vis du facteur humain sont tout aussi indispensables pour garantir la protection des systèmes d'information et la confidentialité des données médicales.

*Du point de vue médical, il faut **protéger la vie ET la vie privée** du patient*

Anthony van der Maren

CYBERATTAQUE DANS LES HÔPITAUX : L'IMPORTANCE DES SIMULATIONS ET DE L'ANTICIPATION

Au sein du secteur hospitalier, la préparation aux attaques informatiques ne saurait être complète sans l'intégration de simulations et d'exercices pratiques. Ces simulations sont cruciales pour anticiper les scénarios potentiels, évaluer les capacités de réaction en cas d'incident et former le personnel à faire face aux situations de crise. Les exercices de continuité permettent aux établissements de santé de se préparer à l'inattendu, de mettre en place des plans d'action concrets et de garantir une réponse rapide et coordonnée en cas d'attaque informatique. Il ne s'agit pas seulement de prévoir les actions techniques, mais aussi de planifier la communication interne et externe, de gérer les ressources humaines, et de maintenir la confiance des patients et des partenaires.

En fin de compte, ces simulations visent à assurer que les hôpitaux disposent de procédures bien définies et de personnel formé, prêt à réagir de manière efficace en cas d'attaque informatique. Savoir à quoi s'attendre et comment réagir peut faire toute la différence dans la préservation de la sécurité des patients et la continuité des opérations hospitalières, même en période de crise.

L'AVIQ : à la confluence de l'innovation numérique, de la protection des données et de la stratégie d'entreprise

par Françoise Lannoy et Séverine Ovyn

Fondée en 2015, l'Agence pour une vie de qualité (AVIQ) joue un rôle crucial en Wallonie. Elle est le pilier des politiques de santé de soutien aux personnes en situation de handicap et des politiques familiales.

L'AVIQ est née de la 6e réforme de l'État, qui a organisé un très vaste transfert de compétences en matière de santé et de sécurité sociale vers les entités fédérées. Pour la Wallonie, ce fut l'occasion de rassembler ces compétences jusqu'alors exercées par sept administrations et organismes publics fédéraux, régionaux et communautaires au sein d'un seul organisme.

Avec près de 900 agents et un budget annuel de 6,7 milliards d'euros, l'AVIQ joue un rôle primordial. Elle régule, contrôle et finance divers secteurs non marchands, tels que les hôpitaux, les maisons de repos, la médecine de première ligne, les services d'accompagnement des personnes en situation de handicap et les allocations familiales. On dénombre quelque 2.500 opérateurs actifs sur notre territoire, eux-mêmes employant plus de 100.000 travailleurs.

Compétence partagée entre le Fédéral et les entités fédérées, l'e-santé constitue un enjeu majeur. En effet, le développement de notre système de santé ne pourra avoir lieu sans un développement massif et cohérent de l'e-santé.

Pour la Wallonie, la mise en place et le soutien d'un écosystème de santé numérique relatif au parcours de vie du citoyen permet de répondre à différents défis.

Premièrement, il permet de réduire le nombre d'examens inutiles et onéreux ce qui évite des doubles encodages et un risque d'erreurs préjudiciables. Deuxièmement, il permet aux prestataires d'aide et de soins de passer plus de temps avec leurs patients en réduisant sa charge administrative, ce qui favorise une prise en charge plus qualitative. Enfin, il permet de renforcer l'empowerment du patient quant à la gestion de ses données de santé pour être un réel acteur de son parcours de vie.

Dans ce cadre, la cybersécurité est bien entendu d'une importance majeure pour nos politiques et nos partenaires afin d'assurer une meilleure maîtrise des systèmes, de maintenir à niveau les normes de qualité et de sécurité et par là même, la continuité des services pour nos concitoyens.

LA PROTECTION DES DONNÉES À L'AVIQ : MINIMALISME ET SÉCURITÉ

Le respect de la vie privée est primordial, a fortiori dans le domaine de la santé, par le respect strict du Règlement général de protection desdonnées (RGPD).

Avant tout échange de données médicales entre des professionnels de la santé ou d'aide, certaines conditions doivent être vérifiées. Premièrement, le consentement éclairé du patient ou de la personne aidée est indispensable. Celui-ci doit faire l'objet d'un accord explicite du citoyen, qui aura préalablement été informé au mieux de la portée de son consentement. De plus, le consentement doit pouvoir être retiré facilement et rapidement par les citoyens qui le désirent.

Deuxièmement, les prestataires de soins qui accèdent aux dossiers médicaux doivent nécessairement prouver une relation de soin avec le patient. Ainsi, il faut veiller à empêcher les médecins qui ne soignent pas le patient (ex. : médecins contrôle, médecins du travail, etc.) d'accéder aux données qui transitent par la plateforme d'échange de données médicales. Le même principe doit s'appliquer dans le champ de l'aide.

En ce qui concerne les données à portée épidémiologique, qui éclairent la décision politique et donc qui intéressent particulièrement l'AVIQ, elles doivent toujours être correctement anonymisées par une institution compétente. L'AVIQ, s'efforce de minimiser la collecte de données personnelles. Françoise Lannoy, Administratrice générale de l'AVIQ, explique que cette philosophie repose sur le principe « au moins on dé-

tient de données et au moins on s'expose aux risques de fuite».

Dès lors l'AVIQ applique une politique de plus en plus stricte et limitative en termes de conservation de données sensibles, strictement nécessaires et pertinentes pour l'exercice de ses missions. Ainsi, dans le cadre de risques sanitaires, l'AVIQ a développé un système de surveillance des maladies infectieuses: captant tous les risques par une déclaration obligatoire des maladies infectieuses possible afin d'évaluer la prise en charge du patient et de son entourage sur base du caractère épidémique de la maladie. L'enjeu était de déployer un outil performant sur l'ensemble du territoire, garantissant un suivi en temps réel de tout risque d'épidémie mais également conforme à l'ensemble des règles de protection de la vie privée et de sécurité des systèmes.

L'AVIQ est donc soumise à un contrôle rigoureux de ses processus de collecte, de traitement et de destruction des données intégrant dans ses équipes de nouvelles disciplines telles que ses DPO et son CISO, maillons essentiels dans la mise en place de nouvelles réglementations et de nouveaux outils rendus indispensables pour l'exercice de ses missions mais également pour la gestion des risques et des crises.

LE DÉVELOPPEMENT DE PROJETS MAJEURS: L'EXEMPLE DU CARNET DE VIE DIGITALISÉ

En juillet 2021, le Gouvernement wallon approuvait le Plan de Relance de la Wallonie avec un budget d'investissement de 7,6 milliards. L'AVIQ est impliquée directement dans le déploiement de l'e-Santé en Wallonie, soutenu par ce vaste plan de relance, en tant qu'autorité régulatrice qui devra à l'avenir définir les contenus, les règles et standards et les diffuser aux prestataires de soins et de services ainsi qu'aux producteurs de logiciels.

Parmi ces projets, le déploiement du carnet de vie digitalisé occupe une place centrale. Cette initiative vise à rassembler un maximum d'informations concernant chaque individu, permettant ainsi aux prestataires de disposer de données partagées sur leur parcours de vie, de soins et d'accompagnement en Wallonie.

Le carnet de vie digitalisé s'articule autour de l'idée fondamentale de garantir les droits des patients et de leur offrir un accès transparent à leurs données. Il vise à créer une plateforme où les patients peuvent consulter et suivre les informations qui les concernent.

Dans ce contexte, le rôle de l'AVIQ est double. Tout d'abord, celui du financement. La Wallonie alloue des ressources substantielles pour soutenir ces projets ambitieux, et l'AVIQ est chargée d'opérationnaliser le plan. Ensuite, la régulation du domaine. Elle veille à la qualité des outils développés, à leur sécurité et à leur certification. Cette responsabilité est cruciale pour garantir que les projets tels que le carnet de vie digitalisé respectent les normes élevées en matière de protection des données et de sécurité de l'information.

Le déploiement de ces projets novateurs nécessite également un élargissement des compétences de l'AVIQ. En particulier, la mise en place du carnet de vie digitalisé requiert un nouveau savoir-faire au sein de l'administration. L'AVIQ doit être en mesure d'assurer que les droits des individus sont préservés, que les données restent intactes et que l'intégrité des informations est garantie. Ainsi, l'AVIQ s'engage dans une évolution majeure en développant de nouvelles compétences pour soutenir efficacement la réalisation de ces projets ambitieux, qui sont à la fois innovants et centrés sur l'amélioration de la qualité des soins et des services de santé en Wallonie.

STRATÉGIE INTERNE DE L'AVIQ: ANTICIPATION ET RENFORCEMENT DE LA CYBERSÉCURITÉ

Au-delà de son rôle externe de régulateur et de gestionnaire de politiques de santé, l'AVIQ accorde une attention significative à sa stratégie interne, notamment en ce qui concerne la cybersécurité et la modernisation de ses systèmes. Cette démarche est essentielle pour garantir la continuité de ses activités et la protection des données, tant pour son organisation que pour les citoyens qu'elle sert.

Ainsi, l'Agence a entrepris un audit de maturité, achevé en 2022, pour évaluer sa capacité à faire face aux menaces et aux vulnérabilités potentielles. Séverine Ovyn, Chief Information Officer (CIO) de l'AVIQ, explique que l'audit a relevé que l'AVIQ avait historiquement adopté une approche de type «forteresse» pour ses systèmes informatiques, en limitant l'accès depuis l'extérieur et en internalisant de nombreuses fonctionnalités. Cette stratégie a fonctionné jusqu'à présent, mais s'annonce inadaptée à mesure que l'Agence se tourne vers la dématérialisation et les outils collaboratifs basés sur le cloud. Cette transition implique une ouverture accrue de ses systèmes, ce qui nécessite une adaptation en matière de cybersécurité.

La feuille de route résultant de l'audit a joué un rôle clé en orientant les efforts de l'AVIQ pour améliorer sa cybersécurité. Elle a identifié plusieurs domaines d'action essentiels. Tout d'abord, l'Agence a établi une cellule cybersécurité interne et nommé un Chief Information Security Officer (CISO) pour coordonner les efforts de protection des données et de sécurité de l'information.

L'AVIQ s'est également engagée à revoir son infrastructure informatique dans son ensemble, afin de la préparer à l'intégration des nouvelles applications de dématérialisation. Cette démarche vise à s'assurer que l'environnement technologique est solide et sécurisé avant de mettre en place de nouveaux outils.

La transposition de la loi NIS 2 en législation belge est un autre point central de la stratégie de cybersécurité de l'AVIQ. Bien que la conformité à cette loi ne soit pas encore obligatoire, l'Agence la considère comme essentielle et anticipe son entrée en vigueur afin de garantir sa propre protection et la continuité de ses services. Elle travaille activement à adapter ses politiques de sécurité, sa gouvernance, et à former son personnel à la gestion des risques, aux meilleures pratiques en matière de sécurité informatique et à la détection des intrusions.

En somme, la stratégie interne de l'AVIQ englobe des aspects techniques, organisationnels et humains. Elle vise à créer une culture de la cybersécurité au sein de l'agence, à anticiper les menaces et à garantir la protection des données et des services, au bénéfice des citoyens wallons et de l'ensemble du personnel de l'AVIQ.

LA GUERRE DES TALENTS DANS LE DOMAINE DE LA CYBERSÉCURITÉ

Un aspect essentiel de la transformation numérique de l'AVIQ concerne la question des compétences au sein du pôle digital. Françoise Lannoy soulève deux points cruciaux:

1. **Stratégie RH spécifique pour le pôle digital:** Il est essentiel de reconnaître que les professionnels de la technologie, en raison de la spécificité du marché de l'emploi, peuvent être soumis à des pressions salariales et de recrutement plus importantes que d'autres domaines. Cette surenchère concurrentielle entre les entreprises et les administrations peut entraîner des déséquilibres dans la gestion des talents. Ainsi, l'AVIQ a dû élaborer une politique salariale et une approche de gestion des talents distinctes pour son pôle digital, tout en maintenant un équilibre global au sein de l'organisation.

2. **Formation des jeunes en cybersécurité:** Un autre défi important auquel l'AVIQ est confrontée est la formation des jeunes talents en matière de cybersécurité. Les jeunes diplômés des écoles et des centres de formation en informatique ne sont pas toujours sensibilisés à la cybersécurité ni formés dans ce domaine. Cette lacune peut se manifester par un manque d'expertise en matière de sécurité informatique et une absence de réflexes appropriés pour assurer la protection des données et des systèmes.

L'INTÉGRATION DU NUMÉRIQUE DANS LA STRATÉGIE D'ENTREPRISE

Lors de cet entretien, Françoise Lannoy et Séverine Ovyn ont souligné un aspect fondamental de la transformation numérique: il ne s'agit pas seulement d'une question informatique, mais d'une véritable stratégie d'entreprise.

Françoise Lannoy a mis en lumière l'importance de développer une vision stratégique pour l'AVIQ, dans laquelle le numérique est intégré à tous les niveaux de l'organisation. Cette vision dépasse largement le champ de la technologie et englobe la manière dont l'agence interagit avec ses partenaires, les services qu'elle offre et son impact sur la qualité de vie en Wallonie.

La transformation numérique à l'AVIQ se veut une transformation inclusive en veillant à n'exclure personne par un accompagnement individuel mais aussi collectif et participatif. Cette démarche s'organise à tous les niveaux: au sein du Conseil général de l'Agence soutenant la stratégie et le plan d'action proposé, du Comité de direction, des équipes, des parties prenantes et des usagers. C'est pour cette raison, que lors de tout le processus de digitalisation, un Comité des utilisateurs sera mis en place pour tester les outils et s'assurer de leur pertinence et de leur accessibilité.

Une transformation inclusive ne peut être complète et adaptée que si elle s'accompagne humainement et physiquement pour toutes les personnes agents comme usagers de l'Agence qui, quoi qu'on fasse et pour des raisons diverses, restent confrontées à l'exclusion numérique.

La transformation numérique de l'AVIQ est donc bien plus qu'une simple mise à niveau technologique. C'est une stratégie d'entreprise qui vise à améliorer la qualité des services offerts, à renforcer la cybersécurité, à attirer et retenir les talents, et à préparer l'agence à un avenir numérique prometteur. Cette vision, portée par le Comité de direction, garantit que le numérique reste au cœur de la mission de l'AVIQ, pour le bénéfice de tous les citoyens wallons.

Sécurité informatique au **CHC**: leçons d'une attaque majeure et perspectives

par Philippe Olivier, Alain Coudijzer, Laurence Delcomminette et Frédéric Pampalone

En région liégeoise, le Groupe santé CHC occupe une place de premier plan dans le secteur médical, avec ses cliniques, centres médicaux, résidences pour personnes âgées, structures d'accueil pour personnes handicapées, crèche, et services opérationnels. Comptant près de 3800 postes de travail sur plusieurs sites, plus de 5000 utilisateurs, 800 serveurs, et un helpdesk traitant quotidiennement 120 tickets, le CHC est, en somme, une petite ville à part entière.

En novembre 2022, le CHC a été la cible d'une attaque informatique majeure. Face à cette crise, plusieurs acteurs clés du CHC ont joué un rôle décisif dans la gestion de cette situation exceptionnelle.

Philippe Olivier, Directeur médical en charge de la transition numérique, après avoir passé deux décennies à la direction médicale opérationnelle, apporte son expertise à la transition vers la technologie numérique et l'intelligence artificielle. Alain Coudijzer, responsable de l'informatique du CHC, assure avec son équipe la mise en place et la fourniture sécurisée des services informatiques nécessaires au Groupe. Laurence Delcomminette est la Risk Manager du CHC, en charge de la gestion des besoins du métier médical et de la communication des demandes entre la cellule de crise informatique et les autres cellules de crise durant la cyberattaque. Enfin, Frédéric Pampalone, en qualité de Chief Information Security Officer (CISO) du CHC, est le gardien vigilant de la sécurité informatique.

Dans cet article, nous plongerons dans l'univers complexe et exigeant du CHC, et nous laisserons la parole à ces experts pour qu'ils nous partagent leur expérience sur le

terrain suite à la cyberattaque de novembre 2022. Comment ont-ils géré la crise ? Quelles leçons ont-ils tirées ? Et comment envisagent-ils l'avenir de la sécurité informatique au sein de l'une des institutions médicales les plus importantes de la province de Liège ? Découvrez comment ils ont fait face à l'adversité pour garantir la continuité des soins de santé.

L'APPEL QUE L'ON VOUDRAIT NE JAMAIS RECEVOIR

Lorsqu'on demande à Frédéric Pampalone de nous décrire le moment où l'attaque a été découverte, la précision des informations démontre l'importance de l'événement : *« 18 novembre à 14 h 27, je reçois un coup de fil d'un collègue qui signalait un problème. Il avait été alerté par le redémarrage d'un antivirus sur l'un des serveurs. Ce redémarrage avait dévoilé un message d'alerte inquiétant : le système était infecté par un ransomware. »*

Face à cette menace soudaine, une série de décisions rapides s'imposaient. En quelques coups de téléphone, l'équipe informatique a rapidement mis en place des mesures pour stopper la propagation de l'attaque. Ces mesures ont nécessité la déconnexion totale du réseau. Toutes les liaisons extérieures, notamment Internet, ont été coupées pour éviter que l'attaque ne se propage davantage.

Bien que la plupart des systèmes internes aient continué à fonctionner, les experts ont découvert que de nombreuses applications étaient connectées à l'extérieur, bien au-delà de ce qui était initialement connu. La priorité absolue, en plus de lancer une enquête sur l'attaque elle-même, a été de rétablir uniquement les connexions essentielles pour la prestation des soins de santé.

Un comité de pilotage a été mis en place, et des réunions se sont succédé à un rythme effréné, reflétant la gravité de la situation. Si tout cela ressemblait à la mise en œuvre d'un plan catastrophe, c'était précisément ce dont il s'agissait.

La véritable crise, cependant, a été de gérer les problèmes créés par la coupure des liens Internet pour arrêter l'attaque. Les équipes ont dû faire face aux conséquences de cette action drastique, mais heureusement, contrairement à d'autres établissements de santé, ils n'ont pas été confrontés à une crise qu'ils n'avaient pas eux-mêmes générée. Dans l'ensemble, la gestion de la crise a été relativement réussie grâce à la réactivité des équipes et l'attaque n'a pas pu causer de dommages majeurs.

Pour les patients, l'impact a été minime, se limitant principalement à l'impossibilité de prendre rendez-vous en ligne et à un léger retard dans la transmission électronique des résultats au médecin généraliste, ce qui a été rapidement résolu.

GÉRER L'APRÈS CRISE

Après la découverte de l'attaque, la première mesure prise a été radicale : la coupure globale d'Internet. Cette crise soudaine a été perçue comme une opportunité de repenser en profondeur la sécurité informatique, conformément aux nouvelles exigences.

En parallèle, de nombreux outils informatiques ont été déployés, tous orientés vers l'amélioration de la sécurité globale du CHC. Alors que certains de ces projets étaient déjà en cours, leur mise en œuvre a été accélérée de manière significative pour répondre à la nouvelle urgence. Cela n'a pas été sans perturbations, car la rapidité du déploiement a parfois généré des contraintes et des défis inattendus.

L'impact financier de cette accélération a également été notable. Les ressources et les investissements qui étaient à l'origine destinés à des projets médicaux ou administratifs ont été réaffectés à des initiatives purement sécuritaires. Bien que ces améliorations auraient été nécessaires à un moment donné, la précipitation avec laquelle elles ont été mises en œuvre a modifié la répartition des ressources.

Cette situation a créé un dilemme, car ces efforts sécuritaires ne se traduisent pas directement en valeur ajoutée pour les utilisateurs finaux. Cependant, ils sont indispensables pour protéger le CHC contre de futures attaques et garantir la continuité des soins de santé. Il est donc crucial de trouver un équilibre entre les investissements en sécurité et les projets métiers qui apportent une valeur directe aux patients et au personnel médical.

Après l'incident et la gestion de la crise immédiate, l'équipe s'est rapidement réunie pour élaborer des processus internes qui, jusqu'alors, n'avaient pas été développés. L'objectif était de mieux gérer la priorisation des incidents en coordination avec les besoins exprimés par les métiers. Un exemple concret de cette démarche est la mise en place d'un flux de données complet, une tâche complexe sur laquelle le CHC travaille activement.

LES ENSEIGNEMENTS CLÉS TIRÉS DE L'ATTAQUE AU CHC

L'attaque subie par le CHC a été une épreuve cruciale, source d'enseignements précieux qui sont applicables à n'importe quelle organisation. Voici quelques-unes des leçons clés qui ont émergé de cette expérience :

- **Gestion des utilisateurs et inventaire :** L'importance d'une gestion efficace des utilisateurs et d'un inventaire à jour ne peut être sous-estimée. Ces éléments permettent de fermer autant de portes que possible aux attaques.

- **Surveillance continue :** La mise en place d'un système de surveillance a été une leçon importante. Elle permet de détecter rapidement les anomalies et les menaces potentielles, et nous recommandons vivement cette pratique à toutes les organisations.

- **Connaissance des risques et des flux :** Une bonne compréhension des risques et des flux de données est essentielle. Cette connaissance permet une réaction plus éclairée en cas d'attaque.

- **Classification des applications :** Identifier les applications à héberger à l'extérieur et celles à conserver à l'intérieur est crucial. Cette distinction permet de mieux résister aux attaques en fonction de la nature du service. Il est nécessaire d'anticiper cette réflexion pour éviter de prendre des décisions à la hâte.

- **Réactivité et compétences :** Les équipes du CHC ont montré une réactivité exceptionnelle, ce qui a été un facteur déterminant pour atténuer les conséquences de l'attaque. Il est essentiel de ne pas se contenter du strict minimum en termes de compétences, mais de cultiver une culture de la sécurité au sein de l'organisation.

- **Résilience :** Le CHC a travaillé en étroite collaboration avec les différents secteurs, notamment les laboratoires, les blocs opératoires, la pharmacie, pour identifier leurs besoins essentiels en matière d'informatique en cas d'indisponibilité prolongée. Cette préparation a permis de gagner du temps au début de la crise. Il est recommandé de consulter régulièrement les métiers médicaux pour comprendre leurs besoins spécifiques et leurs interdépendances.

Ces enseignements se déclinent en trois axes interdépendants :

- **Axe technologique :** Investir dans des logiciels et des systèmes performants, bien que coûteux, est essentiel pour détecter les vulnérabilités et les failles.

- **Axe humain :** Cultiver une culture de sécurité au sein de l'organisation est fondamental. Il ne suffit pas d'avoir des outils performants si les utilisateurs ne sont pas sensibilisés et prêts à adopter des comportements sécuritaires.

- **Axe managérial :** La gestion des procédures, de l'organisation et des mises à jour est tout aussi cruciale. Une attention particulière doit être portée à l'amélioration continue des processus et des protocoles.

Ces trois axes sont indissociables, et aucun ne doit être privilégié au détriment des autres. Ils forment un écosystème complexe qui contribue à renforcer la résilience d'une organisation face aux menaces informatiques croissantes.

LES VULNÉRABILITÉS COMPLEXES D'UN HÔPITAL : ENTRE ACCÈS PHYSIQUES ET MENACES INFORMATIQUES

La vulnérabilité d'un hôpital est un sujet complexe à appréhender, car elle englobe divers aspects, à la fois physiques et informatiques. Au sein de ces établissements, la vulnérabilité physique est une réalité à laquelle il faut faire face. Les hôpitaux sont des environnements ouverts, conçus pour accueillir les patients et leur entourage. Cette ouverture facilite l'accès à l'intérieur de l'établissement, ce qui en fait une cible potentielle pour des intrusions non autorisées.

Cependant, la vulnérabilité ne se limite pas aux frontières physiques de l'hôpital. Les hackers exploitent également la dimension humaine de la sécurité. Ils utilisent des tactiques telles que la « fraude au président », où ils se font passer pour une autorité de l'hôpital, souvent un membre de la direction, pour obtenir des informations sensibles ou demander des actions spécifiques à l'équipe informatique. Ces tentatives trompeuses soulignent l'importance cruciale de la mise en place et du respect des règles de sécurité pour assurer une protection maximale.

Dans cette optique, un chantier majeur est en cours au CHC, axé sur la centralisation de la gestion des identités et des droits d'accès. L'idée est de cloisonner les accès de manière à ce que chaque utilisateur dispose uniquement des autorisations nécessaires à ses fonctions. Cette approche, bien que contraignante pour l'utilisateur, renforce considérablement la sécurité de l'ensemble du système. Dans un environnement comptant jusqu'à 5000 collaborateurs, cette tâche n'est pas anodine, mais elle est essentielle pour minimiser les risques.

Frédéric Pampalone souligne un point crucial : la sécurité des données. Au cœur de l'hôpital, ces données sont souvent irremplaçables et impossibles à recréer. La perte de certaines données peut avoir des conséquences graves, affectant directement la qualité des soins prodigués aux patients. Par exemple, dans le domaine médical, la perte de données d'imagerie médicale peut compromettre gravement le traitement d'un patient atteint d'une maladie grave, comme le cancer.

L'importance de la communication et du partage des leçons apprises

L'expérience du CHC met en lumière l'importance cruciale de la communication et du partage des leçons apprises en matière de cybersécurité.

Dans ce contexte, les autorités ont un rôle crucial à jouer en promouvant la transparence et en encourageant les institutions à partager leurs expériences, même en cas d'attaque. Alain Coudijzer : *« Il ne faut pas avoir honte de reconnaître sa vulnérabilité, car cela renforce la résilience de l'ensemble du système. La communication ouverte et la collaboration entre les établissements de santé peuvent également jouer un rôle clé en matière de cybersécurité. Cette solidarité est précieuse, car elle renforce la sécurité informatique hospitalière collective. »*

En fin de compte, la cybersécurité est un défi permanent, et la sensibilisation, la préparation et la communication sont des éléments fondamentaux pour protéger les établissements de santé et garantir la continuité des soins. Philippe Olivier : *« En partageant les leçons apprises, nous renforçons notre capacité à faire face aux menaces numériques et à assurer la sécurité des patients et du personnel médical. La cybersécurité hospitalière est un effort collectif, et ensemble, nous pouvons renforcer notre résilience face aux défis à venir. »*

Microsoft

Protéger le futur : l'alliance de la cybersécurité et de l'innovation dans le monde médical

par Bart Asnot

La cybersécurité a toujours été au cœur des préoccupations de Microsoft, et en Belgique, la société dispose d'équipes dédiées à cet enjeu majeur. À l'échelle mondiale, Microsoft investit massivement dans la cybersécurité, allouant annuellement 4 milliards de dollars, pour un total impressionnant de 20 milliards de dollars sur les cinq prochaines années.

Dans cet article, nous plongerons dans le monde de la cybersécurité médicale en Belgique et dans le monde. Pour nous guider dans cette exploration, Bart Asnot, National Security Officer et Cloud Solution Architect Manager Security chez Microsoft, partage sa vision, son expertise et ses conseils avisés.

LES BONS RÉFLEXES : LA PROACTIVITÉ

La cybersécurité est un domaine en constante évolution où l'inaction peut s'avérer coûteuse, voire désastreuse. Bart Asnot insiste sur l'importance de la proactivité en matière de sécurité informatique, que ce soit dans le secteur médical ou ailleurs. Il préconise d'adopter une approche proactive dès la phase de conception de projets. Imaginons un projet de digitalisation dans le cloud : la question cruciale à se poser dès le départ est de savoir comment le réaliser de la manière la plus sécurisée possible. Cela signifie intégrer des pratiques de sécurité dès le début du processus, plutôt que de les ajouter en réaction à une menace.

GÉRER UN INCIDENT DE CYBERSÉCURITÉ : LES PRIORITÉS CRUCIALES

Quand un incident survient, que ce soit dans le secteur médical ou ailleurs, il est essentiel de comprendre que toutes les attaques ne sont pas égales. Certaines entreprises, grâce à leur maturité en cybersécurité, peuvent être moins exposées, repoussant ainsi le risque vers des cibles plus vulnérables. Lorsqu'une attaque se produit, l'impact dépend également de la partie de l'entreprise qu'elle affecte. Dans les cas les plus graves, l'activité peut être complètement paralysée. Chez Microsoft, par exemple, lors d'un incident de cybersécurité chez un client, trois questions fondamentales sont posées.

La 1re est « Quel est le niveau de gravité ? ». Est-ce que les infrastructures critiques sont attaquées ? Est-ce que les bases de données contenant des informations sensibles, comme les identifiants et les mots de passe des utilisateurs, sont compromises ? Une attaque visant ces éléments constitue un incident extrêmement grave.

Ensuite, les deux questions suivantes sont « Qui sont les assaillants et depuis combien de temps sont-ils dans mon environnement ? ». Il est crucial de comprendre les attaques en découvrant les techniques, les tactiques et les procédures utilisées par les assaillants pour accéder à l'infrastructure et causer des dommages. Cette information est essentielle pour agir de manière appropriée. Sur la base de ces informations, des procédures sont mises en place pour « reconstruire » l'infrastructure. Dans de nombreux cas, cela implique de recommencer à zéro pour créer une nouvelle infrastructure sécurisée.

Une fois ces étapes franchies, les priorités sont ensuite définies pour permettre à l'entreprise de redevenir opérationnelle. Par exemple, dans le cas des hôpitaux, la priorité pourrait être de rétablir en premier le service des urgences pour assurer la continuité des soins.

Les organisations ayant une maturité élevée en matière de sécurité informatique ont généralement des manuels d'intervention en cas d'incident, avec des procédures claires et une séquence d'actions à suivre. Malheureusement, de nombreux hôpitaux et établissements médicaux manquent souvent de ces procédures essentielles. Bart Asnot met en lumière cette lacune et souligne l'importance de disposer de directives formelles pour réagir efficacement aux incidents de cybersécurité, en particulier dans le domaine médical où la sécurité des données des patients est en jeu.

LES PREMIÈRES ACTIONS POUR RENFORCER LA CYBERSÉCURITÉ DANS LES HÔPITAUX

La sécurité des données médicales revêt une importance cruciale dans les hôpitaux, où la vie et le bien-être des patients sont en jeu. Bart Asnot partage ses recommandations essentielles pour renforcer la résilience contre les cyberattaques, en s'appuyant sur des leviers stratégiques.

1. Connaître son environnement : la cartographie incontournable

Le premier pas vers une cybersécurité solide consiste à comprendre son environnement actuel. Avant de mettre en place des outils et des mesures de sécurité, il est essentiel de découvrir et de cartographier l'infrastructure existante. Cette étape ne nécessite pas de compétences techniques avancées, mais plutôt une collaboration étroite avec les architectes IT et les parties prenantes de l'organisation. L'objectif est de créer un plan d'action clair en cas d'incident, en identifiant les actifs critiques et les points vulnérables. Sans cette base, toute tentative de renforcement de la cybersécurité peut être vaine.

2. La surveillance : un impératif pour les environnements séparés

Dans le secteur médical, de nombreux hôpitaux ont des environnements distincts pour les systèmes informatiques (IT) et les systèmes opérationnels (OT) dédiés aux équipements médicaux. Cependant, la séparation n'implique pas l'isolement en termes de cybersécurité. La surveillance est essentielle pour détecter rapidement toute menace. Si une attaque réussit à migrer du réseau IT vers le réseau OT, les conséquences peuvent être graves. Les hôpitaux doivent donc mettre en place une surveillance continue des deux environnements, permettant de détecter les signes précurseurs d'intrusion et d'agir rapidement pour les contrer.

3. Authentification Multifacteur (MFA) : une protection incontournable

De nombreuses institutions médicales ont adopté des solutions basées sur le cloud pour améliorer leur efficacité et leur collaboration. Cependant, l'utilisation du cloud rend les données d'identification accessibles via Internet, ce qui les expose potentiellement aux cyberattaques. C'est là que l'authentification multifacteur (MFA) entre en jeu. Le MFA exige une double vérification de l'identité de l'utilisateur, ce qui ajoute une couche de sécurité essentielle. Sans cette protection, les hackers peuvent exploiter des techniques d'automatisation avancées, notamment l'utilisation de kits de phishing pour cibler des individus spécifiques.

En résumé, ces trois points ne sont pas seulement des recommandations, mais des piliers fondamentaux de la cybersécurité dans le secteur médical. Même avec les technologies de sécurité les plus avancées, leur absence peut laisser les hôpitaux vulnérables aux cybermenaces. Il est important de noter que le secteur médical, en comparaison avec d'autres industries, peut être moins mature en cybersécurité et dispose de budgets plus restreints. C'est pourquoi ces bases revêtent une importance cruciale pour protéger les données sensibles des patients et garantir la continuité des soins médicaux.

COLLABORATION ET PARTAGE : UNE SOLUTION AU DÉFI BUDGÉTAIRE

L'un des défis majeurs auxquels sont confrontés les établissements de santé, en particulier dans le contexte de la cybersécurité, est le manque de ressources financières et humaines. Face à cette réalité, Bart Asnot propose une approche innovante : la collaboration et le partage de certaines fonctions critiques, telles que les CISO ou DPO.

La création de communautés dédiées à la cybersécurité médicale peut également offrir des solutions concrètes. Ensemble, les hôpitaux peuvent renforcer leur posture de sécurité et mieux protéger les données sensibles de leurs patients, tout en optimisant l'utilisation de leurs ressources limitées.

En conclusion, le message essentiel que Bart Asnot nous livre est clair : nous devons avoir confiance en l'innovation. Dans un monde en constante évolution, l'innovation est la clé pour accélérer la transformation, rester compétitif et répondre aux besoins futurs. Cependant, cette confiance en l'innovation doit s'accompagner d'une conscience des risques associés.

Ralentir l'innovation n'est pas la solution, car cela nous laisserait inadaptés aux défis de demain. Au contraire, nous devons investir dans l'innovation tout en nous assurant que cela se fait de la manière la plus sécurisée possible. La cybersécurité ne doit pas être un frein à l'innovation, mais plutôt une composante intégrale de celle-ci. La confiance en l'innovation et la sécurité sont complémentaires et essentielles pour façonner un avenir numérique prospère et sûr.

Proximus

Cybersécurité, le SOCle indispensable

par Antonio Paci

Les hôpitaux, piliers de notre système de santé, sont aujourd'hui confrontés à une pression croissante en matière de cybersécurité. Les menaces numériques planent, mettant en péril la sécurité des données sensibles et la prestation des soins essentiels. Pourtant, au milieu de cette complexité grandissante, il y a de bonnes nouvelles et des solutions prometteuses. Antonio Paci, Senior Solution Consultant Security chez Proximus, nous éclaire sur ces défis, les opportunités et l'importance cruciale d'un Security Operations Center (SOC).

LES MAUVAISES NOUVELLES : VULNÉRABILITÉS ET MENACES CROISSANTES

Le secteur de la santé est devenu de plus en plus vulnérable aux risques cybernétiques en raison de sa dépendance croissante à la technologie pour offrir des soins de qualité. Cette vulnérabilité est exacerbée par plusieurs facteurs. D'abord, de nombreux établissements de santé ont longtemps sous-estimé leur exposition aux menaces numériques. Cependant il est devenu évident que les hôpitaux et les cliniques sont devenus des cibles attrayantes pour les cybercriminels.

L'un des motifs derrière cette tendance est la conviction des pirates informatiques que les établissements de santé sont plus enclins à payer des rançons pour éviter des interruptions dans la prestation de soins essentiels. Les cyberattaques sont de plus en plus sophistiquées, menées par des groupes d'experts dotés de connaissances approfondies, de ressources humaines et financières considérables. Souvent, ces attaques sont déclenchées de manière indirecte, en exploitant des vulnérabilités dans les machines des utilisateurs ou des dispositifs médicaux connectés pour atteindre les serveurs centraux.

L'extension de la surface d'attaque due à la prolifération des machines connectées a rendu les attaques encore plus complexes. De plus, de nombreux travailleurs indépendants fréquentent les établissements de santé, apportant des appareils non contrôlés, ce qui accroît les risques.

Les motivations des pirates sont variées, allant des gains financiers à des motivations géopolitiques. La mise en place de systèmes de protection est devenue une tâche complexe nécessitant une expertise multiple, tandis que les compagnies d'assurance renforcent leurs exigences et leurs primes.

Les conséquences d'une violation de la sécurité dans le secteur de la santé peuvent être dévastatrices, notamment la modification de données médicales, qui peut avoir un impact direct sur la santé des patients. De plus, les attaques par déni de service pourraient avoir des conséquences mortelles pour les patients en perturbant la prestation de soins.

LES BONNES NOUVELLES : RÉSILIENCE ET INNOVATION EN CYBERSÉCURITÉ

Cependant, il y a aussi des aspects positifs à considérer. Les pirates préfèrent souvent cibler des entités moins bien défendues, incitant ainsi les établissements de santé à renforcer leur sécurité. La technologie de cybersécurité est devenue plus efficace, intégrée et accessible, tandis que l'expérience passée a permis d'apprendre des incidents précédents. Le partage de connaissances et d'expérience se développe, renforçant la résilience du secteur.

Les constructeurs développent des solutions spécifiques et automatisées pour anticiper et répondre aux attaques, tandis que la détection précoce des signes d'attaque est devenue plus rapide en temps réel. L'automatisation permet de pallier le manque de ressources humaines, en particulier en dehors des heures de travail. L'offre de produits et de services sur le marché s'est enrichie, couvrant le cycle complet de la cybersécurité. Il est également rassurant de savoir que des experts en cybersécurité sont disponibles pour guider les hôpitaux dans la mise en place d'un SOC. Antonio Paci souligne que Proximus compte plus de 500 professionnels du cyber, prêts à fournir des composants matériels, logiciels, des services en site, dans le cloud, ou mixtes, ainsi que des conseils en matière de cybersécurité.

En fin de compte, bien que les défis liés à la cybersécurité dans le secteur de la santé soient considérables,

il existe des opportunités pour renforcer la résistance de ces établissements et protéger les données sensibles des patients.

LE RÔLE CRUCIAL D'UN SECURITY OPERATIONS CENTER (SOC) DANS LA CYBERSÉCURITÉ HOSPITALIÈRE

Parmi les solutions qui s'offrent aux hôpitaux pour renforcer leur cybersécurité et répondre aux défis croissants auxquels ils sont confrontés, Antonio Paci souligne l'atout majeur que représente un Security Operations Center (SOC) dans le contexte hospitalier.

Un SOC est le cerveau central de la sécurité informatique. Il évolue désormais en Cyber Security Operations Center (CSOC) pour mieux refléter son rôle dans la défense contre les menaces numériques. Concrètement, un SOC est une plateforme informatique qui joue un rôle crucial dans la protection des données sensibles et la prévention des attaques.

Le SOC, dédié au client (la plupart du temps dans le cloud), collecte en continu des données telles que des logs, des traces de fonctionnement provenant de tous les équipements impliqués dans la sécurité. Dans un environnement hospitalier, cela inclut des pare-feu, des relais de messagerie, des serveurs d'authentification forte, mais aussi les équipements et machines.

Le SOC joue un rôle essentiel en structurant, corrélant et archivant les événements qu'il reçoit en continu, 24 heures sur 24 et 7 jours sur 7. C'est en quelque sorte une plateforme Big Data dédiée à la cybersécurité. Il utilise toute cette masse d'informations pour identifier les comportements anormaux, les indicateurs d'attaques potentielles, et les signes de compromission.

Un SOC fonctionne un peu comme un gendarme au bord de la route, observant le trafic en permanence. Lorsqu'il repère quelque chose de suspect, il émet une alerte à ses collègues pour approfondir les contrôles. En cas de détection d'une menace, le SOC réagit automatiquement ou transfère l'alerte à l'équipe appropriée pour une intervention humaine.

La mise en place d'un SOC ne nécessite pas un investissement initial très lourd, mais il est important de noter que son fonctionnement continu génère des coûts récurrents. Les serveurs qui composent le SOC sont actifs en permanence, traitant un volume considérable d'informations, utilisant des automatismes et des technologies d'intelligence artificielle.

La question se pose alors : les hôpitaux devraient-ils se doter d'un SOC ? Selon Antonio Paci, la réponse est un oui catégorique. Même s'il n'y a pas encore d'obligation légale, les hôpitaux gèrent une quantité considérable de données sensibles, soumises au Règlement général sur la protection des données (GDPR), qui exige la conservation de traces pendant au moins 12 mois. Un SOC permet aussi de répondre à cette obligation.

Quant à l'investissement que représente l'installation d'un SOC, il est crucial de comprendre les avantages qu'il apporte en termes de sécurité par rapport aux coûts d'interruption de service et de réputation en cas de crise. Antonio Paci : *« Dans la législation qui entrera en vigueur en 2025, le rôle du directeur de l'hôpital évolue de manière significative, le rendant personnellement responsable de la sécurité des données. Dans le scénario où un hôpital a pris toutes les mesures de sécurité appropriées et est néanmoins victime d'une attaque, l'audit prendra en considération les efforts déployés pour protéger les données, tout comme un automobiliste respectant les limitations de vitesse peut être impliqué dans un accident imprévisible. Cependant, si lors de l'audit, l'hôpital est incapable de fournir des logs ou de démontrer sa conformité aux bonnes pratiques en matière de sécurité, cela pourrait poser des problèmes graves en termes de responsabilité. »*

RHEA Group

Sans une gouvernance des risques, investir dans des outils revient à gaspiller le budget

par Matteo Merialdo

RHEA, une entreprise composée d'environ 900 employés, se distingue par son engagement dans deux secteurs clés : l'espace et la cybersécurité.

Au sein de son équipe de cybersécurité, on trouve deux principaux pôles : l'équipe Services et Opérations, axée sur la prestation de services, et l'équipe Produits et Ingénierie, dirigée par Matteo Merialdo, Business Director, Security Engineering & Products.

Cette entreprise étend son expertise sur divers domaines, de la sécurisation du secteur spatial à la protection des infrastructures critiques, et offre un large éventail de services en cybersécurité. RHEA développe des solutions de sécurité sur mesure pour répondre aux besoins spécifiques de ses clients, s'impliquant également dans des projets majeurs tels que la construction du centre de formation de l'Agence spatiale européenne. Enfin, RHEA collabore avec des hôpitaux à travers l'Europe, en mettant l'accent sur la sécurité dès la conception des dispositifs médicaux, les tests de pénétration et l'évaluation de la sécurité des réseaux hospitaliers, tout en développant des outils sécurisés pour le partage d'informations médicales entre établissements de santé différents.

LA CYBERSÉCURITÉ DANS LES HÔPITAUX : UN DÉFI EUROPÉEN

Dans le contexte des faiblesses de la cybersécurité dans le secteur des soins de santé, Matteo Merialdo s'appuie sur son expérience au niveau européen, dont l'observation d'une attaque majeure qui a frappé un hôpital en Irlande en 2021, pour illustrer de manière frappante les vulnérabilités inhérentes au secteur de la santé en matière de cybersécurité.

À l'époque, le HSE (le système de santé irlandais) était alors engagé dans un projet en partenariat avec RHEA. Si la société n'a pas été impliquée dans la gestion de la crise, elle a toutefois bien perçu les difficultés rencontrées par l'hôpital concerné. Ce partenariat a fourni à l'équipe un accès en temps réel à des informations cruciales sur cette attaque, qui s'est avérée être une attaque par ransomware. Ce type d'attaque consiste à chiffrer les données d'une organisation et à demander une rançon pour leur restitution.

L'attaque en question a débuté à partir d'un équipement provenant d'un fournisseur qui n'était pas soumis à des vérifications régulières. Le ransomware, une fois infiltré, s'est propagé rapidement dans tout le réseau de l'hôpital, provoquant le chaos et l'indisponibilité de données médicales essentielles. L'hôpital irlandais a dû faire face à une période de quatre mois de perturbations.

Face à cette crise majeure, l'hôpital irlandais a dû mettre en place une série de mesures pour atténuer les dommages. Parmi les actions entreprises, citons la séparation des réseaux pour contenir la propagation du logiciel malveillant, l'activation des sauvegardes pour restaurer les données perdues, et un refus catégorique de payer la rançon exigée par les cybercriminels. Ils disposaient de bons informaticiens ayant une expérience en matière de sécurité, mais ils n'avaient pas de SOC, ce qui leur a probablement causé quelques problèmes.

Cette attaque sur l'hôpital irlandais illustre de manière poignante la nécessité d'une cybersécurité robuste dans le secteur de la santé. Les répercussions sur les patients, les opérations médicales et la confiance du public soulignent l'importance cruciale de protéger les systèmes informatiques des établissements de santé.

L'exemple de cette cyberattaque illustre de manière frappante les vulnérabilités inhérentes au secteur de la santé en matière de cybersécurité :

- **Investissements inadéquats :** Bien que certains hôpitaux soient relativement modernes, les établissements de santé européens n'investissent généralement pas suffisamment dans la cybersécurité. Bien qu'il y ait une volonté croissante

d'investir, il y a un manque de politiques claires sur la façon d'allouer ces ressources de manière efficace. Matteo Merialdo souligne que le simple fait d'équiper les hôpitaux d'outils et de technologies de cybersécurité est insuffisant si l'on n'aborde pas la question plus générale de la gouvernance des risques de cybersécurité. Certains hôpitaux ont mis en place une bonne gouvernance des risques, avec notamment des responsables de la sécurité de l'information (CISO) et des mesures de sécurité spécifiques. Cependant, d'autres sous-estiment l'importance de la cybersécurité ou ont du mal à allouer leurs ressources de manière efficace.

- **Facteurs humains :** les facteurs humains, tels que l'utilisation de mots de passe faibles ou visibles à tout un chacun, posent des problèmes de cybersécurité dans les hôpitaux. Les infirmières et les médecins, en raison de leur emploi du temps chargé, peuvent ne pas accorder la priorité à des pratiques de sécurité rigoureuses.

UN SOC COMME SOLUTION ULTIME ? PAS FORCÉMENT.

Matteo Merialdo met en avant la gouvernance des risques comme élément clé de la cybersécurité dans les hôpitaux, insistant sur le fait que la décision de mettre en place un SOC doit découler d'une analyse approfondie des risques spécifiques à chaque établissement. Les hôpitaux plus importants et complexes peuvent en avoir besoin, tandis que les plus petits, avec des activités moins critiques, peuvent s'en passer.

Il est également mentionné que certains hôpitaux peuvent choisir de confier la gestion de leur SOC à des entreprises externes, ce qui peut être rentable et efficace en fonction des besoins et des ressources de l'établissement.

L'importance de ne pas s'appuyer exclusivement sur le personnel informatique interne est soulignée, car une compréhension globale des risques de cybersécurité va au-delà des capacités de ces équipes.

En outre, l'acquisition aveugle d'outils de cybersécurité est déconseillée, car elle peut créer un faux sentiment de sécurité. Le secteur de la santé est considéré comme en retard par rapport à d'autres secteurs en termes de maturité de la cybersécurité, malgré les initiatives européennes visant à améliorer la situation. Cependant, il existe des exemples positifs d'hôpitaux, tels que l'hôpital universitaire Gemelli à Rome, qui ont réussi à progresser grâce à la mise en place de responsables de la sécurité de l'information, de programmes de gouvernance des risques, d'investissements dans la sécurité et de formations.

En conclusion, l'importance cruciale de la cybersécurité dans le secteur médical ne peut être sous-estimée, d'autant plus que les réglementations européennes, notamment la directive sur les besoins en matière de sécurité, imposent des exigences strictes pour la protection des données et des systèmes. Les centres de coordination nationaux, tels que le Centre pour la Cybersécurité Belgique (CCB), jouent un rôle essentiel en élaborant des directives et en fournissant un soutien précieux aux infrastructures critiques, y compris les hôpitaux, dans le renforcement de leur sécurité en ligne.

Cependant, il est crucial de souligner que la conformité aux réglementations ne se limite pas à une simple question de dépenses. Il est impératif de créer un plan stratégique en collaboration avec des experts, des partenaires commerciaux, et les centres nationaux de coordination. Plutôt que d'opter pour une approche réactive consistant à acquérir des outils au cas par cas, il est préférable de concevoir un plan global pour la mise en place de mesures de cybersécurité robustes.

Solvay Business School

Comment bien gérer la cybersécurité des hôpitaux

par le Professeur Georges Ataya

Des hôpitaux belges continuent à être paralysés par des attaques cybercriminelles. Sommes-nous voués à subir ces innombrables attaques ou est-il possible de sortir de cette série noire qui ne cesse de se répéter ? Que devrons-nous faire pour empêcher des incidents évitables ? Et qui devra agir en premier ?

En réponse à cette dernière question, les yeux se tournent directement vers les techniciens du digital, les informaticiens ou les experts en cybersécurité.

La majorité des entreprises engagent de tels experts en interne ou bien demandent à un service externe de régler leurs problèmes de sécurité. Et pourtant, il est très probable que deux différentes entreprises ou hôpitaux gèrent les activités de cybersécurité de la même manière. Plusieurs cadres de références existent et le centre belge de la cybersécurité (CCB) a récemment adopté un standard mondialement connu pour guider les entreprises dans leurs actions.

Mais peu d'organisations prennent le sujet suffisamment au sérieux que pour allouer les budgets adéquats et les responsabilités aux bons endroits.

En ce qui concerne le budget, lorsque la moyenne des entreprises dans le monde dépense 12 % de leur budget informatique pour la protection de leur activité digitale, le secteur de santé alloue en moyenne une douzaine d'employés à la sécurité de l'information (Rapport ENISA 2021). Ce secteur présente la troisième plus haute moyenne de dépense après le secteur bancaire et le secteur de l'énergie.

Mais face à des budgets limités alloués aux hôpitaux dans nos régions, plusieurs institutions souffrent des deux maux suivants :

1. Manque d'attention des directions générales à ce sujet encore considéré comme purement technique et relevant de la responsabilité du responsable informatique.

2. Manque de moyens libérés pour cette activité et manque d'attention des responsables fonctionnels pour prioriser ces dépenses. Il s'agit parfois de consacrer trop que trop peu sur des dépenses moins essentielles (mais plus prisées par les responsables techniques).

Pour pallier ces manques chroniques, il faudra commencer à impliquer les différents niveaux de directions et de gouvernance à ce sujet devenant stratégique. Voici quelques clés de répartition de cette responsabilité.

LE CONSEIL D'ADMINISTRATION

Une bonne gouvernance des entreprises exige une visibilité étendue des risques les plus graves. Or, les comités de direction sont composés le plus fréquemment de juristes, d'experts en conformité et de financiers. **Il est rare qu'un tel casting soit motivé à poser des questions dans des domaines où ils préfèrent garder une certaine pudeur**, pour ne pas dire une réelle ignorance. Je rassure rapidement les lecteurs qu'une telle crainte n'est plus justifiée. Il suffit de poser trois questions simples et compréhensibles par le commun des dirigeants :

1. « Quelle est notre visibilité des risques et quels risques importants n'avons-nous pas encore tenté d'atténuer ? ».

2. « Qui dirige la sécurité de l'information et avons-nous récemment entendu ses doléances et demandes pour des protections additionnelles ? ».

3. « Comment reprendre les opérations normales pour donner suite à un incident ou à une crise ? ».

Comment faire en sorte d'impliquer plus la direction générale dans des décisions en matière de cybersécurité, alors qu'elles sont traditionnellement de la responsabilité de la direction informatique ?

LE COMITÉ DE DIRECTION ET LA DIRECTION GÉNÉRALE

La direction générale devra s'impliquer activement dans des décisions en matière de cybersécurité. C'est en tout cas, traditionnellement, de la responsabilité de la direction informatique, ou encore de l'équipe

de sécurité de l'information, des gestionnaires de risques, des auditeurs, des conseillers externes voire de la police fédérale.

Actuellement, il est rare qu'un dirigeant de département fonctionnel dispose d'un mode d'emploi en cas de crise ou d'incident grave. Ils ne possèdent parfois pas de listes de ce qui peut aller mal. Et pourtant, il suffit de parcourir l'éternelle liste d'incidents (par exemple konbriefing.com qui ne liste pas moins de 3 attaques d'hôpitaux européens du 1er au 9 mars). Il suffit aussi de prendre le rapport annuel de l'agence Européenne ENISA listant **les menaces cybernétiques les plus fréquentes avec un total dépassant 99 000 incidents en 2022**.

Ces menaces ainsi que les incidents qui s'en suivent méritent que les conseils d'administration et les comités de direction amènent leurs membres à identifier ce qui peut aller mal et ce qui faudra réaliser pour l'empêcher, plutôt que d'aller droit les yeux bandés vers une sentence certaine infligée par un inconnu agissant derrière son clavier dans un endroit du globe qui ne sera probablement jamais identifié.

Les responsables fonctionnels devront établir, en connaissance de cause, leurs **plans d'action pour améliorer la sécurité de leurs activités**. C'est en identifiant les éléments vitaux de leurs organisations qu'ils pourront identifier les risques et initier des projets de protection.

Espérer que les protections viendront sous forme de réglementation globale qu'on pourrait commander pour être livré la semaine prochaine, d'un outil ou dispositif informatique supérieur qui nous sauvera par magie, ou bien d'une série de polices et procédures développées par des experts externes est **un piège dans lequel tombent souvent les dirigeants**.

LES RESPONSABLES INFORMATIQUES

À la suite du travail essentiel à réaliser par les responsables métiers dans l'identification des risques à éviter, des indicateurs de détection d'incidents à observer, et des actions à initier en cas de crise, les responsables techniques devront alors être les **gardiens du temple digital de l'entreprise**.

Ils devront s'assurer tous les jours que l'architecture globale, y compris les dispositifs informatiques, le matériel, le logiciel, les actifs dans les nuages (cloud computing) et les données soient adéquatement préservés.

Les projets mis en place par l'équipe d'informaticiens pour pallier les carences existantes et pour améliorer les protections sont souvent sous le radar des dirigeants. Leurs coûts sont minimisés et leurs actions sont confondues avec les projets plus « nobles » car apportant des nouveautés fonctionnelles apparentes.

Parfois, les projets de protection ne sont même pas identifiés, ou ne sont pas prioritaires par rapport aux autres projets plus « présentables ».

LES RESPONSABLES DE LA SÉCURITÉ DE L'INFORMATION

Ils disposent de trois tâches essentielles. La première, que j'appelle « de haut en bas », consiste à gérer les quatre activités fondamentales d'un responsable services de la sécurité d'information : gérer la globalité des activités de sécurité de l'information à travers l'entreprise. Ceci consiste d'une part à mettre en place des projets d'amélioration et de protection sur base des risques et carences identifiés. Et d'autre part s'assurer que toutes les parties concernées soient impliquées pour assurer une protection.

La deuxième, que j'appelle « de bas en haut », consiste à évaluer la situation des protections internes, telles la protection des accès, la sécurité des données, la protection du réseau, la conscientisation des utilisateurs. Or plusieurs entreprises ne disposent même pas de tableaux de bord avec vue sur la qualité et l'état des protections les plus essentielles. Comment agir en personne prudente et responsable dans ces cas ? **Il suffit qu'un chaînon soit faible ou manquant pour fragiliser l'ensemble des protections et gaspiller les investissements déjà réalisés.**

La troisième dimension (que j'appelle « affaires courantes ») correspond aux tâches de conseil et de suivi des projets en cours et des actions de sécurité opérationnelle. Celle-ci occupe parfois la majorité du temps des professionnels de la sécurité de l'information.

CONCLUSION

La médecine a fait de gros progrès depuis le temps de Molière. De même, la gestion de la sécurité de l'information, aussi appelée Cybersécurité, s'est grandement spécialisée. Elle s'est aussi distribuée entre les responsables des domaines à protéger, les responsables des mises en place des protections adéquates et finalement les donneurs d'ordres et décideurs de l'allocation responsable et du suivi des budgets. Une confusion des tâches ou une paresse à un des niveaux de responsabilité ne peut que faciliter les tâches des attaquants.

Thales

Les trois piliers de la cybersécurité médicale : les recommandations de Thales pour un secteur en évolution.

par Johann Alessandroni

Thales est un acteur de premier plan en cybersécurité, grâce à une large empreinte internationale offrant une expertise complète qui couvre tous les aspects de la sécurité informatique. Cette approche globale lui permet de relever tous les défis de la cybersécurité, qu'ils touchent à la stratégie, à la gouvernance ou aux aspects techniques et opérationnels.

Thales intervient dans des domaines complexes, que ce soit au niveau des systèmes industriels ou informatiques. L'entreprise possède l'expertise nécessaire pour mettre en place des niveaux de sécurité appropriés, en utilisant des solutions éprouvées ou sur mesure. Elle propose également une large gamme de solutions et de produits qu'elle déploie, maintient et surveille pour ses clients.

Dans le domaine de la santé, Thales se distingue par sa capacité à comprendre les enjeux de sécurité liés à la gestion de données hautement confidentielles, telles que les informations médicales des patients. Thales peut non seulement identifier les mesures de sécurité nécessaires, mais aussi les mettre en œuvre de manière complète, de la conception à l'implémentation, avec un suivi continu. Un élément essentiel dans le secteur de la santé est la gestion de la sécurité des équipements médicaux tels que les scanners et les IRM. Thales offre une expertise pointue pour relever ces défis spécifiques, garantissant la sécurité des opérations médicales critiques.

Forte de sa connaissance approfondie des enjeux de cybersécurité, Thales a identifié trois axes essentiels en matière de cybersécurité pour le milieu médical :

1. ADAPTATION DE LA STRATÉGIE DE SÉCURITÉ AU CONTEXTE DE LA SANTÉ :

Face aux risques spécifiques inhérents au secteur de la santé, ainsi qu'aux conséquences potentiellement dévastatrices, notamment sur la vie des individus, il est impératif que les organisations opérant dans le domaine de la santé ajustent leur stratégie de sécurité. Cette adaptation doit prendre en considération les aspects particuliers de ce secteur afin d'identifier les priorités en matière de gestion des risques. Une approche basée sur l'évaluation des risques prend tout son sens pour mettre en évidence de manière explicite les conséquences qui résulteraient de l'ignorance de certains risques. Par exemple, la nature sensible des informations traitées pour les patients impose une sécurité ininterrompue à tous les niveaux, du début à la fin des processus, qu'ils soient numériques ou physiques. De plus, cette approche doit englober l'ensemble des acteurs de l'écosystème de l'organisation, en vue d'évaluer et de surveiller en permanence le niveau de sécurité des tiers impliqués.

Dans de nombreux cas, la priorité dans le secteur de la santé est d'assurer le bon déroulement des opérations médicales, en veillant à disposer du personnel nécessaire pour fournir des soins de qualité. Par conséquent, la sécurité des systèmes peut parfois être reléguée au second plan, avec l'idée que les systèmes doivent d'abord fonctionner avant d'être sécurisés. Toutefois, cette perspective a évolué au fil des années, notamment à la lumière d'incidents de cybersécurité graves survenus dans des hôpitaux en France et en Belgique. Cependant, il subsiste souvent un manque de ressources, notamment au sein des institutions publiques, pour mettre en place des mesures de sécurité robustes. Les organisations du secteur de la santé font souvent de leur mieux avec les budgets limités dont elles disposent pour relever ces défis complexes.

2. CYBER RÉSILIENCE POUR ASSURER LA CONTINUITÉ DES ACTIVITÉS :

Compte tenu des éventuelles conséquences d'une interruption des systèmes d'information sur les activités quotidiennes, il est désormais essentiel de se préparer au pire et de garantir la résilience des opérations, y compris en ce qui concerne les enjeux de cybersécurité. La garantie de cette résilience passe par une prise en compte intégrale de la continuité

des activités et de la reprise des opérations, en considérant tous les aspects de l'organisation, qu'ils soient opérationnels ou technologiques. Par conséquent, il est impératif d'intégrer les éléments de complexité liés aux infrastructures informatiques (IT) et opérationnelles (OT) pour clarifier les dépendances et les priorités en ce qui concerne les activités critiques. La gestion des crises liées à la cybersécurité, qu'il s'agisse de la structure organisationnelle, de la relation avec les groupes d'attaquants, ou de la communication avec l'ensemble des parties prenantes, requiert une préparation minutieuse, garantissant que chaque intervenant soit conscient de ses responsabilités en période de crise et que l'organisation dispose des ressources logistiques (salles, équipement) et technologiques (canal de communication de secours) nécessaires. Enfin, le dispositif de redondance du système d'information doit intégrer des mécanismes de sauvegarde appropriés, en particulier pour les systèmes critiques, en envisageant notamment des sauvegardes hors ligne.

3. ASSURER LES FONDATIONS DE LA SÉCURITÉ :

Afin de garantir un niveau de protection suffisant, il est impératif de prendre en compte les mesures fondamentales de cybersécurité, en particulier pour les composants exposés de l'organisation. Cette vigilance est essentielle pour se prémunir contre les techniques d'attaque les plus courantes. Cela commence par la nécessité d'acquérir une visibilité totale sur les actifs des systèmes d'information, en particulier sur ceux qui soutiennent les activités critiques ou qui sont les plus exposés aux risques. Cette visibilité accrue permettra d'identifier et de mettre en œuvre des mesures de protection appropriées, notamment la configuration et les règles de durcissement des systèmes, ainsi que la mise en place de solutions anti-malware et des procédures régulières d'identification des vulnérabilités. De plus, il est primordial de disposer de mécanismes de détection d'anomalies pour réagir promptement en cas d'activité suspecte.

Les fondamentaux de la cybersécurité englobent également une gestion efficace des accès logiques et physiques. L'authentification multifacteur, adaptée à l'exposition et à la sensibilité des ressources auxquelles on accède, constitue une mesure essentielle. Une attention particulière doit être portée aux comptes à privilège, en réduisant leur nombre et en exerçant un contrôle strict sur leur utilisation.

Enfin, il est crucial de reconnaître que le facteur humain reste une composante essentielle de la sécurité au sein de toute organisation, y compris dans le secteur de la santé. Les employés sont en première ligne pour respecter les règles en matière de sécurité de l'information et pour maintenir un niveau de vigilance élevé au quotidien. Les efforts pour promouvoir et mettre en œuvre une culture de la sécurité doivent être constants afin de faire face de manière adéquate aux risques liés au facteur humain.

Dans de nombreuses organisations, y compris celles du secteur de la santé, il est courant de constater une approche où l'on mettrait trois cadenas sur une porte, tandis qu'une fenêtre à proximité resterait grande ouverte. Cette analogie met en évidence l'importance de s'attaquer aux fondations de la sécurité. Les fondations, telles que la sensibilisation des employés, la connaissance du parc informatique et la gestion des accès, sont souvent négligées, même dans le domaine de la santé. Pourtant, elles sont cruciales pour établir une base solide en matière de cybersécurité.

Pour Johann Alessandroni, Team Leader Information Security Governance dans la division cybersécurité de Thales qui a intégré Excellium, les trois axes stratégiques présentés dans cet article représentent les principaux piliers pour renforcer la cybersécurité dans le secteur médical. Ces recommandations sont le fruit de l'expertise approfondie de Thales et de sa compréhension des enjeux critiques liés à la gestion des données sensibles des patients. En mettant en œuvre ces principes fondamentaux, les organisations du secteur médical peuvent renforcer leur posture de sécurité, prévenir les incidents de cybersécurité, et garantir la protection des données vitales pour la santé des individus. Face à l'évolution constante des menaces, ces piliers demeurent essentiels pour assurer la sécurité et la continuité des opérations médicales dans un environnement de plus en plus numérique et interconnecté.

Université Catholique de Louvain (UCL)

Transformer la cybersécurité médicale en opportunité économique pour la Wallonie

par le Professeur Axel Legay

La cybersécurité est aujourd'hui l'un des domaines les plus cruciaux de l'informatique, et son importance ne cesse de croître à mesure que notre monde devient de plus en plus connecté. Dans le cadre de discussions sur la convergence de la cybersécurité et de la santé numérique, Axel Legay, professeur de Cybersécurité et Software Engineering à l'UCL, membre du Conseil du numérique et de Digital Minds et du Conseil de la politique scientifique, ainsi que co-créateur de *CyberWal by Digital Wallonia*, partage ses réflexions sur les défis croissants et les opportunités prometteuses qui se dessinent dans le secteur médical en Wallonie.

CYBERSÉCURITÉ : FORMER LA PROCHAINE GÉNÉRATION D'EXPERTS

À l'UCL, la formation en cybersécurité est intégrée dans divers cursus, notamment ceux liés à l'ingénierie informatique. Une option en cybersécurité est proposée aux étudiants, comprenant six cours essentiels. Ces cours sont conçus pour former les étudiants à plusieurs aspects de la cybersécurité, de la protection des infrastructures à la sécurisation des codes, en passant par les bonnes pratiques pour la gestion sécurisée des données.

Il existe également à l'UCLouvain, dans d'autres contextes, des cours de Health Data où les étudiants apprennent à manipuler et à analyser des données médicales, à prédire des maladies et à proposer des traitements. Pendant longtemps, la cybersécurité et la gestion des données médicales étaient considérées comme deux axes distincts. La cybersécurité n'était pas vue comme quelque chose d'important, allant jusqu'à être considérée comme un coût inutile. Cependant, cette perception évolue rapidement. Les coûts des attaques étant devenus largement supérieurs aux coûts des défenses, de plus en plus de professionnels de la santé comprennent maintenant que la cybersécurité est indispensable pour protéger les données médicales sensibles.

Cette fusion entre la cybersécurité et la gestion des données médicales offre aux étudiants un bagage de compétences précieux. La demande de spécialistes capables de marier ces deux domaines, la santé et la cybersécurité est en constante augmentation. Les étudiants qui choisissent de se spécialiser dans la gestion des données de santé sont de plus en plus conscients de l'importance de la cybersécurité pour protéger ces données contre les menaces en ligne.

LA CYBERSÉCURITÉ DANS LE SECTEUR MÉDICAL EN WALLONIE : ENTRE DÉFIS CROISSANTS ET PRÉPARATION À NIS 2

En Wallonie, comme ailleurs, le secteur de la cybersécurité est devenu un acteur clé dans la transformation des entreprises, mais il occupe une place particulièrement importante dans le secteur médical. Les récents événements en Belgique, en Wallonie et en France ont mis en lumière une demande croissante pour renforcer la cybersécurité dans ce domaine, d'autant plus que les hôpitaux connaissent une digitalisation sans précédent.

Les hôpitaux sont désormais confrontés à la nécessité de collaborer et de partager électroniquement leurs dossiers avec des prestataires externes, le tout en garantissant la sécurité de ces échanges. Cette transition numérique les expose à un large éventail de menaces cybernétiques. Conscients que tous les acteurs ne sont pas au même niveau de préparation, ils comprennent l'importance d'avoir en interne des experts compétents en cybersécurité ou, au minimum, des employés sensibilisés à ces problématiques.

L'arrivée imminente de NIS 2 (Directive sur la sécurité des réseaux et des systèmes d'information) renforce encore davantage l'urgence de la situation. Les entreprises et les institutions qui ne parviennent pas à se conformer à ces nouvelles réglementations pourraient faire face à des sanctions financières et à des interdictions de fournir des services. Cette perspective pousse le secteur médical à se prépa-

rer activement à répondre à ces exigences. Dans ce contexte, il est important de faire la distinction entre les hôpitaux publics et les entreprises privées du secteur médical, tous ne démarrent pas avec le même bagage ni avec la même vision.

LES DÉFIS BUDGÉTAIRES DE LA CYBERSÉCURITÉ DANS LE SECTEUR DE LA SANTÉ

La gestion des budgets constitue un élément clé dans l'ensemble complexe de défis liés à la cybersécurité. Les hôpitaux, en particulier, fonctionnent avec des budgets souvent limités, mais la nécessité de garantir la sécurité numérique n'en est pas moins cruciale.

La digitalisation des hôpitaux, bien qu'elle ait été encouragée par des financements gouvernementaux, a parfois laissé peu de ressources pour la cybersécurité. Heureusement, le ministre Van den Brouck a alloué un budget récurrent pour renforcer la cybersécurité dans ces établissements de santé. Les hôpitaux sont enthousiastes à l'idée d'utiliser ces fonds, mais ils se heurtent à un obstacle de taille : le recrutement de personnel compétent.

L'un des problèmes majeurs est la difficulté de reconvertir le personnel existant pour répondre aux besoins de cybersécurité. Souvent, les employés sont déjà chargés de multiples responsabilités, et il n'est pas réaliste de leur demander d'ajouter la cybersécurité à leur liste de tâches. La solution réside donc dans le recrutement de nouvelles personnes ayant les compétences nécessaires.

Dans le secteur public, cette transition peut prendre du temps, mais il est encourageant de constater une volonté croissante de le faire.

Les enjeux sont différents dans le secteur privé. Les entreprises privées doivent non seulement se soucier de la sécurité, mais également de la rentabilité. La cybersécurité doit être perçue comme une plus-value, à la fois en termes de protection des données et de réputation de l'entreprise. Cela nécessite un équilibre délicat entre l'investissement dans la cybersécurité et la rentabilité de l'entreprise.

LES HÔPITAUX ET LA CYBERSÉCURITÉ : PRÉPARATION À L'INCONNU

Lorsque l'on aborde la question de la cybersécurité, il est essentiel de comprendre que, mathématiquement parlant, il est impossible d'être totalement prêt à faire face à toutes les menaces. Les attaquants sont imprévisibles, et il est donc difficile de prévoir toutes leurs actions. Ainsi, la véritable question est de savoir si les hôpitaux auront les moyens nécessaires pour décourager les pirates et réagir efficacement en cas d'attaque.

La réponse à cette question est complexe, mais il est certain que des mesures peuvent être prises pour renforcer la posture de cybersécurité des hôpitaux. L'objectif est de mettre en place des défenses solides pour dissuader les pirates et de disposer des ressources adéquates pour réagir rapidement et correctement en cas d'incident.

L'un des défis auxquels le secteur de la santé est confronté est de savoir comment réagir en cas d'attaque. Actuellement, de nombreuses institutions médicales se demandent : « Qu'est-ce qu'on fait ? ». L'une des raisons de cette incertitude réside dans le manque de connaissance du personnel en matière de cybersécurité et de son propre parc informatique.

La formation en cybersécurité est tout aussi importante que la mise en place de défenses techniques. Par exemple, il y a souvent une confusion entre les sauvegardes (backups) et la synchronisation avec le cloud. Le manque de compréhension de ces concepts peut entraîner la perte de données critiques en cas d'attaque.

Une autre considération importante est la nécessité de prévenir les autorités en cas d'incident de cybersécurité. Bien que les hôpitaux aient tendance à bien gérer cette étape, il est essentiel de signaler les attaques, même si l'on sait que les autorités ne pourront peut-être pas agir immédiatement. Ne pas porter plainte peut entraîner la perte de droits essentiels.

Enfin, il est crucial de sensibiliser la direction de l'hôpital à l'importance de la cybersécurité. Parfois, les employés sont disposés à suivre des formations et à prendre des mesures pour renforcer la sécurité, mais cela doit être soutenu par un engagement de la direction.

UN ŒIL SUR DEMAIN

En regardant vers l'avenir, il est clair que de nouvelles complexités émergent à mesure que la technologie médicale évolue.

Nous entrons dans une ère où de plus en plus de dispositifs médicaux sont directement implantés chez les patients. Des pacemakers aux pompes à insuline, ces outils deviennent de plus en plus sophistiqués. Cependant, cette sophistication accrue les rend également vulnérables aux attaques cybernétiques. Imaginez un pirate prenant le contrôle à distance du pacemaker d'un patient, une menace réelle qui nécessite des mesures de sécurité renforcées.

De plus, l'avenir de la médecine pourrait voir une augmentation de la télémédecine et des opérations à distance. La formation d'un chirurgien spécialisé est coûteuse. À l'avenir, il pourrait devenir plus courant de réaliser des opérations à distance grâce à des robots chirurgicaux contrôlés par des experts. Cependant, cela ouvre également la porte à des risques de cyberattaques visant à perturber ou détourner ces procédures.

Un autre développement potentiellement révolutionnaire est la livraison d'organes par drones, une technologie testée aux États-Unis. Cette innovation ne vient pas sans risques, car les drones peuvent être facilement piratés, mettant en danger la vie de ceux qui attendent des transplantations.

SAISIR L'OPPORTUNITÉ DE L'INNOVATION EN CYBERSÉCURITÉ

À la lumière de ces discussions sur la cybersécurité dans le secteur médical en Wallonie, une conclusion s'impose : l'innovation et la sécurité vont de pair pour façonner l'avenir de la santé numérique. C'est précisément l'opinion et le message qu'Axel Legay souhaite faire passer.

Il est clair que la Wallonie, comme de nombreuses autres régions, doit adopter une politique structurelle d'innovation. Il est essentiel de ne pas simplement sauter d'un sujet à l'autre, mais de choisir nos combats avec discernement et de les mener de manière cohérente à long terme. Cette approche stratégique ne profitera pas seulement à la cybersécurité, mais elle peut également générer des retours financiers significatifs.

Les jeunes talents doivent être encouragés à embrasser des domaines tels que NIS 2 et à comprendre que la cybersécurité n'est pas simplement une affaire de geeks, mais une discipline sérieuse avec des règles et des enjeux cruciaux. Avec la croissance rapide de la technologie médicale en Wallonie, il existe une opportunité exceptionnelle de créer de nombreux emplois dans le domaine de la cybersécurité. Le secteur éducatif de la Wallonie est déjà parmi les plus subsidiés au monde, ce qui place la région à la pointe de l'innovation.

Pour prospérer dans ce domaine, il est impératif que les jeunes entrepreneurs puissent créer des start-ups et devenir des certificateurs. Cette démarche favorisera la création de richesse pour la Wallonie et renforcera la sécurité numérique dans le secteur médical.

En fin de compte, la cybersécurité ne peut pas être négligée, et la Wallonie a l'occasion de se distinguer en tant que pionnière de la sécurité dans le domaine médical, créant ainsi un avenir plus sûr et plus prospère pour tous. La clé réside dans l'innovation, la formation et la détermination à relever les défis de la cyber-ère qui s'annonce.

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