Hôpitaux intelligents : le défi de la sécurité informatique

Si la numérisation offre d'énormes opportunités, elle génère de nouveaux défis dans l'écosystème des soins de santé. Si les DME (dossiers médicaux électroniques) bénéficient aux patients comme aux praticiens, le contrôle de la confidentialité et de la sécurité des données médicales devient primordial. Le but est d'améliorer la sécurité des informations et la résilience hospitalière pour prévenir les perturbations provoquées par des composants "intelligents" qui pourraient avoir un impact plus important sur la sécurité des patients.

La numérisation est en plein essor grâce aux dernières technologies qui interconnectent tout : les patients, les soignants, les cabinets médicaux, les appareils à usage médical. En France, le « Dossier médical partagé » (DMP), est déjà bien avancé, avec 3 millions de dossiers ouverts en 2018 et un taux actuel de plus de 200 000 DMP ouverts chaque semaine. L’objectif : améliorer le suivi du patient, éviter les examens en double et mieux prendre en compte d’éventuelles incompatibilités des médicaments prescrits. Au-delà des

avantages de facilité d'utilisation et l'amélioration de l'expérience vécue, le dossier médical électronique vise à accroître la confiance tout en offrant un service confidentiel à accès contrôlé.

Cybersécurité : une préoccupation croissante

Les hôpitaux « intelligents » sont attrayants pour les pirates informatiques et les incidents de sécurité sont en constante augmentation. Le secteur de la Santé est reconnu comme étant le plus vulnérable aux cyberattaques, en raison de la grande valeur de ses données sensibles. Il est la cible idéale des attaques par ransomware ou « logiciels de rançon ». Le secteur doit être mieux armé pour détecter rapidement les cyberattaques et les déjouer.

Malgré la menace croissante, les hôpitaux restent insuffisamment protégés contre les cyberattaques. Beaucoup sont soumis à une énorme pression financière et ont du mal à se montrer innovants au sein d'une infrastructure vieillissante. Dans cette optique, le gouvernement français a lancé une politique nationale des systèmes d'information hospitaliers intitulée « Programme hôpital numérique » pour aider les établissements de santé dans leur transformation numérique, en fixant un certain nombre de conditions préalables pour la consolidation de leurs technologies de l'information et de la communication.

L'utilisation croissante d'Internet et des applications web offre aux pirates de nouvelles possibilités d'attaque. Ces applications rendent la communication entre les patients et les praticiens plus souple et améliorent ainsi les services aux malades. Cependant, le nombre d'attaques ne cessant de croître, les prestataires de soins de santé doivent sécuriser davantage de dispositifs médicaux connectés. La majorité des cyberattaques visent des applications web et les cybercriminels continuent d'exploiter ce canal sans relâche. En effet, les applications sont faciles à pirater. Le web, en particulier le protocole HTTP (même le HTTPS, un peu plus sûr), n'ont pas été conçus pour les applications complexes d'aujourd'hui. Par conséquent, une planification de la sécurité doit être intégrée dans les nouvelles offres de produits et de services afin d'éviter une catastrophe.

Les bases de données sont les cibles les plus visées, car elles contiennent d'énormes quantités de données personnelles sous une forme concentrée. Ainsi, concernant le stockage dans les services en cloud, les utilisateurs et les administrateurs ne sont pas les seuls à pouvoir accéder aux données. Les fournisseurs de services cloud pourraient également y avoir accès, si ces données sont stockées sans protection et sans cryptage. Si des cybercriminels parviennent à accéder à ces données, les patients et les hôpitaux peuvent faire

l’objet d’un chantage direct de leur part. Sans parler de l’implication du CLOUD Act, qui, depuis mars 2018, peut obliger tout fournisseur soumis au droit américain, à donner accès aux données dans le cadre d’une enquête, à la demande d’une autorité judiciaire américaine.

Un retard en matière de cybersécurité malgré les exigences légales

La protection des données relatives à la santé est strictement réglementée. Le Règlement Général Européen sur la Protection des Données (RGPD/GDPR) impose le consentement actif de tout patient résidant dans l’UE. En outre, l’article 17 du RGPD stipule le droit à l’oubli, en vertu duquel tout patient résidant dans l’UE peut demander à toute institution contrôlant et stockant ses données d’effacer celles-ci.

Désormais, le certificat HDS est le garant de la sécurité des données de santé. Avec ce label, 6 activités sont exigées par e-sante.gouv. Toutefois, il faut rester prudent. En effet, chaque semaine un nouvel acteur du Cloud se gargarise d’avoir obtenu le précieux sésame. Certains établissements ayant entre 1 et 5 activités se présentent comme étant « HDS », ce qui est une erreur de langage. On constate que 98 hébergeurs s’annoncent officiellement comme hébergeur HDS, alors que seuls 61 sont officiellement approuvés par e-sante.gouv en 2019.

Les 6 niveaux d’activités pour qu’un hébergeur puisse être officiellement certifié :

1. La mise à disposition et le maintien en condition opérationnelle des sites physiques permettant d’héberger l’infrastructure matérielle du système d’information utilisé pour le traitement des données de santé ;

2. La mise à disposition et le maintien en condition opérationnelle de l’infrastructure matérielle du système d’information utilisé pour le traitement de données de santé ;

3. La mise à disposition et le maintien en condition opérationnelle de la plateforme d’hébergement d’applications du système d’information ;

4. La mise à disposition et le maintien en condition opérationnelle de l’infrastructure virtuelle du système d’information utilisé pour le traitement des données de santé ;

5. L’administration et l’exploitation du système d’information contenant les données de santé ;

6. La sauvegarde des données de santé.

Cet agrément permet à l'écosystème médical de s'assurer d'une alternative technologique et économique reposant sur des infrastructures reconnues par son niveau de haute sécurité. De plus, cela assure une certaine interopérabilité pour permettre d'échanger entre différents établissements de l'écosystème de santé.

Seul souci persistant : la souveraineté. Malheureusement, elle n'est pas encore une prioritaire dans les choix des établissements pour faire une sélection. L'hébergeur, le Cloud Act ou encore le Patriot Act n'ont qu'un impact infime dans les choix des RSSI. La souveraineté doit être un des éléments clés pour obtenir la certification HDS sur le sol européen et ainsi avoir une garantie totale de la confidentialité et de l'intégrité des données de santé.

Les prestataires de soins de santé (y compris les hôpitaux et les cliniques privées) ont été identifiés comme « opérateurs de services essentiels » (ou OSE) dans le cadre de la directive NIS, ce qui les oblige à se conformer à un ensemble d'obligations en matière de sécurité des réseaux et des systèmes d'information et de notification des incidents. La directive NIS est le premier texte législatif européen sur la cybersécurité qui prévoit des mesures juridiques pour renforcer le niveau général de cybersécurité dans l'UE, dont la situation des infrastructures de soins de santé est considérée comme « critique » dans tous les États membres.

Une cyberattaque dans le secteur de la santé peut avoir des effets dévastateurs. Sur cette base, les prestataires de soins doivent acquérir et mettre en œuvre des technologies de sécurité appropriées. Celles-ci doivent provenir de fournisseurs certifiés qui doivent utiliser de nouvelles approches de sécurité dans la conception de leurs produits pour stopper les attaques contre lesquelles les solutions classiques se révèlent impuissantes.

Mesures de sécurité appropriées

Les applications web peuvent être protégées via un « pare-feu applicatif » (Web Application Firewall ou WAF). Un WAF empêche les applications web de devenir une passerelle pour logiciels malveillants, en analysant les échanges de données entre les dispositifs terminaux et les serveurs web. Il vérifie toutes les demandes entrantes adressées aux serveurs web ainsi que les réponses. Dès que certains contenus sont reconnus suspects d'être visités par un logiciel malveillant, le WAF en empêche l'accès. De cette façon, les hôpitaux sont protégés et n'ont pas à craindre d'attaques sur les applications web.

Lors du stockage de données dans un cloud, une solution souveraine est le type d'hébergement le plus adapté pour les protéger. Au-delà de votre propre

réseau d’entreprise, un pare-feu réseau dans le cloud est sans effet. Les solutions de sécurité informatique pour cloud doivent être en mesure de protéger les données contre l’accès par des tiers non autorisés, quel que soit l’endroit où elles sont stockées. Cela peut être mis en œuvre par une approche de sécurité centrée sur les données : celles-ci sont cryptées, fragmentées et stockées d’une manière conforme à la réglementation. Cette solution garantit que les données sont stockées de manière configurable, par exemple dans un centre de données européen, même si elles sont virtualisées et disponibles dans le cloud. Quel que soit l’endroit où un attaquant accède à ces données, il ne peut plus leur causer de dommages. Ce type de stockage est sûr, mais il est conforme aux exigences strictes de protection des données et de sécurité du RGPD/GDPR. Grâce à ces mesures, les établissements de santé peuvent se protéger contre les dangers qui menacent leur infrastructure informatique.

Stéphane de Saint Albin est vice-président de la division Application & Cloud Security de Rohde & Schwarz Cybersecurity

---

Article écrit par STÉPHANE DE SAINT ALBIN