KHIAL Omar
LAFFONT Léo

La sécurité informatique dans les hôpitaux

Introduction

Les budgets alloués à la santé publique ont connu ces dernières années une baisse significative, impactant par conséquent la sécurité informatique dans les hôpitaux. En effet, cette dernière est victime d'un manque de moyens et d'investissements, alors qu'elle constitue un enjeu crucial pour la confidentialité et la protection des données de santé. Les hôpitaux sont des cibles de choix pour les cyberattaques, qui peuvent non seulement compromettre la sécurité des systèmes informatiques, mais également mettre en danger la vie des patients. Dans ce contexte, il est indispensable de comprendre les enjeux liés à la sécurité informatique dans les hôpitaux, et de réfléchir aux moyens de la renforcer malgré les contraintes budgétaires.

Nous sommes en droit de nous demander comment garantir la sécurité des systèmes informatiques dans les hôpitaux malgré les contraintes budgétaires, pour protéger les données de santé et assurer la qualité des soins.

Pour répondre à cette question, nous aborderons dans un premier temps les menaces qui pèsent sur la sécurité informatique des hôpitaux, avant de présenter les différents outils de protection et les bonnes pratiques à mettre en place pour renforcer la sécurité informatique. Nous analyserons également les initiatives et les réglementations mises en place, avant de conclure sur les défis et les perspectives pour la sécurité informatique dans les hôpitaux.

I. Les menaces informatiques pesant sur la sécurité des hôpitaux

A. Présentation des différents types d'attaques informatiques

- Récupération de rançons : l'un des objectifs les plus courants des cyberattaques contre les hôpitaux est de récupérer des rançons. Les cybercriminels peuvent utiliser des ransomwares pour chiffrer les données de l'hôpital et exiger une rançon pour les déchiffrer. Les hôpitaux peuvent être particulièrement vulnérables à ce type d'attaque car ils ont besoin d'accéder rapidement aux données des patients pour assurer la continuité des soins.

- Vol de données : Les données médicales des patients peuvent être très précieuses pour les cybercriminels, qui peuvent les utiliser pour des activités malveillantes telles que l'usurpation d'identité, le phishing ou la fraude à l'assurance. Les cyberattaques peuvent donc viser à voler ces données pour les vendre sur le marché noir.

- Espionnage industriel : Les hôpitaux peuvent être ciblés par des attaquants cherchant à obtenir des informations sur des recherches médicales ou des développements technologiques. Les données sensibles concernant les projets de recherche peuvent être utilisées par des concurrents pour obtenir un avantage concurrentiel.

- Activisme : Les cyberattaques peuvent également être menées par des groupes activistes qui cherchent à perturber les opérations de l'hôpital pour faire passer un message ou pour protester contre une politique ou une pratique en particulier.

B. Exemples d'attaques informatiques dans le secteur de la santé

"Nous sommes revenus au papier et au stylo" car "tout est informatisé à l'hôpital", voici ce qu'à prononcé un membre du centre hospitalier de Dax dans les Landes lors d'une attaque ransomware visant l'établissement.

"Cette attaque a mis hors service la totalité de notre système d'information par cryptage des données. Les données n'ont pas été volées, elles sont toujours sur nos serveurs, mais elles sont cryptées et donc ne sont plus accessibles"

Malgré l'abus de langage utilisé à la place du mot "chiffrées", à la lecture des témoignages on comprend que les attaquants ont bloqué l'accès aux données du système d'information de l'hôpital. Ce que la directrice adjointe de l'hôpital ne prend pas en compte est le fait que les données ont pu être copiées, même si les informations sont toujours sur les serveurs de l'hôpital, cela ne veut donc pas dire qu'elles n'ont pas été volées.

Le cas de l'hôpital de Dax n'est pas isolé, on peut par exemple parler du CHU de Rouen ou de celui d'Albertville-Moûtiers qui ont vécu le même sort avec une différence notable puisqu'il s'agit également de centres universitaires.

On peut donc rapidement comprendre les motivations des attaquants lorsque les établissements disposent de recherches médicales qui pourraient intéresser d'autres puissances mondiales. La valeurs de ces recherches sur le marché noir étant très interessantes pour ces cybercriminels.

C. Conséquences de ces attaques pour les hôpitaux et les patients

Les cyberattaques peuvent avoir de graves conséquences sur les soins de santé, notamment la perturbation des systèmes informatiques, la perte de données, la divulgation d'informations personnelles, la modification de données médicales, l'interruption des opérations de l'hôpital, etc.

Les données personnelles peuvent être utilisées pour du phishing à cause des adresses email stockées. Les données compromettantes, telles que des images intimes, peuvent amener les attaquant à effectuer du chantage aux patients. Les données peuvent également être utilisées pour de l'usurpation d'identité amenant à l'ouverture de comptes bancaires au nom d'une victime ou de la fraude à l'assurance grâce aux dossiers médicaux et aux numéros de sécurités sociales enregistrés.

Dans le cas d'une attaque par ransomware, les cybercriminels peuvent chiffrer les données sensibles et exiger une rançon pour les déchiffrer. Cela peut entraîner une perte de temps et d'argent pour les hôpitaux, qui sont souvent contraints de payer la rançon pour récupérer leurs données.

Les cyberattaques peuvent également perturber les soins de santé, ce qui peut avoir des conséquences graves sur la santé des patients. Par exemple, une attaque sur le système informatique d'un hôpital peut empêcher l'accès aux dossiers médicaux, les médecins ne seront pas en mesure de connaître les antécédents médicaux et les allergies des patients, ce qui peut entraîner des erreurs médicales et des soins inappropriés.

Au vu des dangers évoqués précédemment, il est essentiel que les établissements de santé prennent des mesures appropriées pour se protéger contre ces menaces, notamment en mettant en place des stratégies de sécurité robustes et en formant leur personnel à la sécurité informatique.

II. Les moyens de protection et de prévention de la sécurité informatique dans les hôpitaux

A. Les différents outils de protection informatique

Afin de répondre à la problématique de la sécurité informatique dans les hôpitaux, il est important de présenter les différents outils de protection qui peuvent être mis en place. Nous allons ainsi examiner plusieurs solutions qui peuvent permettre de renforcer la sécurité des systèmes d'information au sein des établissements de santé.

1. Les pare-feux

Les pare-feux (firewalls) sont des dispositifs de sécurité qui permettent de filtrer les données qui entrent et sortent du réseau informatique de l'hôpital. Ils peuvent être installés soit au niveau du réseau, soit sur chaque poste de travail. Les pare-feux peuvent ainsi bloquer les accès non autorisés aux données, en fonction de règles prédéfinies, et permettent également de détecter les intrusions.

2. Les antivirus

Les antivirus sont des logiciels qui permettent de détecter et de supprimer les virus, les malwares et les autres types de logiciels malveillants. Ils sont essentiels pour protéger les ordinateurs et les serveurs contre les attaques informatiques. Les antivirus doivent être régulièrement mis à jour pour garantir leur efficacité contre les nouvelles menaces.

3. Les outils de chiffrement

Les outils de chiffrement permettent de sécuriser les données en les transformant sous une forme codée, qui ne peut être lue que par des personnes autorisées. Les données médicales peuvent ainsi être chiffrées pour garantir leur confidentialité, même en cas de vol ou de fuite. Il existe différents outils de chiffrement, tels que les algorithmes de chiffrement asymétrique ou symétrique, qui peuvent être utilisés en fonction des besoins de sécurité.

4. Les systèmes de détection d'intrusion

Les systèmes de détection d'intrusion (IDS) sont des outils de sécurité qui permettent de détecter les activités suspectes ou malveillantes sur le réseau informatique de l'hôpital. Les IDS peuvent ainsi alerter les administrateurs en cas de tentative d'intrusion ou de violation de la sécurité des systèmes.

B. Les initiatives et les réglementations mises en place pour renforcer la sécurité informatique dans les hôpitaux

La certification Hébergeur de Données de Santé (HDS) a été mise en place en 2018 pour garantir la sécurité des données de santé hébergées par des tiers. Les hébergeurs de données de santé doivent ainsi répondre à un certain nombre de critères de sécurité pour obtenir cette certification, tels que la mise en place de mesures de sécurité physiques et logiques, la formation des personnels à la sécurité informatique et la mise en place de sauvegardes régulières des données.

La directive NIS, et aujourd'hui son extension NIS 2, vise à promouvoir la coopération entre les différents établissements de tout type de secteur au sein de l'Union Européenne. Comme vous l'aurez compris, cette directive s'applique également aux hôpitaux et permet de prévenir des attaques globalisées basées sur une même faille.

III. Les défis et les perspectives pour la sécurité informatique dans les hôpitaux

« Les RSSI ont une très bonne vision des trous de sécurité de leurs systèmes d'information, mais nous n'avons pas forcément les moyens humains pour les combler ».

Cette phrase de Jean-Sylvain Chavanne qui est le **responsable de la sécurité des systèmes d'information** au CHU de Brest, nous permet de comprendre l'un des enjeux majeurs de cette crise qui touche le secteur de la santé, le manque de personnels affectés à la sécurité informatique. Pour améliorer la sécurité de nos hôpitaux, le gouvernement à lancé un plan de ***20 millions d'euros supplémentaires pour la cybersécurité des établissements de santé.***

Le 21 Décembre 2022, le gouvernement à annoncé le lancement d'un plan de préparation aux incidents cyber à destination des établissements de santé afin de réagir plus efficacement en cas d'urgence.

Ce plan se divise en trois grandes mesures :

- 100% des établissements de santé devront effectuer un exercice de crise avant 2024, et même avant mai 2023 pour les établissements prioritaires.
- Un « plan blanc numérique » sera diffusé courant 2023 aux établissements de santé. Élaboré dès le début de l'année par la Direction générale de l'offre des soins, il a pour objectif de donner aux hôpitaux les premiers réflexes à adopter en cas de cyberattaque réussie, de l'activation d'une cellule de crise à la projection des conséquences de l'attaque.
- Enfin, le gouvernement a créé un groupe de travail composé de « l'ensemble des autorités compétentes ». Il aura pour mission de bâtir, depuis décembre, un nouveau projet de plan cyber « massif » pour les quatre prochaines années.

Conclusion

En conclusion, la sécurité informatique dans les hôpitaux est un enjeu crucial pour garantir la confidentialité et l'intégrité des données de santé. Les risques d'attaques informatiques sont de plus en plus nombreux et sophistiqués, ce qui nécessite la mise en place de mesures de protection efficaces et régulières. Les établissements de santé doivent ainsi investir dans des solutions de sécurité adaptées à leurs besoins et à leur budget, et sensibiliser leur personnel à la sécurité informatique. La sécurité des systèmes d'information est un enjeu collectif qui doit être pris en compte pour assurer la qualité des soins et la confiance des patients dans le système de santé.

Sources:

Pourquoi l’informatique des hôpitaux est toujours bien trop vulnérable

Victime d'une cyberattaque, l'hôpital de Dax fonctionne au ralenti

L'hôpital de Villefranche-sur-Saône victime d'un ransomware, des opérations reportées

Cybersécurité des hôpitaux : le recrutement, le talon d'Achille de la politique du gouvernement
(Nous avons dû manipuler le css de ce site pour accéder à l'entièreté de l’article, ce qui est très à propos concernant le module)