FUTURA

Cyberattaques : vos données médicales sur le dark web ?

Podcast écrit et lu par Adèle Ndjaki

[*Générique d'intro, une musique énergique et vitaminée.*]

Vos données médicales dans le viseur des hackers, c'est le décryptage de la semaine dans Vitamine Tech.

[*Fin du générique.*]

L'ANSSI, l'agence en charge de la cybersécurité en France, a réalisé un bilan des menaces numériques pesant sur le secteur de la santé. Selon ses résultats, entre 2022 et 2023, trente hôpitaux en France ont été victimes de cyberattaques. Cela met ainsi en évidence une menace de plus en plus importante pour la sécurité des systèmes de santé. Ces attaques, qui ont exposé des millions de données sensibles, révèlent la vulnérabilité des établissements face à des cybercriminels cherchant à accéder aux informations personnelles des patients. Avec des risques potentiellement graves pour la continuité des soins et la protection des données, la cybersécurité devient un enjeu stratégique pour les hôpitaux. Mais malgré les efforts pour renforcer la sécurité, des défis subsistent, notamment des infrastructures obsolètes et des ressources limitées, ce qui complique ainsi la tâche. Bonjour à toutes et à tous, je suis Adèle Ndjaki, et cette semaine, dans Vitamine Tech, on fait le point sur la cybersécurité dans les hôpitaux.

[*Une musique électronique calme.*]

En 2024, les hôpitaux français ont enregistré plusieurs attaques de grande ampleur. Parmi les cas les plus médiatisés, on trouve l'hôpital Simone Veil de Cannes, victime d'une cyberattaque en janvier, l'hôpital d'Armentières en février, où près d'un million de données patients ont été exposées, ainsi que l'intrusion dans le système du groupe Hospi Grand Ouest en octobre. Et plus récemment, la plateforme Mediboard, utilisée par plusieurs hôpitaux a été piratée, révélant les données personnelles de plus de 750 000 individus. Ces incidents soulignent un problème croissant : la sécurité des données dans les établissements de santé. Mais pourquoi ces institutions sont-elles devenues des cibles privilégiées pour les cybercriminels ? Les hackers cherchent principalement à accéder aux données personnelles des patients :numéros de sécurité sociale, bilans médicaux, antécédents de traitement, évaluations psychologiques, et bien plus encore. Ces informations peuvent être revendues sur le Dark Web à des fins de fraude ou de chantage. Un exemple marquant remonte à 2020, lorsqu'une cyberattaque a menacé des patients en Finlande d'exposer leurs suivis psychologiques en ligne à moins qu'ils ne versent une

rançon. Les hackers déploient des méthodes de plus en plus sophistiquées pour pénétrer ces systèmes. Le phishing par exemple, où des messages frauduleux sont envoyés pour tromper les destinataires et obtenir leurs identifiants de connexion. Il y a aussi les ransomwares, où les pirates cryptent les données d'un établissement et demandent une rançon pour les restaurer. On peut aussi parler de l'exploitation de vulnérabilités dans les systèmes de sécurité non corrigés, comme ce fut le cas avec l'attaque du système de gestion des dossiers médicaux « Aetna » en 2017. Il y en a d'autres, mais je terminerai sur les attaques "Man-in-the-middle" (MITM), où les hackers interceptent les échanges de données entre patients et médecins via des réseaux non sécurisés. Les répercussions de ces cyberattaques sont multiples et particulièrement graves. Au-delà des coûts financiers liés à la rançon, à la remise en état des systèmes et à l'amélioration de la cybersécurité, ces attaques perturbent directement les soins apportés aux patients. Les retards dans les interventions urgentes, le dysfonctionnement de dispositifs médicaux vitaux, ou encore la perturbation des traitements peuvent mettre en danger des vies humaines. En 2020, un décès tragique à l'hôpital de Düsseldorf, lié à une cyberattaque, a montré qu'une attaque informatique pouvait avoir des conséquences fatales. Tout ça peut affecter la confiance des patients dans le système de santé et peut entraîner des pertes financières considérables pour les établissements. C'est un défi majeur pour le secteur hospitalier, qui doit redoubler d'efforts pour renforcer sa cybersécurité afin de protéger à la fois les patients et le bon fonctionnement des soins.

[*Virgule sonore, une cassette que l'on accélère puis rembobine.*]
[*Une musique de hip-hop expérimental calme.*]

Les hôpitaux et cliniques sont devenus des cibles de choix pour les cybercriminels, car ils détiennent des informations extrêmement sensibles. Selon certaines estimations, un dossier médical peut se vendre entre 50 et 250 euros sur le Dark Web, faisant de ce secteur un véritable jackpot pour les hackers. En France, bien que le gouvernement affirme que l'État ne paye pas de rançons, le coût des cyberattaques reste colossal, et la valeur totale du butin pour les pirates est estimée à plusieurs milliards d'euros. Le risque numérique est de plus en plus une priorité dans le plan blanc, un un dispositif de crise, de chaque établissement hospitalier. Pourtant, les hôpitaux, déjà en proie à des difficultés financières depuis des années, peinent à faire face à ce défi. Malheureusement, la cybersécurité dans les établissements de santé présente de nombreux obstacles. D'abord, les infrastructures informatiques vieillissantes sont un véritable point faible. Beaucoup d'hôpitaux utilisent des systèmes anciens ou des équipements médicaux connectés qui ne sont pas régulièrement mis à jour, les rendant vulnérables aux attaques. Le manque de ressources empêche aussi plusieurs établissements d'investir dans des solutions de cybersécurité performantes ou de former correctement leur personnel. Et le nombre élevé de points d'accès aux systèmes hospitaliers, comme les dispositifs médicaux connectés, les dossiers électroniques de santé, et l'utilisation de nombreux outils par un personnel souvent diversifié, multiplie les risques.
Malgré ces difficultés, certains hôpitaux redoublent d'efforts. Ils mettent en place des protocoles pour protéger les données, installent des systèmes de détection des intrusions, et forment leur personnel aux bonnes pratiques de cybersécurité entre autres. Mais la menace reste omniprésente, et face à ce constat, l'État a pris plusieurs mesures pour soutenir les hôpitaux dans la protection de leurs systèmes. Des formations et des campagnes de sensibilisation ont été mises en place pour aider le personnel à adopter les bonnes pratiques. De plus, des normes visant à sécuriser les infrastructures de santé ont été

adoptées, et un soutien financier a été accordé pour l'acquisition d'outils de cybersécurité. En cas de cyberattaque, des agences comme l'ANSSI, l'Agence nationale de la sécurité des systèmes d'information, interviennent pour aider les hôpitaux à gérer la crise et à restaurer leurs systèmes. L'État encourage également des partenariats entre le secteur public et privé pour partager des informations sur les cybermenaces et renforcer ainsi la résilience globale des hôpitaux face aux attaques. Qui sait ? Avec une préparation accrue et un soutien renforcé, les établissements de santé pourront mieux faire face à ces défis et continuer à garantir la sécurité des soins et des données des patients.

[*Virgule sonore, un grésillement électronique*.]

C'est tout pour cet épisode de Vitamine Tech. Pour ne pas manquer nos futurs épisodes, abonnez-vous dès à présent à ce podcast, et si vous le pouvez, laissez-nous une note et un commentaire. Cette semaine, je vous recommande le tout dernier épisode de Futura INNOVATION dans lequel je fais le point sur l'enquête de l'Inserm concernant l'évolution des pratiques sexuelles des Français. Pour le reste, je vous remercie pour votre fidélité à Vitamine Tech, je vous souhaite tout le meilleur, et, comme d'habitude, une excellente journée ou une très bonne soirée.

[*Un glitch électronique ferme l'épisode*.]