NTT Security

Vue d'ensemble

La cybersécurité dans les établissements de santé publics et privés

Depuis de nombreuses années déjà, le risque lié à la sécurité de l'information constitue un véritable enjeu pour les prestataires de santé. C'est pourquoi la cybersécurité demeure une priorité absolue pour les acteurs publics et privés de ce secteur.

Avec des établissements toujours plus innovants et dépendants de l'interconnectivité des systèmes et des données, le secteur de la santé est devenu une cible de choix pour les cybercriminels. Aujourd'hui, la question n'est donc plus de savoir *si*, mais plutôt *quand* une cyberattaque se produira.

Bornes d'information, moniteurs de fréquence cardiaque, pompes à perfusion, systèmes d'imagerie, accès Wi-Fi, BYOD… devant la pléthore d'équipements connectés qu'ils utilisent, les prestataires de santé du monde entier sont confrontés à des menaces aussi multiples que variées. En effet, sécuriser cette multitude d'appareils et de terminaux au sein d'un établissement constitue un véritable défi. Sans parler de la complexité des questions de conformité.

Par ailleurs, le cabinet Gartner estime que le nombre d'appareils médicaux nécessitant une sécurité renforcée devrait augmenter de 45 % d'ici 2020.[1]

Les défis de la cybersécurité dans les établissements publics et privés

Les prestataires de santé sont confrontés à de nombreux problèmes de sécurité de l'information :

- L'émergence perpétuelle de nouvelles menaces et la sophistication incessante des menaces existantes
- L'augmentation des risques de sécurité et de confidentialité causés par la multiplication des appareils médicaux connectés
- L'accroissement de la surface d'attaque – Les objets IoT, les ordinateurs et les systèmes existants peuvent être incompatibles avec les dispositifs de défense de nouvelle génération, constituant ainsi autant de points d'accès potentiels pour les cybercriminels
- La crainte de la publicité négative qu'engendre une violation de sécurité de grande ampleur
- Les conséquences d'une intrusion et les questions qu'elle soulève – Aurions-nous pu l'éviter ? Que s'est-il passé ?
- Les maillons faibles de l'infrastructure – Le secteur de la santé dépend énormément de ses contractuels et autres intérimaires. Or, ces derniers n'appliqueront pas toujours les processus de sécurité à la lettre
- L'hébergement en interne des systèmes propriétaires des fournisseurs
- Le durcissement du cadre réglementaire édicté par les autorités de tutelle
- La confidentialité des données des patients – En France, plusieurs articles de la CNIL régissent l'échange et le partage des informations de santé

75,7 % des personnes interrogées déclarent que leur établissement a subi un incident de sécurité significatif au cours des 12 derniers mois. 61,9 % affirment que tout est parti d'un e-mail.

Enquête cybersécurité HIMSS 2018

Des fonctionnalités exclusives

Nous proposons une vaste gamme de services managés de sécurité, de mise en conformité et de gestion du risque.

Nos experts s'appuient sur notre rayon d'action mondial et nos ressources locales pour identifier les enjeux spécifiques auxquels votre établissement (public ou privé) est confronté.

En collaboration avec notre réseau de partenaires de confiance et les entreprises du groupe NTT, nous garantissons votre cyber-résilience grâce à une combinaison de services de conseil et de sécurité managée, en environnement hybride et dans le cloud.

Services de sécurité complets de NTT Security pour le secteur de la santé

Conformité et conseil

Les établissements de santé doivent quotidiennement relever des défis d'ordre juridique. Quant à leurs RSSI, ils n'ont jamais consacré autant de temps aux questions de conformité. La majorité des règlementations en vigueur visent à garantir la protection des dossiers de santé, ce qui place le secteur sous une immense pression, par crainte de se voir infliger des amendes colossales en cas de non-conformité. En France, l'officialisation du Dossier médical partagé (DMP), le 6 novembre 2018, soulève déjà de nombreuses questions quant à la sécurité des données confidentielles qu'il contient. Le Ministère de la santé se veut

1. *Gartner, Top Three Security and Privacy Impacts of Connected Medical Devices on Healthcare Providers, Saniye Burcu Alaybeyi, Marc-Antoine Meunier, Gregg Pessin, septembre 2017*

Copyright© NTT Security 2018

rassurant sur le sujet, affirmant que toutes les données sont protégées et chiffrées. Aux États-Unis, les prestataires de santé sont tenus de collecter des informations complètes sur leurs patients sous forme de dossiers électroniques. Ils doivent par la suite chiffrer et protéger ces données pour les rendre « inutilisables, illisibles et indéchiffrables » aux utilisateurs non autorisés, puis informer les parties concernées en cas de violation. Toute négligence intentionnelle à envoyer ces notifications les expose à des pénalités sévères pouvant atteindre 1,5 million de dollars. S'ajoute à cela, l'obligation de respecter les exigences d'autres règlementations (HIPAA, HITECH, CMS, ASTM et IEC). Or, dans un tel contexte, les probabilités d'erreurs sont élevées.

Au Royaume-Uni, les établissements doivent aussi s'assurer de notifier les autorités en cas de violation des données personnelles. Toute attaque non signalée qui découlerait d'une infraction sérieuse au Règlement général sur la protection des données (RGPD) exposerait l'établissement concerné à de très lourdes amendes de l'ICO (Information Commissioners Office). Enfin, en Allemagne, l'amendement au règlement national sur la protection des données (Bundesdatenschutzgesetz, BDSG) a considérablement changé les dispositions existantes dans l'optique de les aligner au RGPD.

Connaître vos engagements et vos écarts de conformité est une chose. Savoir les gérer en est une autre.

En misant sur les entreprises du groupe NTT, vous bénéficiez de l'accompagnement d'experts qui vous aideront à gérer tous les aspects stratégiques et techniques de vos politiques et processus de gouvernance, de gestion du risque et de mise en conformité. Vous pourrez ainsi créer une infrastructure de sécurité équipée des politiques, des processus, de l'architecture et de l'expertise adaptés à votre entreprise. Les conseils de prestataires externes peuvent être très utiles pour développer une stratégie de sécurité complète. Grâce à notre Méthodologie globale d'entreprise, nous vous aidons à évaluer votre exposition pour mieux guider vos décisions relatives à la gestion du risque.

Côté conformité, notre expertise couvre le data mining sur les logs (pour améliorer les investigations sur les incidents de sécurité et de conformité), la règlementation PCI, les audits réglementaires, les exigences GRC (gouvernance, risque, conformité), et le conseil en sécurité et gestion du risque.

Services de sécurité managés

Face à l'évolution, à la sophistication et à la fréquence croissantes des menaces, de nombreux prestataires de santé peinent à gérer tous les aspects de leur cybersécurité en interne. Choisir les services de sécurité managés de NTT Security, c'est opter pour une structure mondiale d'experts en sécurité spécialisés dans le secteur de la santé. Nous nous chargeons de la surveillance, de la gestion et du support de vos ressources IT et de vos systèmes de sécurité de bout en bout, 24 h/24 et 7 j/7. Contrairement aux autres solutions, notre offre mondiale de services de sécurité managés inclut des systèmes de détection des menaces, d'analytique avancée et de Threat Intelligence taillés pour votre secteur d'activité. Vous pouvez ainsi confier la gestion de tous vos besoins de transformation numérique à un seul fournisseur, en toute sérénité et en toute sécurité.

Nos services de sécurité managés vous permettent aussi d'appliquer facilement les recommandations de nos équipes de conseil et de bénéficier d'un service de sécurité complet, unique et en phase avec votre secteur.

Conclusions du rapport Risk:Value 2018

Selon le rapport Risk:Value 2018 de NTT Security :

- Plus de 40 % des prestataires de santé publics et privés ne disposent pas encore d'une politique formelle de sécurité de l'information
- Parmi les établissements ayant mis en place une politique, seuls 42 % pensent que tous leurs collaborateurs sont au courant de l'existence de cette politique
- Seulement la moitié des établissements publics et privés disposent d'un plan de réponse à incident
- En cas d'attaque provoquant une perte de données, l'érosion de la confiance des patients constitue un enjeu majeur pour les établissements
- 38 % des prestataires privés et 28 % des prestataires publics pensent qu'ils ne subiront jamais d'attaque
- Seulement 8 % des prestataires privés et 12 % des prestataires publics excluent tout recours à un fournisseur externe de services de sécurité managés pour appuyer leur équipe interne
- 66 % des établissements publics et privés citent le personnel contractuel et intérimaire comme le maillon faible de leur dispositif de sécurité

L'entreprise NTT Security

NTT Security est la branche et centre d'excellence sécurité du groupe NTT. Nous mettons notre expertise au service des entités du groupe NTT en délivrant des solutions métiers résilientes pour accompagner leurs clients dans leur transformation numérique. Forte de ses 10 centres opérationnels de sécurité (SOC), ses 7 centres de R&D et plus de 1 500 experts en sécurité, NTT Security intervient chaque année sur des centaines de milliers d'incidents à travers six continents.

Pour optimiser l'utilisation de nos ressources locales et libérer le potentiel de nos capacités mondiales, nous offrons un ensemble adapté de services de sécurité managés (MSS) mais également de conseil stratégique ou technologique aux entreprises. NTT Security fait partie intégrante du groupe NTT (Nippon Telegraph and Telephone Corporation), l'une des plus grandes entreprises de TIC au monde. Visitez **www.nttsecurity.com/fr-fr** pour en savoir plus sur NTT Security ou **www.ntt.co.jp/index_e.html** pour le groupe NTT.

Copyright© NTT Security 2018