STORMSHIELD

SANTÉ

GROUPEMENTS HOSPITALIERS DE TERRITOIRE

COMMENT OPTIMISER LA SÉCURITÉ DE SYSTÈMES D'INFORMATION UNIFIÉS

2016
DATE DE CRÉATION DES GHT

135
ÉTABLISSEMENTS GHT EN FRANCE

891
HÔPITAUX REGROUPÉS ET CONNECTÉS

Les vulnérabilités des dispositifs médicaux

Le déploiement de l'e-santé est très prometteur pour la santé publique, mais encore faut-il prendre en compte le risque cyber. De plus en plus connectés aux réseaux (wifi, radiofréquence, bluetooth...), les équipements médicaux se modernisent et présentent une avancée pour le monde de la médecine. Mais ils peuvent également présenter des faiblesses face aux cyberattaques, en étant infectés par un code malveillant via une liaison internet ou une clé USB.

Par ailleurs, la sécurité des données de santé devient de plus en plus complexe car elles circulent dorénavant entre les systèmes d'information d'un grand nombre d'acteurs : centres hospitaliers, secteur social et médico-social, médecine de ville, téléconsultation, sécurité sociale, mutuelles...

Le contexte

La loi de modernisation du système de santé français, mise en place en janvier 2016, a donné naissance à la création de Groupements Hospitaliers de Territoire (GHT). Des GHT qui permettent un nouveau mode de coopération entre les établissements publics de santé à l'échelle d'un territoire, notamment avec une mutualisation des équipes médicales et une meilleure répartition des activités de façon à ce que chaque structure trouve son positionnement dans la région. L'objectif est de garantir à tous les patients un meilleur accès aux soins en renforçant la coordination entre les hôpitaux publics autour d'un projet médical.

Les Systèmes d'Information apparaissent alors comme la composante indispensable à cette interaction entre les établissements de santé : partage de l'information médicale, mêmes outils sur l'ensemble du territoire, mutualisation des coûts liés aux systèmes d'information...

C'est la raison pour laquelle six centres hospitaliers au sein d'un même GHT ont décidé d'uniformiser la sécurisation de leurs infrastructures, totalement hétérogènes en matière d'équipements et de choix de constructeurs.

Un Responsable de la Sécurité des Systèmes d'Information (RSSI), faisant aussi office de Délégué à la Protection des Données (DPO), a également été nommé en tant que coordinateur de l'ensemble du projet et du pilotage global sur le long terme, en accompagnement des RSSI locaux.

La solution retenue

Le RSSI étant historiquement satisfait des solutions Netasq (devenues Stormshield en 2014), c'est tout naturellement qu'il a décidé de faire appel à Stormshield pour assurer cette sécurisation globale de l'ensemble du GHT, via le déploiement d'un cluster de SN2100.

Avec un débit pouvant atteindre 60 Gbps, ce pare-feu permet au client de disposer du meilleur rapport prix/performance du marché pour sécuriser son trafic. Par ailleurs, les solutions Stormshield étant déjà en places dans certains hôpitaux, le GHT a profité de cette volonté d'uniformiser le parc existant pour mettre à niveau l'ensemble de ses pare-feux.

Autres atouts du SN2100 : sa capacité à s'adapter à la configuration des réseaux et sa conformité à la réglementation RGPD en vigueur concernant la conservation et l'accès aux données et rapports.

D'un point de vue sécurité, le client est pleinement satisfait des fonctionnalités de ces pare-feux de nouvelle génération : détection et prévention des intrusions, protection contre les attaques DDos (dénis de service distribués), les injections SQL ou encore les fuites de données...

En complément, le client a également décidé de déployer un cluster de SN2000 sur les deux Centres Hospitaliers les plus importants. Il a pu apprécier en particulier la fluidité entre les réseaux (débit pouvant atteindre 30 Gbps), leur puissance et leur rapidité d'exécution.

De taille plus petite, les quatre autres établissements ont quant à eux été équipés avec des SN310 et SN510. Ces sites ont ainsi pu bénéficier des huit ports physiques du SN310 pour plus de souplesse et de granularité dans la définition de la politique de filtrage déterminée par le GHT. Avec le SN510, ces sites disposent de pare-feux intégrant les meilleures fonctionnalités proposées sur le marché.

Enfin, pour assurer le pilotage global de l'ensemble de ces équipements et en faciliter la gestion quotidienne, le GHT souhaitait également disposer d'une solution d'administration centralisée. La solution Stormshield Management Center (SMC) a été retenue pour assurer cette fonction. Elle facilite aujourd'hui la mise en place d'une topologie d'interconnexions sécurisées entre les différents établissements de santé et assure le pilotage des solutions de sécurité Stormshield, l'accès aux équipements et l'exécution de commandes sur plusieurs d'entre eux. Ces derniers peuvent échanger des données de configuration ou de supervision en temps réel, tout en garantissant la confidentialité et l'intégrité de ces données.

Toutes ces évolutions permettent aux établissements regroupés dans ce GHT d'envisager une meilleure mutualisation des compétences (comme par exemple l'intervention à distance d'un chirurgien pour le compte d'un autre hôpital) et une meilleure couverture des besoins fonctionnels.

À suivre...

Parfaitement satisfait de la fiabilité (au niveau des performances, de la disponibilité et de la redondance) des produits Stormshield, qualifiés ANSSI, et de l'interface ergonomique et facile d'accès de la solution d'administration centralisée SMC, le client envisage aujourd'hui de nouvelles évolutions. Et notamment, une segmentation du réseau afin de mieux protéger les outils biomédicaux. L'objectif de ce projet de cloisonnement étant d'isoler les flux critiques de ces équipements par rapport aux flux d'information courants. Une mesure nécessaire afin de limiter les risques pour les patients et de renforcer la résilience des Centres Hospitaliers.

STORMSHIELD

Partout dans le monde, les entreprises, les institutions gouvernementales et les organismes de défense ont besoin d'assurer la cybersécurité de leurs infrastructures critiques, de leurs données sensibles et de leurs environnements opérationnels. Les technologies Stormshield, certifiées et qualifiées au plus haut niveau européen, répondent aux enjeux de l'IT et de l'OT afin de protéger leurs activités. Notre mission : cyber-séréniser nos clients pour qu'ils puissent se concentrer sur leur cœur de métier, si cruciale pour la bonne marche de nos institutions, de notre économie et des services rendus aux populations. Choisir Stormshield, c'est privilégier une cybersécurité européenne de confiance. Pour en savoir plus : www.stormshield.com

Version 1.0 - Copyright Stormshield 2020