GESUNDHEIT

REGIONALE KLINIKGRUPPE

OPTIMIERUNG DER SICHERHEIT IN VEREINHEITLICHTEN INFORMATIONSSYSTEMEN

2016
GRÜNDUNGSDATUM DER GHT

135
GHT-EINRICHTUNGEN IN FRANKREICH

891
GRUPPEN- UND VERBUND-KLINIKEN

Schwachstellen von medizinischen Geräten

Der Einsatz von E-Health birgt vielversprechende Möglichkeiten für das öffentliche Gesundheitswesen, aber Cyber-Risiken sind dabei nicht außer Acht zu lassen. Die zunehmend vernetzten (über WLAN, Funk, Bluetooth...) modernen medizinischen Geräte stellen einen Durchbruch in der Welt der Medizin dar. Allerdings können sie auch Schwachstellen gegenüber Cyber-Angriffen aufweisen, wenn sie über das Internet oder einen USB-Stick mit Malware infiziert werden.

Darüber hinaus wird die Sicherheit von medizinischen Daten immer komplexer, da diese nun zwischen den Informationssystemen zahlreicher Akteure zirkulieren. Dazu zählen Klinikzentren, der soziale und medizinisch-soziale Sektor, Hausärzte, Anbieter von Tele-Sprechstunden, Krankenversicherungen usw.

Hintergrund

Nach dem Inkrafttreten des Gesetzes zur Modernisierung des französischen Gesundheitssystems im Januar 2016 wurden zahlreiche regionale Klinikgruppen (Groupements Hospitaliers de Territoire, GHT) gegründet. Diese GHTs ermöglichen eine neue Art der Zusammenarbeit zwischen Einrichtungen des öffentlichen Gesundheitswesens auf regionaler Ebene, vor allem durch die Zusammenlegung von medizinischen Teams und einer besseren Aufgabenverteilung, sodass jede Struktur sich auf eigene Weise in der Region positionieren kann. Das Ziel besteht darin, allen Patienten einen besseren Zugang zur Versorgung zu garantieren, indem die Koordination zwischen den öffentlichen Krankenhäusern rund um ein medizinisches Projekt verstärkt wird.

Für die Zusammenarbeit zwischen Gesundheitseinrichtungen haben sich Informationssysteme als unerlässlich erwiesen: Sie ermöglichen den Austausch von medizinischen Informationen, die Vereinheitlichung von Tools in der gesamten Region sowie die Vergemeinschaftung von Kosten im Zusammenhang mit den Informationssystemen und vieles mehr.

Aus diesem Grund beschlossen sechs Klinikzentren innerhalb derselben GHT, die Sicherheit ihrer Infrastrukturen zur vereinheitlichen, die bis dato in Bezug auf die Ausstattung und die Wahl der Hersteller vollkommen heterogen waren.

Zudem wurde ein Information Systems Security Officer (ISSO), der auch als Datenschutzbeauftragter (DPO) fungiert, zum Koordinator für das gesamte Projekt und die langfristige Systemverwaltung ernannt, um die lokalen ISSOs zu unterstützen.

Die Lösung der Wahl

Da der ISSO in der Vergangenheit mit den Lösungen von Netasq (das 2014 in Stormshield umbenannt wurde) zufrieden war, entschied er sich natürlich für Stormshield, um die Sicherheit der gesamten GHT durch die Implementierung eines SN2100-Clusters zu gewährleisten.

Mit einem Durchsatz von bis zu 60 Gbit/s bietet diese Firewall im Hinblick auf die Sicherung des Datenverkehrs das beste Preis-Leistungs-Verhältnis auf dem Markt. Da in einigen Krankenhäusern bereits Stormshield-Lösungen eingesetzt wurden, nutzte die GHT den Wunsch nach Vereinheitlichung der bestehenden Systeme, um alle ihre Firewalls zu aktualisieren. Zu den weiteren Vorteilen der Firewall SN2100 zählt ihre Anpassungsfähigkeit an Netzkonfigurationen und ihre DSGVO-Konformität hinsichtlich der Aufbewahrung und des Zugriffs auf Daten und Berichte.

Was die Sicherheit angeht, so ist der Kunde mit den Funktionen dieser Firewalls der neuen Generation vollauf zufrieden: Erkennung und Vorbeugung von unerlaubtem Eindringen, Schutz vor DDoS-Angriffen (Denial of Service) und SQL-Injections, Schutz vor Datenverlust usw.

Zusätzlich hat der Kunde beschlossen, an den beiden größten Kliniken einen SN2000-Cluster einzurichten. Besonders angetan war er von dem reibungslosen Datenfluss zwischen den Netzwerken (bei einem Durchsatz von bis zu 30 Gbit/s) sowie von der Leistung und der Arbeitsgeschwindigkeit der Firewalls.

Die vier kleineren Einrichtungen wurden mit SN310 und SN510 ausgestattet. Diese Standorte können so die acht physischen Ports der SN310-Firewall nutzen, die ihnen mehr Flexibilität und Granularität bei der Definition der GHT-Filterrichtlinien bietet. Mit der SN510 verfügen sie über Firewalls mit den besten Funktionen, die derzeit auf dem Markt erhältlich sind.

Um die Gesamtsteuerung aller Geräte zu gewährleisten und die tägliche Verwaltung zu erleichtern, suchte die GHT auch nach einer zentralen Verwaltungslösung. Hier fiel die Wahl auf das Stormshield Management Center (SMC). Diese Lösung ermöglicht heute die Implementierung einer Architektur von sicheren Verbindungen zwischen den einzelnen Gesundheitseinrichtungen sowie die Erprobung der Sicherheitslösungen von Stormshield, den Zugriff auf Geräte und die gleichzeitige Ausführung von Befehlen durch mehrere Geräte. Letztere können Konfigurations- oder Überwachungsdaten in Echtzeit austauschen und dabei die Vertraulichkeit und Integrität der Daten gewährleisten.

Durch all diese Entwicklungen können die in dieser GHT zusammengeschlossenen Einrichtungen eine bessere Bündelung ihrer Kompetenzen (wie z. B. Fernintervention durch einen Chirurgen im Auftrag einer anderen Klinik) und eine bessere Abdeckung des funktionalen Bedarfs ins Auge fassen.

Fortsetzung folgt...

Der Kunde ist mit der Zuverlässigkeit der ANSSI-zertifizierten Stormshield-Produkte (hinsichtlich Leistung, Verfügbarkeit und Redundanz) sowie mit der ergonomischen und leicht zugänglichen Schnittstelle der zentralisierten SMC-Verwaltungslösung vollkommen zufrieden und denkt nun über neue Entwicklungen nach. Dazu zählt vor allem eine Segmentierung des Netzwerkes zum besseren Schutz von biomedizinischen Geräten. Das Ziel dieser Partitionierung ist es, kritische Datenflüsse zwischen diesen Geräten von dem normalen Datenfluss zu trennen. Diese Maßnahme ist notwendig, um die Gefahren für Patienten zu minimieren und die Belastbarkeit der Klinikzentren zu stärken.

STORMSHIELD

Überall auf der Welt müssen Unternehmen sowie Regierungs- und Verteidigungsbehörden die Cyber-Sicherheit ihrer kritischen Infrastrukturen, sensiblen Daten und Betriebsumgebungen gewährleisten. Die auf höchster europäischer Ebene zertifizierten und qualifizierten Stormshield-Technologien erfüllen die Herausforderungen von IT und EO zum Schutz ihrer Aktivitäten. Unser Ziel: Unsere Kunden sollen in Sachen Cyber-Sicherheit auf uns vertrauen können, damit sie sich auf ihre Kernaufgaben konzentrieren können, die so wichtig für das reibungslose Funktionieren unserer Behörden, unserer Wirtschaft sowie der Dienstleistungen für die Bevölkerung sind. Mit der Wahl von Stormshield setzen Sie auf vertrauenswürdige Cyber-Sicherheit – made in Europe. Weitere Informationen: www.stormshield.com