UNITED
SECURITY
PROVIDERS

NETZWERKSICHERHEIT FÜR SPITÄLER

NSN MEDICAL GRUPPE & NIOS

SUCCESS STORY

Die Ansprüche an das Netzwerk sind im modernen Spital ausgesprochen hoch und vielschichtig. Das Netzwerk besteht aus IT- und Medizinal-Infrastruktur. Während das Hauptaugenmerk auf dem Schutz von Patientendaten liegt, soll der Netzzugang trotzdem Flexibilität bieten: Patienten möchten im Internet surfen, das medizinische Personal benötigt für eine effiziente Behandlung flexiblen Datenzugriff. Der NSN medical Gruppe gelingt mit der Network Access Control Lösung von United Security Providers der Spagat zwischen dem gewollten Mass an Sicherheit und Benutzerfreundlichkeit.

Die Netzwerksicherheit aufrecht zu erhalten ist eines der wichtigsten IT Anliegen für Unter-nehmen im Healthcare Segment. Das weiss auch die NSN medical Gruppe, welche dies gleich für 9 Unternehmen an 14 Standorten – darunter zwei Listenspitäler – sicherstellen muss. Das medizinische Personal benötigt rund um die Uhr Zugang zu aktuellen Gesundheitsinformationen, um eine kompetente Be-handlung bieten zu können.

Die Patienten im stationären Aufenthalt suchen – sobald ihr Gesundheitszustand es erlaubt – wieder Anschluss an die digitale Welt und möchten Informations- und Entertainmentdienste nutzen, im Internet surfen oder chatten. Sogar medizinische Spezialgeräte wie Computertomographen entfalten die volle Bandbreite ihrer Funktionalitäten erst mit dem Anschluss ans Netzwerk.

BEDÜRFNISSE ERKENNEN UND LÖSUNGSORIENTIERT HANDELN

Die Spitalgruppe erkannte die neuen Herausforderungen und entschied sich, sein Netzwerk an die geänderten Bedürfnisse anzupassen. Das zukünftige Netzwerk sollte der IT die Flexibilität bieten, den unterschiedlichen Stakeholder einen adäquaten Netzzugang zur Verfügung zu stellen. Ein wirkungsvoller Schutz der Patientendaten musste dabei auch in Zukunft oberste Priorität behalten.

OPERATION NETZWERKSICHERHEIT

Die Modernisierung des Netzwerks erfolgte in zwei Schritten. Im Zuge einer Neusegmentierung des Netzwerks wurden zunächst verschiedene Netzwerkzonen geschaffen. Applikationen mit sensiblen Patientendaten wurden logisch von Anwendungen, die beispielsweise via Internet erreichbar sind, getrennt. Ein Gäste-VLAN ergänzte die Netzwerksegmentierung.

Das neue, ausgeklügelte Zonenkonzept bringt nur dann den erwarteten Nutzen, wenn neu an das Netzwerk angeschlossene Geräte bereits am Zugangspunkt ins richtige Netzwerksegment eingeteilt werden. Die Grundlage dazu wurde im Rahmen des zweiten Teilprojekts, mit der Implementierung einer modernen Network Access Control Lösung, geschaffen.

USP NETWORK AUTHENTICATION SYSTEM®

NSN medical AG entschied sich zusammen mit NIOS für die Network Access Control Lösung von United Security Providers. Das USP Network Authentication System® detektiert neu am Netzwerk angeschlossene Geräte und entscheidet anhand ihrer Authentisierungs-merkmale über deren Zugangsberechtigung. Nur bekannte und policykonforme Geräte der Mitarbeitenden erhalten Zugang zu produktiven Netzwerkbereichen. Patienten oder Gäste können sich mit ihren mobilen Geräten registrieren und verfügen anschliessend über Zugang zum Internet. Die Lösung wurde nach einer Testphase zunächst in kleineren Standorten produktiv geschaltet und dann stufenweise auf grössere Standorte, wie zum Beispiel das Paracelsus Spital in Richterswil oder die Limmatklinik in Zürich, ausgeweitet.

©Teil der NSN Gruppe:
Die Limmatklinik in Zürich

VORTEILE AUCH IM IT OPERATIONS

Die Flexibilität der Strukturgestaltung sowie der fortgeschrittene Automatisierungsgrad bringen viele Vorteile im Betrieb der Lösung. Aus technischer Sicht interessieren vor allem das automatische V-LAN Management, die vorhandene Sicherheit und die Flexibilität. Die Virtual Appliance bietet die Möglichkeit, betriebseigene Geräte zu kennzeichnen. Diese Erkennung wird vom zentralen System gespeichert und, egal wo das Gerät sich mit dem Netz verbindet, wiedererkannt. Die Zuweisung in das definierte Netzwerksegment erfolgt automatisch und sehr performant. Das ermöglicht eine vielseitige Nutzung der Hardware-Infrastruktur mit einem gleichzeitig sehr hohen Sicherheitslevel.

Ein Medizinalgerät, das bisher im Hauptgebäude an Switch 4 hing und neu in Nebengebäude an Switch 7 soll, kann so ganz einfach gezügelt werden. Nach dem Einstecken am neuen Ort verfügt das Medizinalgerät automatisch über die korrekte Provisionierung und ist einsatzbereit. Die für den Spitalbetrieb unverzichtbaren Medizinalgeräte sind so stets einsatzbereit – und verfügen jederzeit über die optimale gerätespezifische Netzwerk-Konfiguration.

Durch die hohe Automatisierung im Netzwerk gewinnen die Mitarbeiter an Effizienz, der Betrieb ist einfacher und schlanker als in klassischen Netzwerken, was IT-Kosten spart. Ausserdem enorm wichtig: Die Gewissheit, dass nicht registrierte Geräte keine Möglichkeit mehr haben, sich logisch mit der Spitalinfrastruktur zu verbinden, ist schlicht beruhigend und entspricht dem gängigen Standard.

FAZIT ZUR NETZWERKSICHERHEIT IN DER SPITAL-BRANCHE

NSN medical AG und alle Tochterhäuser verfügen, dank der Netzwerksegmentierung in Kombination mit der Netzwerkzugangskontrolle durch das USP Network Authentication System®, über höchste Flexibilität und Sicherheit im Netzwerk. Damit ist die Gruppe gerüstet für die Zeiten, in denen die Uhren noch schneller ticken – und in denen betreuendes Personal nebst Skalpell und Stethoskop auch Smartphone und Tablet für ihre Arbeit nutzt.

Weitere Informationen zu unserem Partner NIOS AG finden Sie auf der Website: www.nios.ch

swiss made software

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

UNITED SECURITY PROVIDERS

ZERO TRUST UNIVERSE

Besuchsadressen
Hauptsitz | Stauffacherstrasse 65/15, 3014 Bern
Baslerpark | Baslerstrasse 60, 8048 Zürich

+41 31 959 02 02
info@united-security-providers.ch
united-security-providers.ch