



Referenz-Projekt

Flexibles und dennoch sicheres Netzwerk für einen +20 Krankenhausverbund

Mandantenfähiges Network Access Control (NAC) ermöglicht
Sicherheit & Compliance in den Netzwerken der Gesundheitsdienstleister

Ausgangssituation

Ein regionaler Gesundheitsdienstleister betreibt 21 Krankenhäuser und Pflegeheime mit mehr als 8.000 Betten und 14.000 Mitarbeitern, die jährlich 250.000 Patienten versorgen. Die Gruppe, bekannt für den Einsatz neuester Technologien zur Verbesserung der klinischen Versorgung und Pflege der Patienten, hat eine innovative Lösung von Auconet zur Steuerung, zum Schutz sowie zur Einhaltung der Sicherheitsvorschriften für ihre Multi-Mandanten-IT-Infrastruktur implementiert.

Herausforderung

In der sich äußerst schnell verändernden Landschaft der Medizintechnik muss eine Krankenhauskette alle ihre Netzwerke und sensiblen Patientendaten schützen, jedoch gleichzeitig den medizinischen Testinstrumenten und lebensrettenden Geräten den Zugang zu den benötigten Netzwerkressourcen gewähren.

Die Gruppe hatte eine unzureichende Zugangskontrolle für ihre Netzwerke mit etwa 50.000 Switch-Ports und 23.000 Endgeräten. Ein Sicherheitsaudit hatte diese

Schwachstelle aufgedeckt. Das Fehlen einer aktuellen Bestandsaufnahme und eines Überblicks über alle IT-Assets machte die Diagnose und Lokalisierung von Fehlern zu einem manuellen Prozess, der durch Vermutungen und Ineffizienz gekennzeichnet war.

Der Gesundheitsdienstleister ist von Netzwerkheterogenität abhängig. Die eigene IT Abteilung betreibt medizinische Komponenten und Computer einer Vielzahl von Hardwareanbietern innerhalb ihres Netzwerks. Dies begründet den Bedarf an einer robusten, herstellerunabhängigen Sicherheitslösung, um den Zugang zum Netzwerk zu regeln. Dabei wurde die manuell gepflegte Datenbasis der IT-Assets durch eine dynamische Erfassung ersetzt.

Lösung

Das Netzwerk-Team des Dienstleisters suchte nach einer Lösung, die sowohl Port-Sicherheit als auch Zugangskontrolle (NAC) ermöglichte und gleichzeitig ein Profiling der Endgeräte unterstützte. Eine einfache Installation, die Fähigkeit, mehrere Netzwerke zu überwachen, und die Sicherheitsfunktionen zur

„In nur einer Woche installierten die Auconet-Techniker und unser Systemadministrator Auconet BICS am Pilotstandort. Nach einem erfolgreichen Proof of Concept gingen wir zu einer vollständigen Mehr-Mandanten-Implementierung über. Damit haben alle unsere Krankenhäuser die lokale Kontrolle und wir haben gleichzeitig eine zentrale Steuerungsmöglichkeit. Dies verbessert die Produktivität und gewährleistet die kontinuierliche Sicherheit der Endgeräte und Einhaltung der Audit-Richtlinien.“

Blockierung des Netzwerkzugriffs durch Gäste (Patienten und Besucher) oder unbefugte Benutzer waren ebenfalls wichtige Kriterien. Darüber hinaus sollten für den zukünftigen Einsatz Sicherheitsfunktionen nach dem 802.1X-Standard unterstützt werden.

Das IT-Team stellte fest, dass das Auconet Business Infrastructure Control System (BICS) all diese Kriterien erfüllt, zusätzlich Mandantenfähigkeit unterstützt, eine Schnittstelle zur SAP-Datenbank der Gruppe herstellen kann und die gesamte IT-Infrastruktur durchgehend überwacht.

Umsetzung

Die Pilotphase begann mit zwei Krankenhäusern in nahe gelegenen Städten. Die primäre BICS-Appliance wurde in einem Rechenzentrum am Hauptsitz des Unternehmens installiert. Eine redundante Backup-BICS-Appliance wurde in einem 200 km entfernten Datenzentrum installiert.

Ein Auconet-Techniker konnte den einfachen Installationsvorgang abschließen und die BICS-Appliance in der Zentrale platzieren, wo sie sowohl die MAC- als auch die IP-Adresse jedes Netzwerk- und Endgeräts in allen einzelnen Netzwerken der Gruppe zusammen mit deren physischen Standorten erfasst. BICS bietet zudem Echtzeit-Updates der SAP-Asset-Management-Datenbank, die jederzeit eine aktuelle Sicht auf alle Krankenhausnetzwerke ermöglichen.

Ergebnis

Die Gruppe hat eine vollständige Mehr-Mandanten-Umgebung etabliert. Jedes Krankenhaus und jede Einrichtung innerhalb der Gruppe hat nun eine vollständige Echtzeitsicht des eigenen Netzwerks mit Sicherheit, Kontrolle und Verwaltung für jeden Port und jedes Endgerät, während im Headquarter alle Netzwerke von einer zentralen Konsole überwacht werden können. Dies bietet eine effiziente Ausgewogenheit zwischen der

zentralen Verantwortung für das Netzwerk und der Betriebskontrolle vor Ort. Jetzt wird jedes IT-Asset und jedes medizinische Gerät im Inventar eines jeden Krankenhauses erfasst und sein Profil in der virtuellen CMDB des BICS gepflegt. Damit wird ebenfalls eine exakte Erfassung und Abrechnung der Netzwerknutzung durch die einzelnen Geschäftsbereiche ermöglicht.

Schnelle Amortisation und ständige Kontrolle der Infrastruktur

- ✓ **Vertraulichkeit mit Flexibilität** - Patientendaten und medizinische Geräte sind jetzt sicherer. Wichtige medizinische Geräte können in jedem Krankenhaus sicher auf das entsprechende Netzwerk zugreifen, was schnellere Tests und Behandlungen ermöglicht.
- ✓ **Stabilität** - Schützt die Robustheit des Netzwerks, indem falsch konfigurierte oder verdächtige Geräte, die das Netzwerk stören oder beeinträchtigen könnten, sofort blockiert werden.
- ✓ **Vollständige Informationen** - Die Netzwerke arbeiten jetzt mit präzisen, genauen Informationen, die eine hochgradig automatisierte Kontrolle und Richtliniendurchsetzung ermöglichen.
- ✓ **Vertrauen** - Die IT-Abteilung hat Vertrauen sowohl in ihre Netzwerkzugangskontrolle als auch in die Qualität der Daten über die IT-Infrastruktur, die das BICS liefert.
- ✓ **Automatisierung** - Die BICS-Lösung ersetzt ein schwieriges, weitgehend manuelles Netzwerk-Kontrollverfahren, bei dem die Ursachen von Problemen erahnt werden konnten.
- ✓ **Genauere interne Buchhaltung** - Das BICS überwacht ständig die Nutzung jedes Ports im Netzwerk und ermöglicht so 100% genaue Rückbuchungen an die richtige Benutzerabteilung.
- ✓ **Produktivität** - IT-Mitarbeiter benötigen jetzt deutlich weniger Zeit und Reisen, um Netzwerkprobleme zu diagnostizieren und zu beheben.
- ✓ **Konformität** - BICS hat die in einer Konformitätsprüfung festgestellten Sicherheitslücken geschlossen.
- ✓ **Zukunftssicherheit** - Die Gruppe für das Gesundheitswesen kann 802.1X-Sicherheit Schritt für Schritt hinzufügen; BICS wurde so konzipiert, dass 802.1X und MAC Layer-2 nebeneinander verarbeitet werden können.

Nehmen Sie Kontakt mit uns auf!



Auconet GmbH

An den Treptowers
12435 Berlin / Deutschland
Tel. Tel.: +49 (0) 30 254 690-0
info@auconet-it.com