## Netzwerkzugangskontrolle im Gesundheitswesen

Die Bedeutung der Informationstechnologie in deutschen Krankenhäusern ist in den letzten fünfzehn Jahren stark gestiegen. In der stationären Versorgung, der Ambulanz, selbst in den Operationssälen sind IT-gestützte Behandlungsplätze nicht mehr wegzudenken.

Auch die Verbreitung von PACS (Bildablage- und Kommunikationssystemen) oder die Einführung des Fallpauschalen-Systems (DRG) haben zu einer signifikanten Zunahme von PC-Arbeitsplätzen geführt. Als zeitgemäßen Komfort bieten viele Krankenhäuser ihren Patienten und Mitarbeitern Zugang zum Internet über mobile Devices an. Dies alles führt zu einem Anstieg der aktiven Netzwerkknoten und einem zusätzlichen Ausbau der Infrastruktur.

Die besondere Herausforderung liegt zweifellos im Wandel der Medizintechnik. Waren einzelnstehende Medizingeräte bisher nur über proprietäre Schnittstellen erreichbar, sind diese heute netzwerkfähig. Im Bereich der Medizintechnik wird ein Wachstum der Netzwerkknoten um 50 % prognostiziert.

Die Vernetzung der Medizintechnik bietet klare Vorteile: Geräte lassen sich lokalisieren, Behandlungsdaten sowie Software- und Wartungsstände zentral auslesen und abfragen. Die Zusammenführung medizinischer (MT) und nicht medizinischer Geräte (IT) zu einem medizinischen IT-Netzwerk (MIT) ist sinnvoll und wirtschaftlich. Diese Vernetzung birgt Risiken, zumal die Zielsetzung von IT und MT gegensätzlich ist. Während IT-Netzwerke einen hohen Bedarf an Funktionsumfang abdecken, ist die Medizintechnik auf Verfügbarkeit und Sicherheit getrimmt. Um beide Seiten aufeinander gut vorzubereiten bedarf es unter anderem einer Kontroll – und Zugangslösung.

ARP-GUARD begleitet die Flexibilisierung des Netzwerks und schützt den Zugang zu sensiblen Daten und Systemen. ARP-GUARD sorgt konsequent für die Durchsetzung Ihrer Richtlinien. Unbekannte Geräte werden lokalisiert und nicht unentdeckt in Ihr Netzwerk eingebracht. Krankenhauseigene Endgeräte werden identifiziert und dynamisch in die vorgesehene Umgebung (VLANs) gebracht. Auch besteht die Möglichkeit, das WLAN mit ARP-GUARD zu kontrollieren. Durch die Nutzung dieser Lösung wird das Netzwerk transparent und übersichtlich.

- Kontrolle und Steuerung für MT und IT-Systeme und Geräte
- Zugangskontrolle für das gesamte Krankenhausnetzwerk, auch standortübergreifend - Unbefugte bleiben draußen!
- Flexibler und sicherer Zugriff auf Patientendaten für autorisierte Systeme
- Internetzugang für Gäste/Patienten
- ARP-GUARD unterstützt Sie bei den Zertifizierungen ISO 27001, BSI-Standard zum Informationssicherheitsmanagement/IT-Grundschutz, KTQ/DIN EN 80001
- Kompletter Überblick und Kontrolle aller sich im Netzwerk befindlichen Geräte
- Echtzeitdokumentation aller Zugriffe auf das Krankenhausnetzwerk
- Inventar/Bestandslisten sind auf Knopfdruck verfügbar

**Das sagen unsere Kunden:**

**Marienhospital in Bottrop**

„Wir haben den ARP-GUARD eingesetzt, um einen Überblick über unser Netzwerk zu bekommen und um das Risiko durch fremde Endgeräte zu eliminieren. Das Produkt hat alle unsere Vorstellungen übertroffen und lässt sich dank seiner übersichtlichen Oberfläche auch leicht und mit geringem Aufwand administrieren. Jetzt haben wir nicht nur ein sicheres Netzwerk, sondern sehen neuen Anforderungen wie z.B. der ISO 80001 auch gelassen entgegen, weil wir den technischen Teil mit dem ARP-GUARD bereits umgesetzt haben."

Olaf Milde, EDV-Leiter des Marienhospitals in Bottrop

**Segeberger Kliniken**

„Der ARP-GUARD verschiebt Clients aktiv in das VLAN und übernimmt parallel die Autorisierung - eine ungeheure Erleichterung des Netzwerkmanagements und des vernetzten Arbeitens insgesamt."

Andreas Griese, IT-Leiter der Segeberger Kliniken GmbH