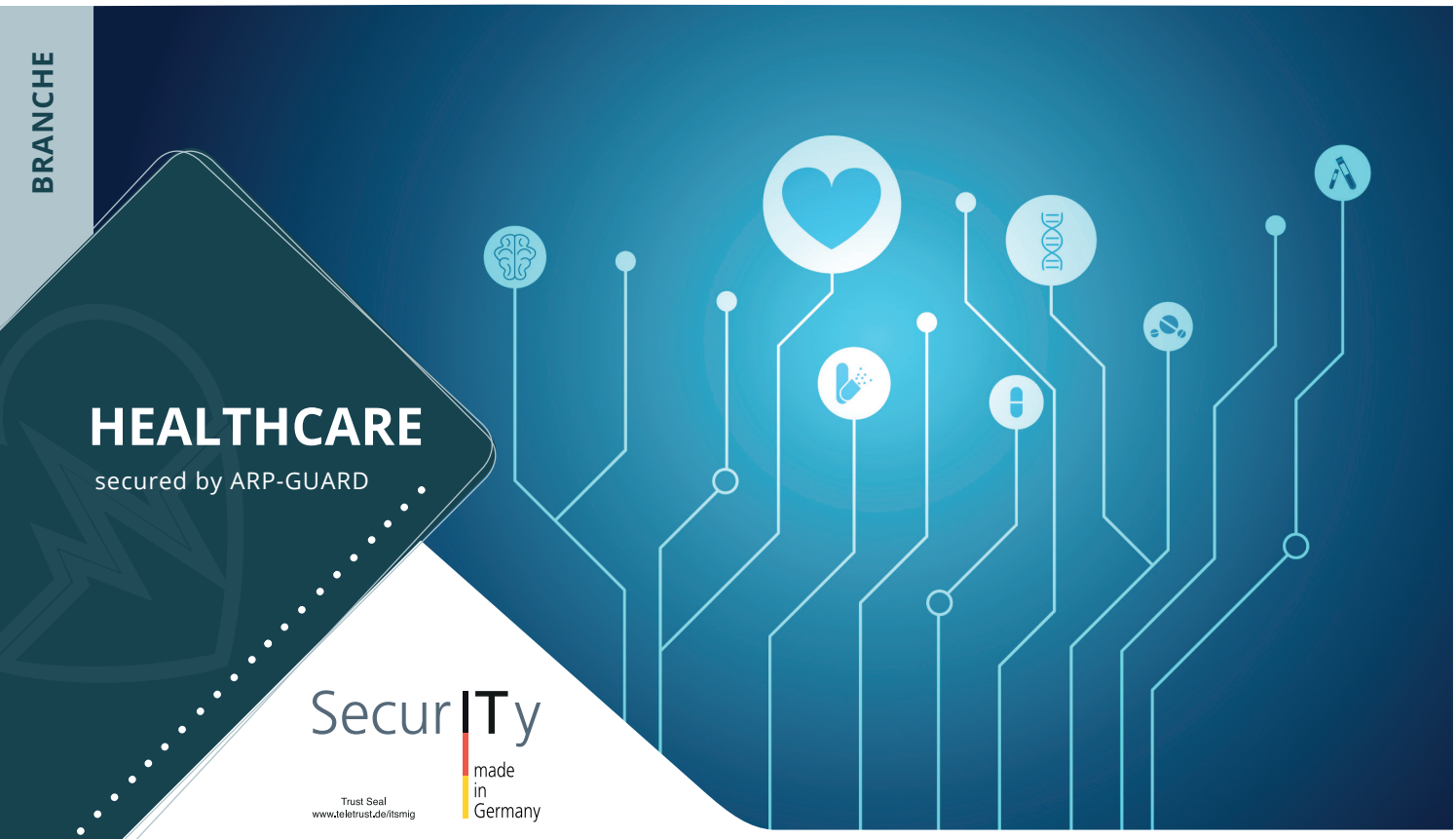
ARP GUARD by ISL

BRANCHE



HEALTHCARE

secured by ARP-GUARD

SecurITy made in Germany

Trust Seal www.teletrust.de/itsmig

DAS GESUNDHEITSWESEN IM BLICK

LIEBER VORSORGEN ALS NACHSORGEN

Dieses Motto betrifft nicht nur Patienten, sondern auch die IT-Landschaften in der Gesundheitsbranche. Mit der zunehmenden Digitalisierung nimmt auch die Zahl der Angriffsvektoren für Gesundheitseinrichtungen stetig zu. Ziel sind meist die vertraulichen Patientendaten oder die Schädigung der kritischen Infrastruktur. Damit steht die Patientenversorgung auf dem Spiel mit unmittelbaren Folgen für das Leib und Leben der Patienten. Dementsprechend werden die Gesundheitseinrichtungen stärker in die Pflicht genommen, eine resiliente Informationstechnik zu gewährleisten und die medizinische Versorgung sicherzustellen. Der branchenspezifische Standard B3S konkretisiert für das Klinikumfeld, wie die Anforderungen zum Stand der Technik erfüllt werden können – ARP-GUARD liefert hierzu geeignete Schutzmechanismen.

ERREICHUNG VON SCHUTZZIELEN

Mit der Sicherung der Netzwerkintegrität bis zum Endpoint sowie der eineindeutigen Geräteidentifizierung mittels Fingerprinting unterstützt ARP-GUARD bei der Erreichung der Schutzziele nach dem Standard B3S. Der Multi-Protokoll-Ansatz gewährleistet eine Verfügbarkeit per SNMP auch bei Ausfall des Systems. Darüber hinaus bietet die Sensor-Management Architektur die Möglichkeit, beliebig viele Standorte zu integrieren und zentral zu verwalten. Komplexere Anforderungen wie ein mandantenfähiges System oder georedundante Instanzen in verteilten Netzwerkstrukturen können ebenfalls bedient werden. ARP-GUARD unterstützt Sie tatkräftig bei notwendigen Zertifizierungen, wie ISO 27001, ISO 27799 oder Risikomanagement nach DIN EN 80001. Ein weiterer Vorteil ist die einfache Integration von ARP-GUARD in die bestehende Infrastruktur, welche in nur vier Schritten durchführbar ist. Der operative Geschäftsbetrieb bleibt dabei ungestört.

1. **Auslesen, identifizieren und lokalisieren** der Endgeräte. Abfrage der Switches/Router per SMNP.
2. **Klassifizierung der Endgeräte** durch DNS-Name, Hersteller, IP/MAC-Adresse oder Bestandslisten.
3. **Policy Definition.** Abwehr von unbekannten Devices und dynamische VLAN-Zuweisung.
4. **Schrittweise Aktivierung** der definierten Policies. Aktivierung der Schreibrechte auf den Switches.

WIR GEBEN IHNEN SICHERHEIT

Die Integration der medizintechnischen Geräte in die IT-Netzwerke bedient die Anforderung, digitale Befunde wie Röntgenbilder den Ärzten jederzeit und unkompliziert zur Verfügung zu stellen. Gleichzeitig sind die MT-Geräte und die vertraulichen Daten einem höheren Risiko ausgesetzt. Mit der logischen Netzwerksegmentierung bietet ARP-GUARD die Möglichkeit, diese Bereiche besonders gegenüber sich ausbreitenden Gefährdungen im Netzwerk zu schützen. ARP-GUARD identifiziert dank Fingerprinting-Technologie jedes Gerät eineindeutig und leitet es regelbasiert in das zugehörige, dynamische VLAN. Unerwünschte Geräte werden isoliert – Geräte, die nicht den Compliance-Anforderungen entsprechen, in Quarantäne-VLANs verschoben oder blockiert. Umfangreiche Reportings und die Sichtbarkeit aller Assets im Netzwerk liefern die Basis für ein Risikomanagement nach DIN EN 80001 und die Einleitung entsprechender Maßnahmen.

Marienhospital gGmbH 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 intuitiven Oberfläche leicht administrieren. Jetzt haben wir nicht nur ein sicheres Netzwerk, sondern sehen neuen Anforderungen wie der DIN EN 80001 gelassen entgegen, weil wir den technischen Teil mit dem ARP-GUARD bereits umgesetzt haben."

Olaf Milde, EDV-Leiter des Marienhospital

Segeberger Kliniken GmbH in Bad Segeberg

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

Andreas Griese, IT-Leiter der Segeberger Kliniken

CAPTIVE PORTAL ALS IDEALE ERGÄNZUNG

Mit Hilfe des Captive Portal wird eine komfortable und sichere Einbindung von verschiedenen mobilen Fremdgeräten durch Patienten oder Gästen innerhalb der Einrichtung schnell organisiert. Das System beinhaltet ein Gäste-Portal zur Selbstregistrierung, regelbasierte Zugangsberechtigungen und eine integrierte dynamische Firewall. Durch diese funktionale Erweiterung wird der administrative Aufwand für die Verwaltung von Gastzugängen signifikant reduziert.

DAS LEISTET ARP-GUARD IM KLINIKUMFFELD

- Assetmanagement – Sichtbarkeit und Kontrolle aller Geräte im Netzwerk
- Standortübergreifende Zugangskontrolle für das gesamte Krankenhausnetzwerk
- Schutz von Patientendaten vor Fremdgeräten und Systemmissbrauch durch Innentäter
- Netzwerksegmentierung und dynamische VLAN-Zuweisung
- Gastzugang für Patienten (Captive Portal) und BYOD
- Echtzeitdokumentation aller Zugriffe auf das Krankenhausnetzwerk
- Unterstützung bei der Zertifizierung nach ISO 27001, ISO 27799 und DIN EN 80001