ANWENDERBERICHT
HASSBERG-KLINIKEN

macmon intelligent einfach

Netzwerksicherheit in den Haßberg-Kliniken

Schutz kritischer Infrastrukturen

Das Kommunalunternehmen Haßberg-Kliniken betreibt zwei Krankenhäuser der Grundversorgung in Haßfurt und in Ebern, Raum Würzburg. Insgesamt werden jährlich rund 10.300 stationäre und fast 17.200 ambulante Fälle von einem hochqualifizierten Ärzte- und Pflegeteam versorgt.

Wir wollen, dass es Ihnen gut geht!
Haßberg-Kliniken

Für moderne Operations- und Diagnoseverfahren sind vor allem medizinische Geräte notwendig. Diese schützt macmon NAC vor unberechtigten Zugriffen.

Die Haßberg-Kliniken verfügen über eine hohe Kompetenz im Bereich moderner Operations- und Diagnoseverfahren. Für die qualitativ hochwertige, schnelle und zuverlässige Versorgung der Patienten steht ein IT-Netzwerk mit 1.000 Endgeräten bereit. Das Netzwerk integriert moderne Medizingeräte über eine Netzwerkverbindung und kann so Ärzten und Pflegekräften einen sicheren und direkten Zugang zu digitalen Informationen, wie beispielsweise MRT-Daten, ermöglichen.

Die Arbeitsplätze der Klinikmitarbeiter sind ausgestattet mit 160 Thin Clients, 165 Computern und 75 Laptops. Zu den Endgeräten zählen beispielsweise 250 Drucker. Aktuell sind 76 medizinische Geräte, wie MRT- oder Sonographie- oder Röntgengeräte integriert, Tendenz steigend. Aber auch Überwachungskameras oder Kartenlesegeräte gehören zur Infrastruktur. Klassische IT-Netzwerke, die Endgeräte wie beispielsweise MRT-Systeme integrieren, werden zu medizinischen Netzwerken. Damit muss z. B. für jedes noch so kleine Gerät, wie auch eine Kamera oder einen Laptop, eine Risikoabschätzung nach DIN 80001-1 gemacht werden. Die Kontrolle und Sicherheit dieser gemischten Netzwerke sind essentiell, eine Störung kann für Patienten lebensbedrohliche Folgen haben, wenn beispielsweise Beatmungsgeräte auf der Intensivstation gestört sind.

„Die Ziele unseres IT-Sicherheitskonzepts sind der Schutz vor internen und externen Angriffen, die Gewährleistung der Funktionalität aller Systeme und natürlich das Thema Datensicherheit, da wir es hier mit hochsensiblen Patientendaten zu tun haben. Auch die Sicherheit besonders kritischer Bereiche wie den Operations- oder Aufwachräumen, der Labor-Abteilung und der Intensivstation gehören zu unserem Security-Konzept. Spezielle schützenswerte Systeme sind: das Krankenhausinformationssystem (KIS), das Labor Informationssystem (LIS), das Radiologie Informationssystem (RIS) und diverse Befundsysteme."

Jan Schmitt, Systemadministrator der Haßberg-Kliniken

Stand: 09/2022

„Ein Penetrationstest hatte aufgezeigt, dass signifikante Defizite in der Netzwerktransparenz bestanden. Aufgrund einer Empfehlung eines Sicherheitsberaters haben wir uns für macmon NAC entschieden. Mit macmon Network Access Control wissen wir jederzeit, welche Geräte sich im Netzwerk befinden und können diesen durch switch-portgenaue Regeln automatisiert Zugänge gewähren oder verweigern. Die Sicherheitslücke konnte geschlossen und die Netzwerksicherheit deutlich verbessert werden."

Jan Schmitt,
Systemadministrator der Haßberg-Kliniken

Sensible Daten müssen dem medizinischen Personal stets zur Verfügung stehen. Für den Schutz vor dem Zugriff unberechtigter Dritter sorgt macmon NAC.

Ausgezeichnete Unterstützung der Netzwerksicherheit durch macmon NAC

In der Praxis werden in der Klinik mit macmon NAC unbekannte MAC-Adressen bei der Anmeldung an das Netzwerk sofort gesperrt, beispielsweise wenn ein Mitarbeiter ein neues Endgerät in die Datendose einsteckt. Und auch das unbekannte Gerät eines Angreifers erhält keinen Zugriff auf das Unternehmensnetzwerk und kann keinen Schaden anrichten – bei der zunehmenden Brisanz von Security-Themen für die Krankenhaus-IT ein wichtiger Vorteil. Da sich das Klinikum an zwei Standorten befindet hatte laut Schmitt die IT-Abteilung vor dem Einsatz von macmon NAC keinen sofortigen Überblick über Veränderungen im Netzwerk. So wurden durch den lokalen Hausmeister PCs oder Thin Clients umgebaut, oder Service-Techniker führten Änderungen an wichtigen Endgeräten wie MRTs durch, ohne Abstimmung mit der IT.

„Hier unterstützt macmon zuverlässig die Arbeit der IT-Abteilung. Jetzt informieren uns die Anwender, wie Service-Techniker, im Vorfeld, da sie sonst nicht weiterarbeiten können."

Jan Schmitt, Systemadministrator der Haßberg-Kliniken

Bewegungen im Netzwerk werden der IT-Abteilung jetzt sofort angezeigt und die Geräte, angepasst auf die Situation, behandelt. Nicht vertrauenswürdige Geräte können von macmon, sobald sie im Netzwerk erscheinen, in ein Besucher- oder Quarantäne-VLAN geschaltet werden. Außerdem zeigt macmon NAC an, wann ein Gerät das letzte Mal im Netzwerk aktiv war, somit können laut Schmitt „Leichen im Netzwerk gefunden werden." Geräte, die lange nicht im Netz gesehen wurden oder nach einem „Compliance-Check" als unsicher eingestuft werden, können bis zur Klärung des Status in einem Quarantäne-Netz gehalten werden.

Generell verfügen die Haßberg-Kliniken über drei Sicherheitszonen: Unautorisierte Geräte im LAN und WLAN werden von macmon NAC erkannt und bleiben außen vor. Geräte, die sich über eine bekannte MAC-Adresse identifizieren, werden in definierte Bereiche des Netzwerks gelassen. Geräte, die über ihre Computeridentität erkannt werden, können im dritten Segment arbeiten. Dazu gehören beispielsweise Laptops oder PCs.

Die drei Sicherheitszonen bei den Haßberg-Kliniken

Zone 1: Autorisierte Geräte im LAN/WLAN mit Computeridentität

Zone 2: Autorisierte Geräte im LAN/WLAN mit MAC-Adresse

Zone 3: Unautorisierte Geräte im LAN/WLAN

Stand: 09/2022

Sichere und zukunftsfähige Investition in die Sicherheit kritischer Infrastrukturen

Anwender von macmon NAC profitieren nicht nur vom hohen Sicherheitsniveau der Software bei einfachem Handling und Betrieb, sondern insbesondere auch von der Schnittstellenfähigkeit mit anderen führenden Security-Produkten. In Zusammenarbeit mit IT-Security-Lösungen kann macmon NAC beispielsweise ein non-konformes Gerät automatisch in Quarantäne stellen und den Netzwerk-Administrator über eine Attacke informieren, bevor eine gefährliche Ausbreitung im Klinikbetrieb stattfindet. macmon verfügt über Schnittstellen zu gängigen AntiVirus-Lösungen, zu Endpoint Security, IT-Notfallmanagement, Intrusion Detection- oder Prevention-Systemen (IDS/IPS), Asset Management, Inventory, Security Incident & Event Management-Lösungen (SIEM). macmon NAC lässt sich außerdem nahtlos in andere Security-Produkte wie Compliance-Anbindungen, Infrastruktur-Anbindungen, Asset-Management und Identitätsquellen, integrieren. Somit kann das Potential existierender Lösungen gemeinsam mit macmon NAC optimal ausgeschöpft, und dank der Skalierbarkeit, an wachsenden Anforderungen schrittweise angepasst werden.

macmon NAC – umfassender Netzwerkschutz für Krankenhäuser

- ✓ **Einbinden aller Medizintechnik** ohne Gefahr für das bestehende Netzwerk oder die medizinischen Geräte
- ✓ Ermöglichung des zeitlich und räumlich flexiblen **Zugriffs auf Patientendaten für Ärzte** bei gleichzeitigem **Schutz vor unbefugtem Zugriff**
- ✓ **Bereitstellen** von dedizierten und zeitlich **befristeten Internetzugängen für Gäste und Patienten**, ohne für Ärzte und Patienten getrennte WLAN-Infrastrukturen aufbauen zu müssen
- ✓ **Sicherstellung der Integrität des Netzwerkes** durch ausschließliches Gewähren des Netzwerkzugangs für die definierten (eigenen und zugelassenen) Geräte
- ✓ **Überwachung und Kontrolle aller** im Netzwerk befindlichen **Geräte** (Live-Bestandsmanagement) und Dokumentation aller Zugriffe auf das Krankenhausnetzwerk
- ✓ **Unterstützung bei der Zertifizierung nach ISO 27001**, der Umsetzung der BSI-Standards zum Informationssicherheitsmanagement, der IT-Grundschutz-Kataloge und von Krankenhaus-Zertifizierungsverfahren (z.B. KTQ-Zertifizierung oder DIN EN 80001)

Schauen Sie sich die Use-Cases im gemeinsam durchgeführten Webinar **„Kritische Infrastrukturen im Klinikum absichern“** an: **https://youtu.be/mKybXNITOqw**

FAZIT von Jan Schmitt:

„macmon NAC läuft im Hintergrund, da es zuverlässig arbeitet. Ich bin nur auf dem Web-Interface, um MAC-Adressen frei zu schalten oder um ein Gerät aus dem Netzwerk zu entfernen. Die Implementierung war reibungslos und schnell. Dabei wurde die OVA-Vorlage genutzt und in die virtuelle Umgebung eingebunden, die IP-Adresse eingestellt und die Switche hinzugefügt. Nach einer zweiwöchigen Testphase haben wir die MAC-Adressen den einzelnen Gruppen zugewiesen und konnten den Live-Betrieb starten. Zudem können Updates vom macmon Serviceportal einfach heruntergeladen werden.“ Zusammenfassend bringt Schmitt es auf den Punkt „macmon läuft, wie es soll.“

Kontakt macmon secure GmbH | Alte Jakobstraße 79-80 | 10179 Berlin | Tel.: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu

Stand: 09/2022