

macmon Network Access Control: Absicherung von IT- und medizinischen Netzwerken

**Handbuch - Umsetzung
DIN EN 80001-1
mit macmon NAC verfügbar !!!**

IT-Netzwerke, die Medizinprodukte integrieren, werden zu medizinischen Netzwerken – damit sind in nahezu allen Kliniken inzwischen die IT-Netzwerke gleichzeitig auch medizinische Netzwerke. Die Anforderung, dass die modernen Geräte über eine Netzwerkverbindung verfügen und die Anforderung der Ärzte, auf die digitalen Ergebnisse z.B. der MRT-Systeme (jederzeit und überall) zugreifen zu können, zwingt die IT-Abteilungen in der Regel zur Integration der früher getrennten Netze.

macmon-Nutzen für den Netzwerkschutz im Gesundheitswesen

- ✓ 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
- ✓ 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)
- ✓ Überwachung und Kontrolle aller im Netzwerk befindlichen Geräte (Live-Bestandsmanagement) und Dokumentation aller Zugriffe auf das Krankenhausnetzwerk
- ✓ Definition von gezielten Datenrouten und Übergabeschnittstellen zum besseren und gezielteren Schutz von sensiblen Daten wie Patienteninformationen



Die DIN EN 80001 betrachtet genau die IT-Netzwerke, die Medizinprodukte integrieren. Durch die Integration steigen sowohl die Komplexität, als auch die Gefahren und Risiken. Mit Hilfe der Definition allgemeiner Anforderungen, gerade in Bezug auf das Risikomanagement der betroffenen Netze, sollen wesentliche Eigenschaften, wie explizite Verfügbarkeiten und Schutz vertraulicher Daten, erreicht werden. Eine Reihe von Besonderheiten in Netzwerken der Gesundheitsbranche erfordern daher strategische Schutzmaßnahmen, zu denen macmon mit seinen vielfältigen Schutzmechanismen bereits auf den untersten Layern 2 und 3 beiträgt.

Das Einführen gesonderter VLANs war für viele Kliniken eine mögliche Lösung, um diesen Anforderungen zu begegnen. Diese wurde jedoch oft verworfen, da das manuelle Patchen der Ports aufgrund zu vieler Geräte-Umzüge und mobiler Arbeitsplätze eine nicht zu erfüllende Aufgabe war. macmon hilft gerade hier durch eine enorme Vereinfachung.

Der vlan manager von macmon unterstützt effektiv das Einführen dynamischer VLANs, dabei werden den Gerätegruppen die VLANs innerhalb der macmon GUI zugeordnet. Das VLAN-Schalten wird dann - unabhängig vom Hersteller der Switchinfrastruktur - automatisiert durch macmon übernommen. So kann das medizinische Personal jederzeit – sogar ohne weitere Rücksprache mit der IT-Abteilung - flexibel mit den Netzwerkzugängen umgehen.

Über macmon secure gmbh

macmon secure ist ein deutscher Software-Hersteller spezialisiert auf Netzwerk-Sicherheit. Die von macmon secure entwickelte, herstellerunabhängige und modulare NAC-Software macmon schützt das Netzwerk vor unautorisierten, nicht sicheren Geräten und internen Angriffen.

Zum Kundenstamm gehören europaweit mehr als 350 Unternehmen unterschiedlicher Branchen. Firmensitz der macmon secure gmbh ist Berlin. macmon secure ist Mitglied bei BITKOM und der Trusted Computing Group (TCG).

Systemanforderungen

macmon ist als virtuelle Appliance für VMware (Version 5.X empfohlen) und MS HyperV (MS Windows Server 2008 R2 empfohlen) verfügbar.

Die macmon Appliance ist mit einem 500 GB Raid-System, 4 LAN Ports und auf Wunsch redundantem Netzteil verfügbar und wird inkl. 3 Jahre vor Ort Austausch Service angeboten.

Bezugsquellen

Kontaktieren Sie Ihren nächstgelegenen macmon-Partner, um macmon für den Schutz Ihres Netzwerkes zu erwerben oder besuchen Sie www.macmon.eu für weitere Informationen.

Eine macmon Partner-Liste ist hier verfügbar: www.macmon.eu/partner.

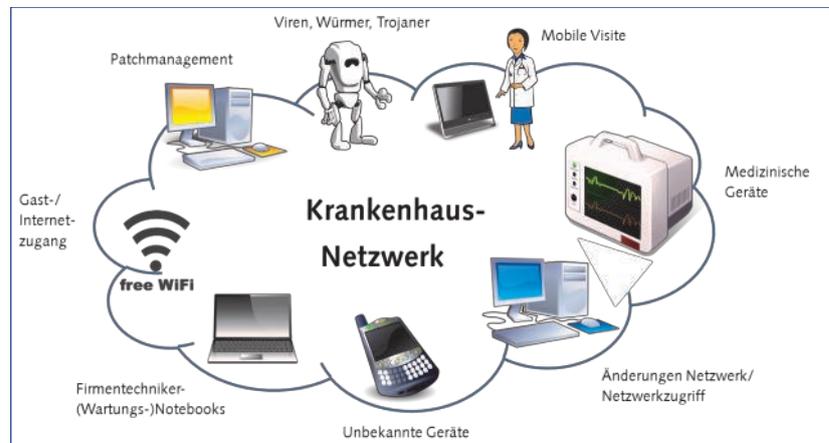


Abbildung: Gefährdungen und Risiken von medizinischen Netzwerken und von IT-Netzwerken

Die Sicherstellung, dass sich ausschließlich zugelassene Geräte in den Netzen bewegen, entspricht bereits der grundsätzlichen Aufgabe und Funktion der Zugangskontroll-Lösung macmon.

Jedes Gerät, das an das LAN angeschlossen wird, stellt ein Sicherheitsrisiko dar. Das gilt sowohl für ältere Medizintechnik, die nicht mit aktuellen Sicherheits-Updates versorgt werden und damit als Malware-Infektionsquelle dienen kann, als auch für die stetig steigende Anzahl der Patientensysteme, die keinerlei Kontrolle unterliegen.

Die Lösung für die vielfältigen Sicherheitsanforderungen ist somit eine „Sortierung“ des Netzwerkes. macmon identifiziert jedes Gerät eindeutig – ob über diverse Systemeigenschaften oder zertifikatsbasierte Technologien wie 802.1X –, sortiert diese dann anhand vordefinierter Regeln in ihre entsprechenden Gruppen und zugehörigen VLANs und isoliert fremde Geräte, um das Netzwerk vor unbefugten Eindringlingen zu schützen. Durch dieses Vorgehen erreichen Sie mit macmon ein sehr hohes Sicherheitsniveau für Ihr Kliniknetzwerk.

macmon: Erprobte NAC-Lösung im Gesundheitswesen

