Ganzheitliche IT-Security: Den Anforderungen gewachsen?

Krankenhausbetreiber und Medizinproduktehersteller im Fokus

Die Gesundheitsbranche ist verstärkt zum Ziel von IT-Angriffen geworden. Medienberichten zufolge waren jüngst vor allem Krankenhäuser von Sicherheitsbedrohungen durch Schadsoftwares betroffen. Aber auch Medizinproduktehersteller und -anwender müssen sich neuen Herausforderungen stellen, wenn es um die sichere Herstellung sowie das sichere Betreiben und Anwenden ihrer Produkte innerhalb von medizinischen IT-Netzwerken (MIT) geht.

Die Gründe für die enorm hohe Anfälligkeit sind ebenso vielfältig wie prekär. Häufig werden unzureichende Hardware-Kapazitäten, veraltete Betriebssysteme und Prozesse, ungenügende personelle Ressourcen sowie fehlende Budgets angeführt. Krankenhausbetreiber sind vermehrt dazu angehalten, geeignete Maßnahmen zu ergreifen. Gleichzeitig ergeben sich neue Anforderungen an Medizinproduktehersteller, -beauftragte und -anwender, nicht zuletzt durch unterschiedlichste Verordnungen und Richtlinien, wie etwa das Medizinprodukte-Gesetz (MPG).

Das übergeordnete Ziel liegt dabei stets auf dem Erreichen eines Höchstmaßes an Sicherheit für Patienten, Anwender und Betreiber von IT-Netzwerken und Medizinproduktehersteller sowie eines Mindestmaßes an Haftungsrisiken für Krankenhausbetreiber und Compliance-Verantwortliche. Einfache organisatorische Maßnahmen lassen sich bereits aus branchenspezifischen Standards ableiten.

Der 1. Schritt: Aktives Risikomanagement nach DIN EN/IEC 80001

Die DIN EN 80001-1 bildet eine gute Grundlage für den Nachweis der Einhaltung der Sorgfaltspflicht von Krankenhausbetreibern. Von Anwendungsfällen über Aufgaben bis hin zu Verantwortlichkeiten greift sie alle Aspekte des Risikomanagements auf, die die Komplexität eines Krankenhausbetriebs erfassen und gleichzeitig die Hersteller von Medizinprodukten einbeziehen. Darüber hinaus werden in ihr Aussagen über den erforderlichen Prozess getroffen sowie zusätzlich Handlungsempfehlungen zu dessen Realisierung und Implementierung gegeben (vgl. Abb.).

Der 2. Schritt: Aktives Schwachstellen-Management nach ISO 27001 und IT-Grundschutz

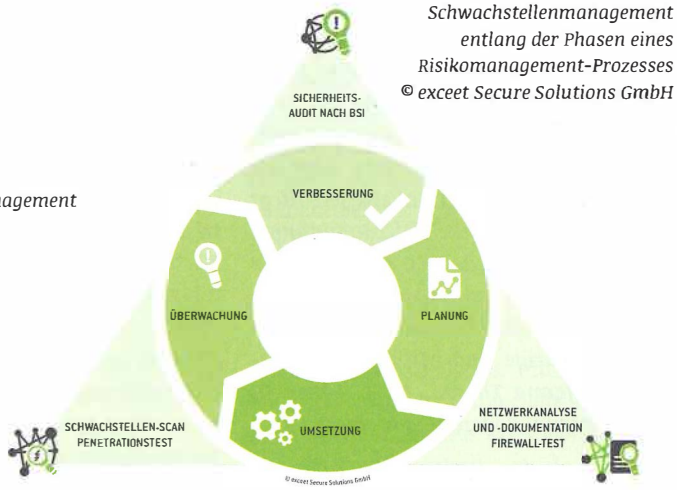
Neben der Erarbeitung eines individuellen Risikomanagements ist die Einführung eines geeigneten Schwachstellen-Managements zu empfehlen. Angesichts limitierter Budgets und Ressourcen gilt es zu ermitteln, wo potenzielle Schwachstellen liegen, welche Sicherheitsrisiken konkret damit verbunden sind und welcher Schutzbedarf im Einzelnen besteht. Während sich also das Risikomanagement vor allem auf organisatorische und prozessuale Aspekte bezieht, zielt das Schwachstellen-Management in jeder Phase des Risikomanagements zusätzlich auf die Absicherung von IT-Infrastrukturen und -Netzwerke (vgl. Abb.).

Fazit:

Mit zunehmender Zahl digitaler Medizinprodukte und ihrer Vernetzung verändert sich auch die Bedrohungslage. Entscheidend ist daher, die neuen Anforderungen an die Sicherheit der IT-Infrastrukturen und IT-Netzwerke angemessen zu berücksichtigen und regelmäßig auf den Prüfstand zu stellen. Organisatorische und technische Aspekte sollten dabei dringend im Zusammenwirken betrachtet werden. Erst durch die Kombination von Risiko- und Schwachstellen-Management kann die Sicherheit patientenbezogener Daten, medizinischer Geräte sowie ihrer Einsatzumgebung vor Beeinträchtigungen garantiert und die Einhaltung der gesetzlichen Sorgfaltspflicht im Krisenfall gewährleistet werden.

White Paper: Risikomanagement mit DIN EN 80001

White Paper: ISO 27001 im Gesundheitswesen



Schwachstellenmanagement entlang der Phasen eines Risikomanagement-Prozesses
© exceet Secure Solutions GmbH