„Medizinprodukte in IT-Netzwerken“

Was die Normenfamilie IEC 80001 hier leisten kann

Dipl.-Ing. Volker SUDMANN

Informationstechnik ist in modernen Gesundheitseinrichtungen nicht mehr wegzudenken. IT-Netzwerke sind wie die Nervenverbindungen im Organismus eines Krankenhauses. Kommt es hier zu Problemen oder Unregelmäßigkeiten, kann dies gravierende und weitreichende Konsequenzen haben.

Als die Informationstechnik begann auch in das Krankenhaus vorzudringen, standen zunächst rein verwaltungstechnische Aufgaben im Vordergrund. Heute, im Internetzeitalter geht der Trend mehr und mehr dazu alle Arten von Geräten, insbesondere auch von medizinischen Geräten, in ein solches Netzwerk einzubinden. Damit steigen auch die Anforderungen an dieses komplexe Netzwerk, um den unterschiedlichen Erwartungen der Nutzer gerecht zu werden.

Diese zunehmende Vernetzung ganz unterschiedlicher Geräte und Anwendungen bringt gerade im Krankenhaus besondere Herausforderungen mit sich. So gibt es eine Vielzahl von Problemen, die erst dann entstehen, wenn man Medizinprodukte in IT-Netzwerke einbindet.

Zu dieser Art von Problemen gehören beispielsweise:

- Unzureichende Berücksichtigung von Risiken aus der Benutzung von IT-Netzwerken in der klinischen Bewertung von Medizinprodukten;
- Unzureichende Unterstützung durch die Hersteller von Medizinprodukten hinsichtlich der Einbindung Ihrer Produkte in IT-Netzwerke;
- Fehlerhafter Betrieb oder auch nur eine veränderte oder verringerte Leistungsfähigkeit von Medizinprodukten, die aus der Kombination, der im IT-Netzwerk miteinander verbundenen Komponenten und Geräte herrühren können;
- Fehlerhafter Betrieb, der durch die gemeinsame Anwendung von Medizinprodukte-Software neben allgemeinen Anwendungen im selben IT-Netzwerk entstehen kann;
- Grundsätzlicher Konflikt zwischen der für Medizinprodukte erforderlichen strikten Änderungskontrolle und der Notwendigkeit bei Bedrohungen des IT-Netzwerks von außen schnell reagieren zu müssen.

Wenn Probleme dieser Art entstehen, hat dies unter Umständen viele und auch weitreichende Konsequenzen. Wenn heute beispielsweise ein Patientenmonitor mit dem IT-Netzwerk verbunden wird um kritische Patientendaten zu Schwesternstützpunkt zu übertragen, kann ein Softwareupdate einer Verwaltungssoftware, die gar nichts mit dem Patientenmonitor zu tun hat, das Netz in einer Art und Weise belasten, dass der Alarm des Patientenmonitors nicht oder nur verzögert an den Schwesternstützpunkt übermittelt wird. Dabei werden Patienten unnötigen Risiken ausgesetzt und es können möglicherweise lebensbedrohende Situationen entstehen.

Eine Möglichkeit sich diesem Problemfeld zu nähern ist die Implementierung eines Risikomanagementprozesses für den Betrieb von IT-Netzwerken, in die Medizinprodukte eingebunden sind. Die Norm IEC 80001-1 „Anwendung des Risikomanagements für IT-Netzwerke die Medizinprodukte beinhalten“ ist eine Anleitung dazu, wie Risikomanagement eingesetzt werden kann, um einen sicheren Betrieb von Medizinprodukten in einem IT-Netzwerk zu ermöglichen. Diese Aufgabe kann nicht allein vom Betreiber des IT-Netzwerks geleistet werden. Daher richtet sich diese Norm nicht ausschließlich an die für den Betrieb von IT-Netzwerken verantwortlichen Organisationen, sondern gleichermaßen an die Hersteller von Medizinprodukten und die Anbieter von Informationstechnik.

Mit der Anwendung der Norm IEC 80001-1 wird ein Risikomanagementprozess implementiert, mit dem erreicht werden kann, dass die Risiken, die sich aus dem Betrieb von Medizinprodukten in IT-Netzwerken ergeben, erkannt, bewertet und auf ein vertretbares Maß reduziert werden. Dieser Risikomanagementprozess soll ermöglichen, dass die Schutzziele „Sicherheit“ (Safety), in Bezug auf die Sicherheit von Patienten, Anwendern und Dritten und „Daten- und Systemsicherheit“ (Security) erreicht werden.

Um die Implementierung des Risikomanagementprozesses angehen zu können, werden in dieser Norm zuerst einmal die Aufgaben und Verantwortlichkeiten der Betreiber, der Medizinproduktehersteller und der Hersteller von Informationstechnik beschrieben. Die Umsetzung des Risikomanagements obliegt einem Med-IT-Risikomanager, dessen Funktion ebenfalls in der Norm beschrieben wird. Dieser Med-IT-Risikomanager nimmt in der betreibenden Organisation eine ganz zentrale Rolle ein.

So ist er unter anderem verantwortlich für:

- die Zusammenstellung risikorelevanten Informationen zu den vernetzten Medizinprodukten;
- die Planung der Einbindung von Medizinprodukten, gemäß den Angaben der Hersteller und in Übereinstimmung mit den Richtlinien der betreibenden Organisation, in das IT-Netzwerk;
- die Durchführung des Risikomanagements im Rahmen der Konfigurations- und Änderungsprozesse für das IT-Netzwerk;

- die Autorisierungen für den Echtbetrieb nach Änderungen im IT-Netzwerk;
- die Information der Leitung der betreibenden Organisation über unvertretbare Risiken;
- die Überwachung aller Projekte oder Veränderungen im IT-Netzwerk, für das er als Med-IT-Risikomanager verantwortlich ist.

Der Aufbau und Aufrechterhaltung der erforderlichen Kommunikation zwischen den internen und externen Teilnehmern am Risikomanagement ist für den Erfolg des Risikomanagement essentiell und eine der zentralen Aufgabe des Med-IT-Risikomanagers. So sollten in den Risikomanagementprozess beispielsweise folgende Teilnehmer eingebunden werden:

- die Hersteller von Medizinprodukten;
- die Lieferanten von Informationstechnik, Software und IT-Dienstleistungen;
- die eigene IT-Abteilung;
- der eigene technische Service für Medizinprodukte, z.B. die Medizintechnikabteilung;
- andere Abteilungen der betreibenden Organisation wie z.B. das Gebäude Management;
- die klinischen Anwender.

Der Med-IT-Risikomanager stellt sicher, dass der von ihm betreute Risikomanagementprozess über die gesamte Lebensdauer des medizinischen IT-Netzwerkes und der darin befindlichen Komponenten aufrechterhalten wird.

Diese Norm richtet sich, wie schon gesagt, aber ebenso an die Hersteller von Medizinprodukten. Diese müssen für die betreibenden Organisationen Informationen bereitstellen, die den sicheren und effektiven Betrieb der Medizinprodukte in einem IT-Netzwerk ermöglichen.

Zu dieser Art Information gehören unter anderem:

- der Zweck der Einbindung der Medizinprodukte in das IT-Netzwerk;
- die Anforderungen an das IT-Netzwerk hinsichtlich seine Eigenschaften und Leistungsmerkmale;
- die erforderliche Konfiguration des IT-Netzwerkes;
- die technischen Spezifikationen sowie die „Security“-Spezifikationen der Netzwerkanbindung;
- den vorgesehenen Informationsfluss zwischen Medizinprodukt, IT-Netzwerk und anderen Geräten und Software im Netzwerk;
- eine Übersicht über die Gefährdungssituationen, die entstehen können, wenn das IT-Netzwerk nicht die erforderlichen Eigenschaften oder Leistungsmerkmale aufweist.

Der sichere Betrieb von Medizinprodukten in einem IT-Netzwerk ist ein weites und komplexes Feld. Er fordert von allen beteiligten ein hohes Maß an Entgegenkommen und Einsicht in die Problem und Notwendigkeiten der für ein wirksames Risikomanagement beteiligten Partner. Für alle Beteiligten stellen sich eine Reihe von Fragen, die auf einen befriedigende Antwort warten und es zeigen sich Probleme, die gelöst werden müssen. Dies wurde auch in den Normungsorganisationen erkannt. So sind bereits neben der Grundnorm

IEC 80001-1 Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten - Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten

eine Reihe von Leitfäden erschienen, die sich mit der Umsetzung der IEC 80001 im Detail beschäftigen:

IEC/TR 80001-2-1 Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten - Teil 2-1: Schritt-für-Schritt-Risikomanagement von medizinischen IT-Netzwerken - Praktische Anwendung und Beispiele

IEC/TR 80001-2-2 Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten - Teil 2-2: Leitfaden zur Angabe von Bedingungen für die Kommunikationssicherheit von Medizinprodukten, Risiken und Risikobeherrschung

IEC/TR 80001-2-3 Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten - Teil 2-3: Leitfaden für drahtlose Netzwerke

IEC/TR 80001-2-4 Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten - Teil 2-4: Anwendungsleitfaden - Allgemeine Empfehlung zur Implementierung für Gesundheitseinrichtungen

OVE-Richtlinie/ONR R 8 Leitfaden für die Beschaffung und den Betrieb von Medizinprodukten in IT-Netzwerken.

Weitere Leitfäden werden derzeit erarbeitet und liegen zum Teil bereits als Entwurf vor:

IEC/TR 80001-2-5 Application of risk management for IT-networks incorporating medical devices - Part 2-5: Application guidance - Guidance on distributed alarm systems

IEC/TR 80001-2-6 Application of risk management for IT-networks incorporating medical device - Part 2-6: Application guidance - Guidance for responsibility agreements

IEC/TR 80001-2-7 Application of risk management for IT-networks incorporating medical devices - Application guidance - Part 2-7: Guidance for Healtcare Delivery Organizations (HDOs) on how to selfassess their conformance with IEC 80001-1

IEC/TR 80001-2-8 Application of risk management for IT-networks incorporating medical devices - Application guidance - Part 2-8: Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2

TÜV AUSTRIA SERVICES GMBH
Dipl.-Ing. Volker SUDMANN
volker.sudmann@tuv.at

TÜV AUSTRIA