



Problempatient IT-Sicherheit?

Ansätze zum ISMS in medizinischen Einrichtungen

Für Krankenhäuser und kritische Infrastrukturen der Gesundheitsversorgung in Deutschland greift der klassische Grundschutz-Ansatz zu kurz, meint unser Autor: Denn die Ausrichtung auf die klassische IT-Sicherheit unterschlägt wichtige Aspekte der Sicherheit von Patienten und Anwendern. Details und Auswege beleuchtet der vorliegende Beitrag.

Von *Frederik Humpert-Vrielink, Schüttorf*

Die informationstechnische Infrastruktur eines Krankenhauses zu steuern gleicht dem Versuch, alle Zootiere davon zu überzeugen sich freiwillig ruhig zu verhalten und die Tierpfleger nicht zu beißen. Anders als in der produzierenden Industrie fällt es dem Unternehmen Krankenhaus schwer, seine IT-Infrastruktur außerhalb der Verwaltungssysteme mittels einer Strategie zu standardisieren und die eingesetzten Plattformen zu harmonisieren.

Das liegt schwerpunktmäßig daran, dass medizinisches Personal regelmäßig neue und aktuelle Medizinprodukte benötigt, deren Einbindung in das IT-Netz eine große Herausforderung darstellt. Zusätzlich unterliegen Medizinprodukte einem Zulassungsprozess [1] und sind nur in einer bestimmten Konfiguration am Markt verfügbar. Auch dieser Umstand erschwert es, Informationssicherheit in einem Krankenhaus nach klassischen Regeln umzusetzen – zumeist werden daher die Bereiche der Medizinprodukte und der Informationstechnik getrennt voneinander betrachtet (vgl. Abb. 1).

Der Versuch, die Sicherheit dieser Infrastruktur mit den klassischen Ansätzen der IT-Sicherheit zu erhöhen, muss denn auch scheitern oder sich zumindest auf

die informationsverarbeitende Verwaltungsinfrastruktur eines Krankenhauses beschränken. Dies liegt nicht zuletzt an der Ausrichtung der anerkannten Normen des Informationssicherheitsmanagements. Der BSI-Standard 100-2 [4] ist für standardisierte technische Einsatzszenarien gedacht: Gemeinsam mit den weiteren BSI-Standards ist der IT-Grundschutz regelmäßig dort einsatzfähig, wo keine starken regulatorischen Anforderungen auf Teile der IT-Infrastruktur einwirken. Damit ergibt sich jedoch automatisch, dass sich dieser Ansatz beim Einsatz von Medizinprodukten in IT-Netzen nicht oder nur in Teilen eignet.

Auch die einzelne Anwendung der ISO/IEC 27001 [5] oder verwandter Normen der ISO-Familie greift zu kurz: Denn die in diesen Normen definierten Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität (das sog. „C-I-A-Paradigma“ bzgl. der Ziele Confidentiality – Integrity – Availability) decken nur einen Bruchteil dessen ab, was in einem Krankenhaus an Sicherheitszielen umzusetzen ist. Nicht nur, weil die C-I-A-Schutzziele im Krankenhaus nicht ausreichen, sondern auch, weil die rechtlichen Rahmenbedingungen dort die klassische Einbindung in Methoden der IT- oder Informationssicherheit wie Patch- und Updatemanagement nicht zulassen (vgl. Kasten).

Neue Ansätze

Es ist daher Zeit, über andere Ansätze zu diskutieren, die ein integriertes Management der Informationssicherheit im Krankenhaus ermöglichen. Vielversprechend erscheint hierbei eine Kombination der klassischen Managementsystemmethode mit einer Methodik, die das Risikomanagement für IT-Netze mit Medizinprodukten beleuchtet – Letztere liegt in Form der IEC 80001-1 [6] vor.

Die Norm IEC 80001-1:2001 „Risikomanagement für IT-Netzwerke mit Medizinprodukten“ verfolgt im Gegensatz zu klassischen Managementsystemen einen Ansatz, der auf der Kommunikation und Verantwortungsteilung zwischen Herstellern und Anwendern von Medizinprodukten basiert. Dies trägt den Vorgaben Rechnung, dass Änderungen an Medizinprodukten, nachdem diese genehmigt und zugelassen wurden, nur durch Hersteller vorgenommen werden dürfen – die juristischen Dimensionen des Betriebs eines IT-gestützten Medizinproduktes sind im ## nebenstehenden Kasten kurz erläutert.

Dabei weist die IEC 80001-1 einige Parallelen zur ISO-20000-Familie [8] auf – das macht die Norm für ein

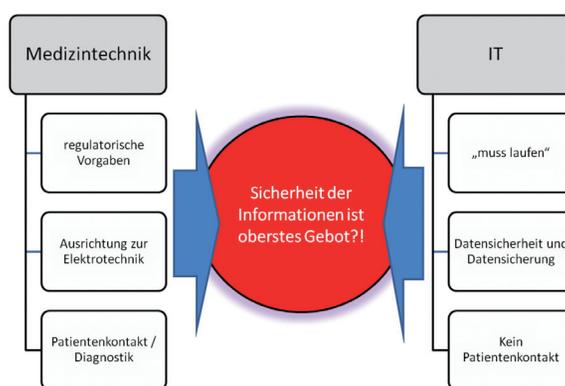


Abbildung 1: Medizintechnik und IT bilden in Krankenhäusern zwei nebeneinander liegende Inseln

komplettes, integriertes Managementsystem auf Basis der ISO 27001 in einem Krankenhaus gut anwendbar. Zusätzlich zu diesen IT-Management-Parallelen definiert die IEC 80001-1 eigene Schutzziele für den Betrieb von IT-Netzwerken mit Medizinprodukten. Diese sind

- _____ **Safety**, also vorrangig die Sicherheit von Patienten oder Dritten bei Einsatz eines Medizinprodukts,
- _____ **Effectiveness**, was hier die korrekte Bereitstellung von korrekten Informationen zu rechten Zeit am

Rechtliches zu ISMS im Gesundheitswesen

Der Betrieb von IT-Netzwerken mit Medizinprodukten ist herausfordernd sowohl für die Organisation als auch die IT-Strategie. Gerade der Bereich der IT-Compliance wird durch gesetzliche Regelungen berührt, insbesondere durch:

- _____ die „Medical Device Directive“ (MDD, EU-Richtlinie 93/42/EWG) [7],
- _____ das Medizinproduktegesetz (MPG) [1] und
- _____ die Medizinprodukte-Betreiberverordnung (MP-BetreibV) [2].

Dies erschwert im Rahmen einer ISMS-Einführung die Einbindung der Medizinprodukte in die Gesamt-Sicherheitsstrategie. Zunächst ist zu betrachten, was genau als Medizinprodukt zählt und was nicht: Gemäß Medizinproduktegesetz (§ 3I MPG) und MDD (Art. 1 Abs. 2 Buchst. a) sind Medizinprodukte „... einzeln oder miteinander verbunden verwendete Instrumente, ... Software, ... und für ein einwandfreies Funktionieren des Medizinproduktes eingesetzte[n] Software...“, die einem bestimmten Zweck dienen.

So ergibt sich ein weiterer Bereich: Betriebssystem und installierte Produkte sind mit Sicherheit für ein einwandfreies Funktionieren des Medizinproduktes notwendig. Diese Plattform und alle verbundenen Komponenten – auch Hardware – werden damit automatisch mit erfasst.

ISMS-Strukturen und IT-Sicherheitsmaßnahmen greifen Sicherheitslücken über Eingriffe in das Betriebssystem, bestehende Netzstrukturen oder einfache Updates und Patches auf. Dies funktioniert in „klassischen“ homogenen Umgebungen sehr gut, wirft aber aus rechtlichen Gründen im Krankenhaus Schwierigkeiten auf: Denn zugelassene und mit der CE-Kennzeichnung versehene Medizinprodukte sind einer Baumusterprüfung (gem. Anhang III MDD) unterzogen worden. Diese basiert auf einer technischen Dokumentation, die eine allgemeine Beschreibung enthält. Und hier wird unter anderem auf eingesetzte Software und verwendete Versionen verwiesen, um die gleichzeitig geforderte Risikoanalyse liefern zu können und Interoperabilitätstests nachweisen zu können.

Greift nun ein Betreiber (z. B. ein Krankenhaus) über ein nicht vom Hersteller autorisiertes Sicherheitsupdate oder einen Patch ein, verändert er die Struktur des Produkts. Damit wandelt er gleichzeitig seine Rolle vom Betreiber zum Hersteller des Medizinprodukts und müsste fortan alle Anforderungen der MDD erfüllen, die sich an Hersteller richten. Dies wird für die meisten Betreiber von Medizinprodukten eine nicht zu erfüllende Aufgabe sein. ## Im Umkehrschluss sind alternative Ansätze zum ganzheitlichen Risikomanagement für Krankenhaus-IT gefordert.

rechten Ort bedeutet (damit also eine Kombination aus Verfügbarkeit und Integrität) sowie

_____ **Security**, also die allgemeine Datensicherheit, die in der ISO 27001 unter den Schutzzielen Verfügbarkeit, Vertraulichkeit und Integrität abgebildet wird.

Diese Sicherheitsziele ergeben sich aus dem rechtlichen Rahmen für den Betrieb von Medizinprodukten: Einerseits dürfen solche Produkte aufgrund der Medizinproduktebetrieberverordnung (§2 (3) MPBetreibV [2]) nur angewendet werden, wenn sie unter Berücksichtigung der Sicherheit der Patienten geeignet sind – andererseits ist es gesetzlich verboten, Medizinprodukte in Verkehr zu bringen, welche die Sicherheit der Patienten oder Dritter beeinträchtigen könnten (§ 4 (1) MPG [1]).

Integriertes ISMS

Ein moderner Ansatz des Informationssicherheits-Managements in ## medizinischen Einrichtungen verbindet somit zweckmäßigerweise die Normen ISO/IEC 27001 [5] und IEC 80001-1 [6], nutzt Synergien und berücksichtigt die Unterschiede sowie die Anforderungen der Gesetzgebung für Hersteller und Betreiber von Medizinprodukten.

Wichtigster Aspekt dieses Ansatzes ist es, den in der ISO/

IEC 27001 beschriebenen Plan-Do-Check-Act-(PDCA)-Zyklus vollständig zu durchlaufen. Auch die umgebenden Variablen des ISMS müssen dazu vollständig – wie in der Norm definiert – umgesetzt werden, zum Beispiel

- _____ interne Audits,
- _____ Korrektur- und Vorbeugemaßnahmen,
- _____ Controls aus dem Annex A,
- _____ Management-Reviews,
- _____ Schulung und Ausbildung sowie eine
- _____ Methodik zur Risikoanalyse

Parallel dazu wird im Herzstück des ISMS bei der Risikoanalyse die Methodik aufgespalten (vgl. Abb. 2). Dies bedeutet hier, bereits auf der Ebene der anwendbaren Risikoanalysenormen klare Unterschiede herauszuarbeiten und in den entsprechenden Dokumenten zu beschreiben. So entstehen zwei Richtlinien für Risikoanalysen: für den klassischen IT-Teil und für den IT-Teil mit Medizinprodukten.

Für den Verwaltungsteil der Infrastruktur eines Krankenhauses ist es zielführend, eine klassische Risikoanalyse zur Informationssicherheit vorzunehmen. Dies betrifft besonders diejenigen „kritischen Werte“ an Informationen, welche die Bereiche

- _____ kaufmännisches Rechnungswesen,

- _____ Personalverwaltung und
- _____ allgemeine Verwaltung umfassen.

Ob und wie stark das klinische Informationssystem (KIS) in den Verwaltungsteil des ISMS einbezogen wird, ist ein strittiger Punkt: Je nach Betrachtungsweise der Rechtsvorgaben könnte man das KIS auch als Medizinprodukt bewerten. Hilfreich ist hier der Rückgriff auf die so genannte „Medical Device Directive“ [9]: Ihr zufolge unterläge der Betrieb eines KIS den Rechtsnormen für den Betrieb von Medizinprodukten, insbesondere der Medizinproduktebetrieberverordnung [2] – dies schlosse dann eine problemlose Integration in die klassischen ISMS-Maßnahmen aus. Hieraus können bei unkoordinierter Steuerung große Sicherheitslücken entstehen. Um das zu vermeiden, sollte das KIS in Zweifelsfällen daher immer als Medizinprodukt gewertet werden – weniger aus Sicht der IT- oder Informationssicherheit als aus dem Blickwinkel der rechtlichen Konformität heraus.

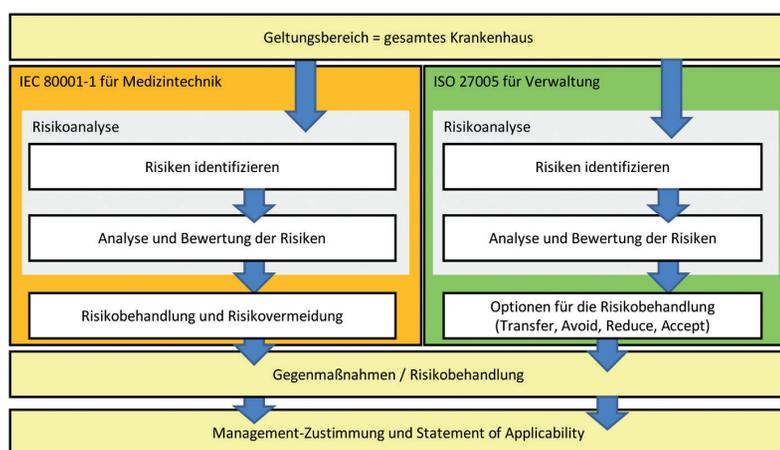
Bei den problemlos zum Bereich der Verwaltungssysteme zählenden Systemen kommt zur Bewertung von Risiken fast immer das klassische Modell „Transfer–Avoid–Reduce–Accept“ (TARA) zum Einsatz.

Spezifische Risikoanalyse

Für den Teil des Netzwerks, der Medizinprodukte umfasst, ist hingegen eine gesonderte Art der Risikoanalyse vorzunehmen: Auf Basis der IEC 80001-1 [6] werden dazu die besonderen Aspekte beim Einsatz von Medizinprodukten beleuchtet und analysiert. Diese umfassen nicht nur die rein informationstechnischen Auswirkungen auf den Netzbetrieb, sondern besonders auch das Vorgehen bei erkannten oder bereits bekannten Risiken.

Dabei berücksichtigt die Norm nicht nur die internen Pro-

Abbildung 2: IEC 80001-1 und ISO 27001 als Teamplayer für ein integriertes ISMS in medizinischen Einrichtungen



zesse, sondern auch die Verantwortung der Hersteller von Medizinprodukten für die Sicherheit bei der Einbindung in das Netz. Die Norm verlangt neben einer Risikoanalyse auch, den Hersteller eines Medizinprodukts, das in die Infrastruktur eingebunden werden soll, mit in die Pflicht zu nehmen und die Verantwortung entsprechend aufzuteilen.

Aus dieser spezifischen Risikoanalyse erwachsen analog zur „normalen“ Risikoanalyse Risiken, die zu bewerten sind: Es ist darauf zu achten, dass bei Risiken, welche die Patientensicherheit (Safety) betreffen, eine Risikoübernahme grundsätzlich ausgeschlossen werden sollte. Bei den anderen oben genannten Schutzgütern ist auf der Basis von Szenarien zu ermitteln, wie mit Risiken umgegangen werden soll. Dabei kann die Entscheidung sowohl von der Geschäftsführung des Krankenhauses als auch vom medizinischen Personal beeinflusst werden.

Mehr als Informationen

Die ISO 27001 [5] legt ihren Fokus rein auf die verarbeiteten Informationen. Dabei steht der Datenschutz im Vordergrund, besonders gekennzeichnet im Schutzgut der Vertraulichkeit, aber auch in den spezifischen Ausprägungen zur praktischen Umsetzung, wie sie beispielsweise für das Gesundheitswesen in der ISO 27799-10 [7] detailliert beschrieben sind.

Dennoch entstammt dieser Ansatz der „reinen Lehre“ der IT-Sicherheit und greift aus den oben beschriebenen Gründen im Gesundheitswesen massiv zu kurz. Auch die deutsche Ausprägung in Form des BSI-„ISMS-Standards“ 100-1 [3] versucht, über verschiedene Wege Eingang in das deutsche Gesundheitswesen zu finden. Doch auch diese Methodik greift zu kurz –deutlich wird das gerade beim IT-Grundschutz allem voran in der starken Betonung technischer Maßnahmen der IT-Sicherheit.

Wie bereits in der Betrachtung der rechtlichen Rahmenbedingungen für den Betrieb von Medizinprodukten (siehe Kasten) ausgeführt, ist ein Medizinprodukt nur dann verwendbar, wenn es den Zulassungskriterien entspricht. Dabei sind regelmäßig auch die verwendete Software, das verwendete Betriebssystem sowie mitgelieferte Virens Scanner oder sonstiges Bestandteile fester Teil des zugelassenen Produktes.

Die klassischen Ansätze der IT-Sicherheit verlangen von Betreibern und Unternehmen einen durchgängigen Prozess sowie in hohem Maße homogene technische Systeme beispielsweise für Patch- und Updatemanagement einzuführen. Würde diese Betrachtung auch für die Medizinprodukte gelten, käme ein Krankenhaus sehr schnell in schwieriges Fahrwasser: Gegebenenfalls

Literatur

[1] Gesetz über Medizinprodukte (Medizinproduktegesetz – MPG), www.gesetze-im-internet.de/mpg

[2] Verordnung über das Errichten, Betreiben und Anwenden von Medizinprodukten (Medizinprodukte-Betreiberverordnung – MPBetreibV), www.gesetze-im-internet.de/mpbetreibv/

[3] BSI-Standard 100-1, IT-Grundschutz – Managementsysteme für Informationssicherheit (ISMS), Version 1.5, 2008, www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

[4] BSI-Standard 100-2, IT-Grundschutz-Vorgehensweise, Version 2.0, 2008, www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

[5] DIN ISO/IEC 27001:2005, Informationstechnik- IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen, erhältlich über www.din.de

[6] DIN EN 80001-1:2010 / VDE 0756-1:2011-11, Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten – Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten, erhältlich über www.din.de

[7] DIN EN ISO 27799, Medizinische Informatik – Sicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002, erhältlich über www.din.de

[8] ISO/IEC TR 20000-x, Information Technology – Service Management, erhältlich via www.iso.org/iso/store.htm

[9] Richtlinie 93/42/EWG des Rates vom 14. Juni 1993 über Medizinprodukte (Medical Device Directive), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31993L0042:DE:NOT>

[10] Reinhard Voßbein, IT-Sicherheitsstandards im Gesundheitssektor – Entwicklungen und Besonderheiten, <kes> 2010#6, S. 50

[11] Robert Vattig, Marco-Antonio Retzlaff, Walter Swoboda, Ali Sunyaev, Grundschutz im Klinikum, Praxisbericht zum Einsatz von IT-Grundschutz an einem bayerischen Universitätsklinikum, <kes> 2011#1, S. 70

würden „eigenmächtig“ durchgeführte Änderungen an Medizinprodukten – auch wenn sie der Sicherheitsstrategie entsprechen – das Medizinprodukt seine Zulassung verlieren lassen und das Krankenhaus in der Folge ein nicht zugelassenes Produkt betreiben.

Fazit

Gerade weil das Gesundheitswesen durch eine hohe Dynamik gekennzeichnet ist, erscheint ein konsequent gesteuertes ISMS sinnvoll und auch notwendig. Vor allem im Zuge der Einführung der Gesundheitskarte und vernetzter Abrechnungssysteme sind hier steigende Anforderungen zu erwarten (vgl. [10]). Dennoch ist ein Fokus auf die von Vertraulichkeit und Integrität getriebenen Normen der Informationssicherheit nicht ausreichend – eine ganzheitliche Sicherheitspolitik darf die Besonderheiten der Medizintechnik nicht vergessen.

Eine Weiterentwicklung der Informationsverarbeitung im Rahmen der Krankenhäuser wird gerade in Zukunft eine immer stärker konvergierende Landschaft von klassischer IT und Medizinprodukten hervorbringen. Versäumnisse auf dieser Ebene dürften sicherlich die größten Schwachstellen nach sich ziehen, die ein Sicherheitskonzept im Krankenhaus haben kann – nicht zuletzt, weil Sicherheitsprobleme bei eingesetzter Medizintechnik konkrete Auswirkungen auf Leib und Leben der Patienten haben können.

Wo man kritischen Infrastrukturen der Gesundheitsversorgung Hinweise und Hilfestellung zu IT-Sicherheit und Notfallmanagement gibt, darf man Medizinprodukte im IT-Netz nicht nur als „Black Box“ begreifen. Vor diesem Hintergrund ist auch zu hoffen, dass aktuelle Projekte (z. B. zur „Risikoanalyse Krankenhaus IT“ – RiKrIT) hier zeitnah notwendige Ergänzungen und Verbesserungen erfahren. ■

Frederik Humpert-Vrielink, CETUS Consulting GmbH, Schüttorf