SYSTEMINFRASTRUKTUR IN KRANKENHÄUSERN

Problempatient IT-Sicherheit

Dieser Beitrag skizziert ein Modell, wie ein Sicherheitsmanagement auf der Basis der ISO/IEC 27001:2013 kombiniert mit der IEC 80001-1:2011 Krankenhäusern ermöglicht, Sicherheit zu steuern und herzustellen.

Aus Sicht der IT-Strategie ist Informationsverarbeitung im Krankenhaus oft ein großer Zoo ohne homogene Strukturen und Systeme. Im Gegensatz zur produzierenden Industrie fällt es Krankenhäusern zumeist schwer, die Infrastruktur außerhalb der Verwaltungssysteme mittels einer Strategie zu standardisieren und die eingesetzten Plattformen zu harmonisieren.

Dies liegt im Schwerpunkt daran, dass das medizinische Personal regelmäßig neue und aktuelle Medizinprodukte benötigt, deren Einbindung in das IT-Netz eine große Herausforderung darstellt. Zusätzlich sind Medizingeräte nur in einer bestimmten Konfiguration am Markt verfügbar. Auch dieser Umstand erschwert es, Informationssicherheit in einem Krankenhaus nach klassischen Regeln umzusetzen. Daher werden hier die Bereiche Medizintechnik und IT noch zu häufig getrennt betrachtet und geführt.

Das führt dazu, dass der Versuch, die Sicherheit dieser Infrastruktur mit den klassischen Ansätzen der IT-Sicherheit zu erhöhen, scheitert oder zumindest auf die informationsverarbeitende Verwaltungsinfrastruktur eines Krankenhauses begrenzt bleibt. Dies liegt nicht zuletzt an der Ausrichtung der anerkannten Normen des Informationssicherheitsmanagements in Deutschland. Die Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sind für standardisierte technische Einsatzszenarien gedacht. Sie sind dort einsatzfähig, wo keine starken regulatorischen Anforderungen auf Teile der IT-Infrastruktur einwirken. Damit ergibt sich jedoch automatisch, dass dieser Ansatz beim Einsatz von Medizinprodukten in IT-Netzen nicht oder nur in Teilen geeignet ist. Daher hat das BSI in seinem Projekt RiKrIT auch auf die Einbindung der Medizingeräte verzichtet. Auch die einzelne Anwendung der ISO/IEC 27001 oder verwandter Normen der ISO-Familie greift zu kurz. Die in diesen Normen definierten Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität (C-I-A-Paradigma) decken nur einen Bruchteil dessen ab, was in einem Krankenhaus an Sicherheitszielen umzusetzen ist. Nicht nur, weil das C-I-A-Paradigma im Krankenhaus nicht ausreicht, sondern auch, weil die rechtlichen Rahmenbedingungen keine Einbindung in Methoden der IT- oder Informationssicherheit wie Patch- und Updatemanagement zulassen.

ZEIT FÜR NEUE ANSÄTZE

Es ist also Zeit, über andere Ansätze zu diskutieren, die ein integriertes Management der Informationssicherheit im Krankenhaus ermöglichen. Vielversprechend ist hier eine Kombination der klassischen Managementsystemmethode mit einer Methodik wie der DIN EN 80001-1, die das Risikomanagement für IT-Netze mit Medizinprodukten beleuchtet.

Diese Norm verfolgt im Gegensatz zu den klassischen Managementsystemen einen Ansatz, der auf der Kommunikation und Verantwortungsteilung zwischen Herstellern und Anwendern von Medizinprodukten basiert. Damit trägt sie den Vorgaben Rechnung, dass Änderungen an Medizinprodukten nur durch Hersteller vorgenommen werden dürfen, nachdem diese geprüft sind.

Dabei weist die DIN EN 80001 Schnittstellen zur ISO-20000-Familie auf. Vor allem dieser Umstand macht diese Norm gut anwendbar, um in ein komplettes Managementsystem für Informationssicherheit in einem Krankenhaus integriert zu werden. Zusätzlich zu den IT-Management-Parallelen definiert die DIN EN 80001-1 eigene Schutzziele für den Betrieb von IT-Netzwerken mit Medizinprodukten. Diese sind:

- Safety: die Sicherheit des Patienten oder Dritter bei Einsatz des Medizinproduktes.
- Effectiveness: die korrekte Bereitstellung von korrekten Informationen zur rechten Zeit am rechten Ort.
- Security: die allgemeine Datensicherheit, die in der ISO/IEC 27001:2013 unter den Schutzzielen Verfügbarkeit, Vertraulichkeit und Integrität abgebildet wird.

Diese Sicherheitsziele ergeben sich aus dem rechtlichen Rahmen für den Betrieb von Medizinprodukten. Einerseits dürfen Medizinprodukte nach § 2 (3) Medizinprodukte-Betreiberverordnung (MPBetreibV) nur angewendet werden, wenn sie dazu unter Berücksichtigung der Sicherheit der Patienten geeignet sind. Andererseits ist es entsprechend § 4 (1) Absatz 1 Medizinproduktegesetz (MPG) verboten, Medizinprodukte in Verkehr zu bringen, die die Sicherheit der Patienten oder Dritter beeinträchtigen könnten.

INTEGRIERTES ISMS

Ein moderner Ansatz des Managements der Informationssicherheit in einem Krankenhaus verbindet die o.g. Normen, 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 27001:2013 beschriebenen PDCA-Zyklus (Plan-Do-Check-Act) vollständig zu durchlaufen. Auch die umgebenden Variablen des Information-Security-Management-Systems (ISMS), so z.B.

- interne Audits,
- Korrektur-/Vorbeugemaßnahmen,

- Controls aus dem Annex A,
- Management Review,
- Schulung und Ausbildung sowie
- Methodik zur Risikoanalyse

werden vollständig wie in der Norm definiert umgesetzt. Parallel hierzu wird im Herzstück des ISMS, bei der Risikoanalyse, die Methodik aufgespalten. Dies bedeutet, bereits auf der Ebene der anwendbaren Risikoanalysenormen klare Unterschiede herauszuarbeiten und in den entsprechenden Dokumenten zu beschreiben. Damit entstehen zwei Richtlinien für Risikoanalysen – für den klassischen IT-Teil und für den IT-Teil mit Medizinprodukten.

Für den Verwaltungsteil der Infrastruktur ist es zielführend, eine klassische Risikoanalyse zur Informationssicherheit vorzunehmen. Dies betrifft besonders diejenigen „kritischen Werte" an Informationen, die die Verwaltungsbereiche umfassen. Hier würde sich auch das KIS wiederfinden. Das KIS sollte jedoch einer besonders intensiven Schnittstellenanalyse unterzogen werden, so dass alle Risiken für Diagnoseinformationen und deren Übermittlung erfasst werden. Die Bewertung der Risiken nach dem Modell Transfer-Avoid-Reduce-Accept (TARA) erfolgt mittels einer definierten Bewertungsgrundlage. Für den Teil des Netzwerkes, der Medizinprodukte umfasst, ist eine gesonderte Art der Risikoanalyse vorzunehmen.

Auf Basis der DIN EN 80001-1 werden die besonderen Aspekte beim Einsatz von Medizinprodukten beleuchtet und analysiert. Diese umfassen nicht nur die rein IT-technischen Auswirkungen auf den Netzbetrieb, sondern insbesondere das Vorgehen bei erkannten oder bereits bekannten Risiken. Dabei berücksichtigt die Norm nicht nur die internen Prozesse, 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 Medizinproduktes, das in die Infrastruktur eingebunden werden soll, mit in die Pflicht zu nehmen und die Verantwortung entsprechend aufzuteilen.

Aus dieser Risikoanalyse erwachsen analog zur normalen Risikoanalyse Ergebnisse, die bewertet werden müssen. Hierbei ist darauf zu achten, dass bei Risiken, die die Safety, also die Patientensicherheit betreffen, eine Risikoübernahme grundsätzlich ausgeschlossen werden sollte. Bei den anderen oben genannten Schutzgütern ist ebenfalls auf Basis von Szenarien zu ermitteln, wie mit diesen Risiken umgegangen werden soll. Dabei kann die Entscheidung sowohl von der Geschäftsführung als auch vom medizinischen Personal beeinflusst werden.

„Gerade weil das Gesundheitswesen durch eine hohe Dynamik gekennzeichnet ist, ist ein konsequent gesteuertes ISMS sinnvoll und notwendig."
NINA VRIELINK

INFORMATIONEN IM FOKUS

Die Basis dieser Diskussion, die ISO 27001, legt den Fokus rein auf die Informationen, die im Gesundheitswesen verarbeitet werden. Dieser Ansatz stammt aus der reinen Lehre der IT-Sicherheit. Aus den oben beschriebenen Gründen greift er jedoch zu kurz. Auch die deutsche Ausprägung BSI-Standard 100-1 versucht, über verschiedene Wege Eingang in das deutsche Gesundheitswesen zu finden. Diese Methodik greift jedoch ebenfalls zu kurz. 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. Sofern diese durchgängige Betrachtung auch für die Medizinprodukte gelten würde, käme ein Krankenhaus sehr schnell in schwieriges Fahrwasser. Gegebenenfalls würde bei eigenmächtig durchgeführten Änderungen an Medizinprodukten – auch wenn sie der Sicherheitsstrategie entsprechen – das Krankenhaus zum Eigenhersteller mit allen Konsequenzen.

FAZIT

Gerade weil das Gesundheitswesen durch eine hohe Dynamik gekennzeichnet ist, ist ein konsequent gesteuertes ISMS sinnvoll und notwendig. Vor allem im Zuge der Einführung der Gesundheitskarte und vernetzter Abrechnungssysteme sind hier steigende Anforderungen zu erwarten. Dennoch ist ein Fokus auf die von Vertraulichkeit und Integrität getriebenen Normen der Informationssicherheit nicht ausreichend. Die ganzheitliche Sicherheitspolitik darf die 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. Daher sind Versäumnisse auf dieser Ebene sicherlich die größten Sicherheitslücken, die ein Sicherheitskonzept im Krankenhaus haben kann. Dies nicht zuletzt v.a. deswegen, weil Sicherheitsprobleme bei der eingesetzten Medizintechnik konkrete Auswirkungen auf Leib und Leben der Patienten haben können.

Der Ansatz des Bundesamtes für Sicherheit in der Informationstechnik, kritischen Infrastrukturen der Gesundheitsversorgung Hinweise zu IT-Sicherheit und Notfallmanagement zu geben, ist gut. Aber er ist nicht vollständig, sofern er Medizinprodukte im IT-Netz nur als „Black Box" begreift. Hier sind v.a. die Verbände gefragt, pragmatische Lösungen voranzutreiben, um Krankenhäusern Hilfestellung zu geben.

ONLINE EXKLUSIV

Präsentation zum Download

Eine ausführliche PowerPoint-Präsentation mit vielen anschaulichen Grafiken und Erläuterungen können sich *HCM*-Abonnenenten im Archivbereich dieser Ausgabe unter www.hcm-magazin.de herunterladen.

NINA VRIELINK

Geschäftsführerin, CETUS Consulting GmbH,
Kontakt: nina.vrielink@cetus-consulting.de

Foto: privat