EHEALTHCOM
Magazin für Health-IT, vernetzte Medizintechnik und Telemedizin

DIN EN 80001-1: Chancen und Potenziale für vernetzte Medizintechnik

Ein Expertenbeitrag von Armin Gärtner

Die DIN EN 80001-1 (Quelle 1) über die Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte enthalten, ist am 1.11.2011 als Weißdruck erschienen und kann somit als Regel der Technik angewendet werden.
Die Norm hat bereits im Vorfeld zu vielen Diskussionen und zu Fragestellungen sowohl von Betreibern als auch von Herstellern geführt, sodass dieser Beitrag die grundsätzliche Bedeutung, die Chancen und vor allem die Potenziale der DIN EN 80001 herausstellt und sinnvolle Ansätze zur initialen Umsetzung diskutiert.
Die Norm beinhaltet kein Kochrezept, das der Betreiber „einfach abarbeiten“ kann, sie stellt mehr die (komplexe) Aufforderung an Betreiber (und indirekt auch an Hersteller) dar, sich mit den Gefahren und Gefährdungen der Integration von Medizinprodukten in IT-Netzwerke und den daraus resultierenden Risiken für Patienten auseinanderzusetzen, um diese möglichst zu reduzieren respektive soweit wie möglich zu beherrschen. Somit bietet diese Norm dem Betreiber trotz des damit verbundenen Aufwandes etliche Chancen und Potenziale, die es im Sinne der Patientensicherheit und zum Vorteil eines Krankenhauses/Arztpraxis zu nutzen gilt.

1. Ausgangssituation und Entstehung der Norm

In den 90`er Jahren des vergangenen Jahrhunderts setzte die Digitalisierung der Medizintechnik als Konsequenz der Entwicklung der Computer- und Softwaretechnik in der Radiologie mit der Entwicklung des DICOM-Standards ein.
Heutige aktive Medizinprodukte wie Beatmungsgeräte, EKG-Schreiber, bildgebende Geräte im Ultraschall- und Radiologiebereich u. a. sind ohne Betriebssysteme, Software und Netzwerkanbindung gar nicht mehr vorstellbar.
Die moderne Medizintechnik besteht aus einem immer kleiner werdenden medizintechnischen „Hardwareteil“ mit zugleich zunehmender Bedeutung und wachsendem Anteil von IT-Applikationen (Software) und Netzwerkverbindung (Hardware und Infrastruktur).

Diagnostische und therapeutische Funktionen sowie Prozesse verlagern sich vom Stand-alone Medizinprodukt zunehmend in das IT-Netzwerk des Krankenhauses, indem immer mehr aktive Medizinprodukte ihre Daten über das IT-Netzwerk eines Krankenhauses senden, austauschen und auf Servern speichern. Es entstehen also sogenannte Med. IT-Netzwerke. Die folgenden Beispiele verdeutlichen diese Entwicklung:

Beispiel 1:
In der Ambulanz eines Krankenhauses werden EKG-Schreiber eingesetzt, um das Elektrokardiogramm von Patienten aufzuzeichnen, die z. B. über unklare Brustschmerzen klagen. Die EKG-Schreiber können die aufgezeichneten EKG über eine WLAN-Anbindung direkt an den Arbeitsplatz (Desktop) und/oder auf das Mobilgerät (Tablet) eines Kardiologen schicken, der die EKG-Aufzeichnungen befunden soll.

Bild 1: EKG-Übertragung über WLAN

Beispiel 2:
Linearbeschleuniger werden zur kurativen/palliativen Bestrahlung onkologischer Patienten eingesetzt. Sie werden von Bestrahlungsplanungssystemen (Software) gesteuert, die ihre Daten in Form von medizinischen Bilddaten z. B. aus dem PACS und/oder anderen bildgebenden Systemen in Form digitaler Daten über das Netzwerk erhalten.

1.1 Medizinisches IT-Netzwerk

DN EN 80001-1 definiert in Kapitel 2.16 ein Med.-IT-Netzwerk als ein Netzwerk, das mindestens ein Medizinprodukt enthält. Sie schlägt ein Risikomanagement über den Lebenszyklus eines solchen Med. IT-Netzwerkes vor, dass bedeutet, der Risikomanagementprozess muss solange betrieben werden, wie ein solches Netzwerk existiert und für die Patientenversorgung genutzt wird.

Bild 2 zeigt das Beispiel eines einfachen Med. IT-Netzwerkes in Form eines bildgebenden Ultraschallgerätes, das z. B. in einer Ambulanz in das dortige IT-Netzwerk integriert ist, um Patientendaten und medizinische US-Bilder über das Netzwerk zu empfangen bzw. zu senden.
Bei einer geschätzten Nutzung des Ultraschallgerätes über vrsl. 8 Jahre muss dieser Prozess mit der entsprechenden Dokumentation also über diesen Zeitraum betrieben werden.

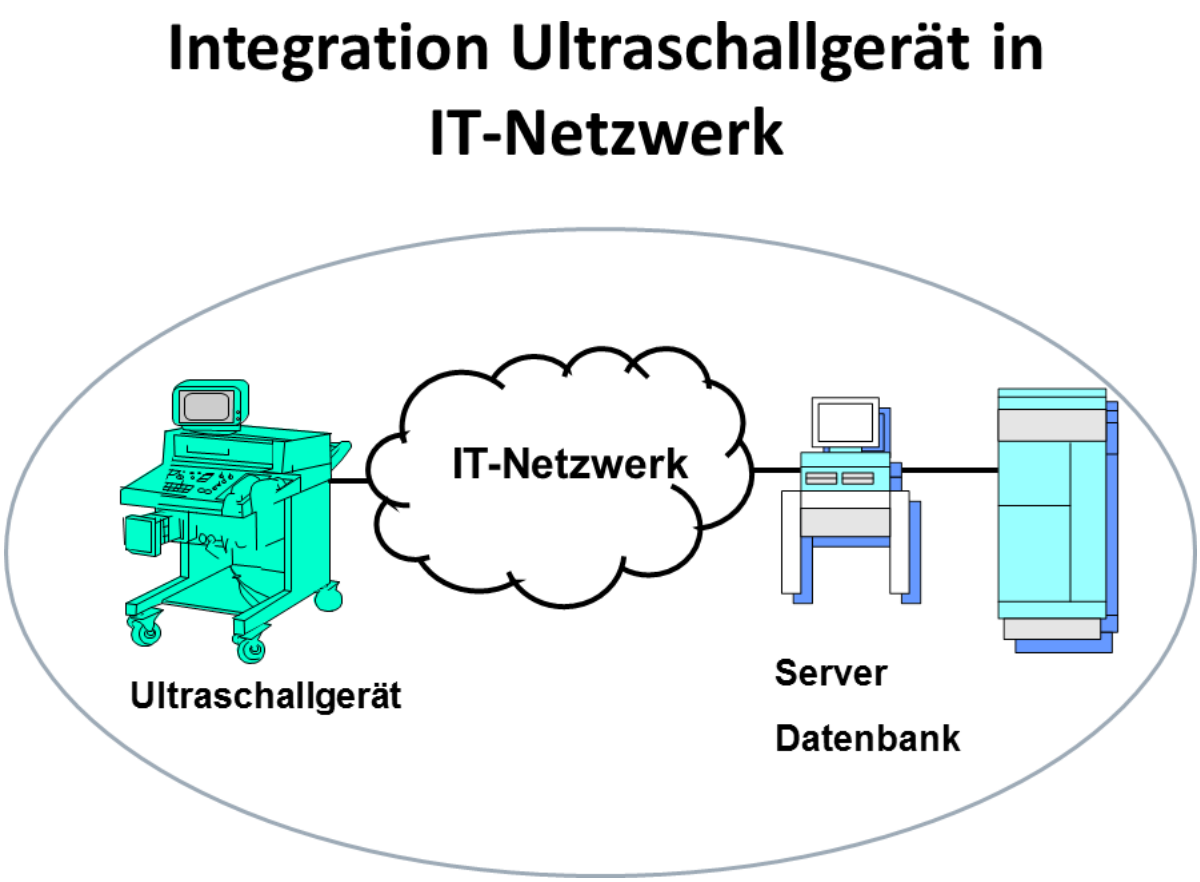

Bild 2: Integration von Medizinprodukten in ein IT-Netzwerk am Beispiel eines Ultraschallgerätes

1.2 Beispiele von Gefährdungen von Med. IT-Netzwerken

Mit dieser wachsenden Integration von Medizinprodukten in IT-Netzwerke entwickelten sich auch neue Gefährdungen der diagnostischen und therapeutischen

Funktionsfähigkeit von vernetzten Medizinprodukten. Ursachen solcher Gefährdungen können u. a. sein

- Netzwerkbelastung
- Malware
- Remote Access Zugriff
- Ungekannte Geräte
- usw.,

die dazu führen können, dass Daten nicht zur Verfügung stehen, Geräte nicht in Betrieb genommen oder Alarme nicht übertragen werden können. Diese Gefährdungen können also zu indirekten oder direkten Risiken (Auftretenswahrscheinlichkeit und Schadensausmaß nach DIN EN ISO 14971) für Patienten führen.
Bild 3 zeigt beispielhafte Ursachen von Gefährdungen der Funktionsfähigkeit Med. IT-Netzwerke und der darin integrierten Medizinprodukte.

Bild 3: Ursachen der Gefährdungen von IT-Netzwerken mit Medizinprodukten

Die DIN EN 80001-1 ist daher das Ergebnis der Bemühung der Normengremien, Betreibern von Med. IT-Netzwerken mit einem neuen Standard als Regel der Technik eine Hilfestellung zu geben, durch ein individuelles Risikomanagement

Gefährdungen/Risiken möglichst zu reduzieren respektive soweit wie möglichst zu beherrschen.

2. Erste Ansätze in der DIN EN 60601-1 3. Ausgabe

Die zunehmende Vernetzbarkeit von Medizinprodukten wurde bereits in der 3. Ausgabe der DIN EN 60601-1:2007 (Quelle 2) behandelt, die Anforderungen an vernetzbare medizinische elektrische Geräte (ME-Geräte) bzw. Systeme (ME-Systeme) und notwendige Informationen betrachtet. Kapitel 14.13 dieser Norm definiert wesentliche Informationen, die ein Hersteller für die Integration eines Medizinproduktes in ein IT-Netzwerk mitliefern muss. Mit dieser Normenvorgabe können Hersteller und Betreiber schon wesentliche Informationsbedürfnisse austauschen bzw. Informationen zur Verfügung stellen.

3. Warum eine technische Regel = Norm für die Integration von Medizinprodukten?

Die seit Anfang des Jahrhunderts aufkommenden und auftretenden Gefährdungen von vernetzbaren Medizinprodukten wie Malware auf Medizinprodukterechnern und –systemen u. a. führten ca. 2005/2006 bei den Normengremien zu Überlegungen, einen Standard zu entwickeln, der generell Betreibern helfen soll, sich mit den zunehmend offenbar werdenden Risiken von vernetzten Medizinprodukten in IT-Netzwerken auseinander zu setzen und eine Hilfestellung bei der Bewältigung der Risiken zu geben.
Aus diesen Ansätzen entstand eine international geprägte Norm in Form der IEC 80001-1:2010 bzw. der DIN EN 80001-1:2011. (siehe Literaturangabe 1)

Dieser Weg über eine Regel der Technik ergab sich, weil weder die Medizinprodukterichtlinie Medical Devices Directive 2007/47/EG noch das deutsche Medizinproduktegesetz (MPG) und auch nicht die Medizinprodukte-Betreiberverordnung (MPBetreibV) konkrete Vorgaben zur IT-Vernetzung von Medizinprodukten beinhalten. Ob sich das in Zukunft ändert, ist momentan noch nicht abzusehen.
Der erste Entwurf der zukünftigen Medical Devices Regulation MDR 9/2012 (Quelle 3) berücksichtigt die zunehmende Integration von Medizinprodukten in IT-Netzwerke derzeit erkennbar nicht. Bei der Diskussion um die Frage, ob nicht die Medizinprodukte-Richtlinien bzw. die zukünftige Medizinprodukte-Verordnung Anforderungen definieren müssen, darf man nicht vergessen, dass die Regularien ja primär das Inverkehrbringen und weniger den Betrieb von Medizinprodukten regeln.

4. Was will die Norm bewirken?

DIN EN 80001-1 ist die erste Norm, die sich spezifisch an die Betreiber von vernetzten Medizinprodukten und Med. IT-Netzwerken richtet.

Sie soll bewirken, dass sich Betreiber (Krankenhäuser, Arztpraxen u. a. Anbieter von Gesundheitsdienstleistungen) mit den Gefährdungen der zunehmenden Vernetzung auseinandersetzen und Maßnahmen treffen, die daraus resultierenden Risiken für Patient, Anwender und Dritte zu minimieren respektive weitgehend zu beherrschen.
Die Norm ist demnach als klarer Impuls bzw. eindeutige Aufforderung an Betreiber (Krankenhäuser, Arztpraxen) anzusehen, sich mit den Sicherheitsfragen vernetzter Medizinprodukte und IT-Netzwerke auseinanderzusetzen und zwar im Vorfeld, bevor ein Medizinprodukt in ein Netzwerk integriert wird.

5. Warum eine Norm für den Betreiber?

Die Norm stellt als Regel der Technik eine Hilfestellung für den Betreiber dar, der letztendlich die Verantwortung für den vernetzten Betrieb im Rahmen der Zweckbestimmung der Medizinprodukte trägt.
Sie stellt derzeit allerdings noch keine anerkannte Regel der Technik dar, nach denen der Betreiber gemäß der Medizinprodukte-Betreiberverordnung (MPBetreibV) Medizinprodukte zu installieren, einzuweisen, anzuwenden und instand zu halten hat.

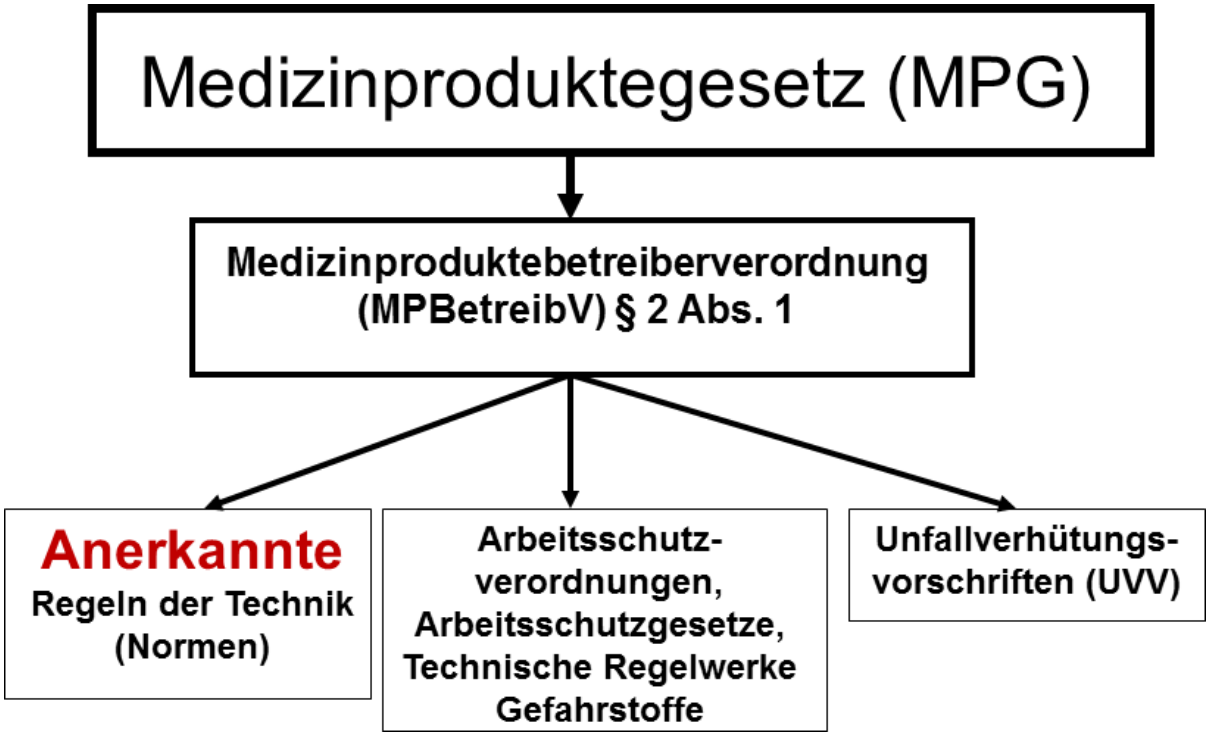

Bild 4: Verpflichtung MPG – MPBetreibV – anerkannte Regeln der Technik

Die DIN EN 80001-1 und die darauf aufbauenden sogenannten Technical Reports (TR 80001-2-X) werden sich aber erfahrungsgemäß zu anerkannten Regeln der Technik entwickeln, wenn sie beispielsweise von einem Gericht bei einem Schadensfall herangezogen werden, um zu prüfen, ob ein Betreiber seine Sorgfaltspflicht beim Betrieb vernetzter Medizinprodukte erfüllt hat.

Wie ein Malware-Befall eines EKG-Schreibers in einer Krankenhaus-Ambulanz einen Patienten gefährden kann, verdeutlicht das folgende Beispiel aus der Sachverständigen-Praxis des Autors.

Ein Patient sucht mit akuten Schmerzen in der Brust die Notfallambulanz eines Krankenhauses auf. Auf Grund dieser Symptomatik wird üblicherweise sofort ein Elektrokardiogramm aufgezeichnet und ausgewertet. In dem vorliegenden Beispiel hat ein Betreiber neue EKG-Schreiber mit WLAN-Anbindung beschafft, sodass eine EKG-Aufzeichnung über das IT-Netzwerk an einen Kardiologen zur mobilen Erstbefundung geschickt werden kann, der nicht mehr permanent in der Ambulanz anwesend ist.
Beim Versuch, den EKG-Schreiber (im Prinzip ein PC mit angeschlossener Sensorik und Netzwerkanschluss) zu starten, verhindert ein über das IT-Netzwerk verbreiteter elektronischer Virus die Funktionsfähigkeit des Schreibers, d. h., es konnte in diesem Fall kein Elektrokardiogramm des Patienten aufgezeichnet werden.
Der Patient kam nicht zu Schaden, weil noch ein älterer, nicht netzwerkfähiger EKG-Schreiber in der Ambulanz vorhanden war, mit dem ein EKG in Form eines Papierausdrucks geschrieben werden konnte.

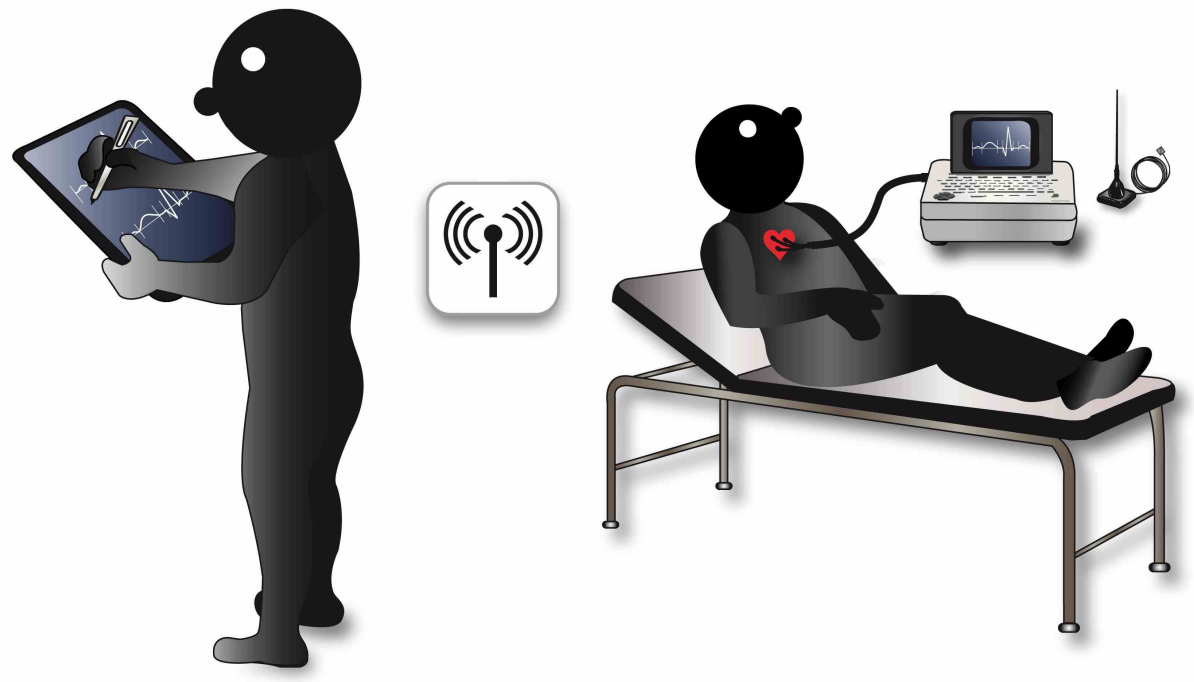

Bild 5: PC-gestützter EKG-Schreiber in der Ambulanz mit WLAN-Übertragung

Bei der Beschaffung der WLAN-fähigen EKG-Schreiber und der Definition des Workflows war kein Risikomanagement für diese in das IT-Netzwerk des Krankenhauses integrierten (Notfall-)Geräte durchgeführt worden. Die Wahrscheinlichkeit des Auftretens von Malware und der mögliche Befall der vernetzten EKG-Schreiber war nicht betrachtet worden.

Dieses Praxisbeispiel zeigt, dass ein Risikomanagement vernetzbarer und vernetzter Medizinprodukte nach DIN EN 80001-1 dem Betreiber nicht nur hilft, seine rechtlich geforderte Sorgfaltspflicht zu erfüllen, sondern ein wesentliches Element darstellt, derartige Risiken schon im Vorfeld zu erkennen und möglichst zu vermeiden.

6. Was kann die Norm leisten und was nicht?

Die Norm stellt das Risikomanagement als Arbeitsmittel in den Fokus, mit dem der Betreiber individuell selber die Gefährdungen und Risiken seiner Med. IT-Netzwerke für Patient, Anwender und Dritte ermitteln muss.
Dass bedeutet, dass die DIN EN 80001-1 keine Checklisten o. a. Arbeitsmaterialien beinhaltet, die man abarbeitet und damit seine Sorgfaltspflichten erfüllt.
Dies kann und soll die Norm nicht leisten. Checklisten sind statisch und können individuelle Situationen – wenn überhaupt – nicht oder nur schlecht abbilden. Gerade weil die betrieblichen Situationen, unter denen vernetzbare Medizinprodukte betrieben werden, von Krankenhaus zu Krankenhaus so unterschiedlich sind, stellt das Risikomanagement als Handwerkzeug die Chance dar, die sehr unterschiedlichen Risiken individuell zu erfassen, zu bewerten und damit auch möglichst zu beherrschen.
Risikobeurteilung hängt auch sehr stark von der individuellen Risikowahrnehmung ab, sodass das Risikomanagement von einer Gruppe aus Angehörigen der verschiedenen Berufsgruppen durchgeführt werden sollte, die alle unterschiedliche Sichtweisen, Erfahrungen und Prägungen haben. Somit besteht die Chance, dass weitgehend alle Gefährdungen erkannt werden, wenn alle Berufsgruppen im Krankenhaus gemeinsam die Risiken eines Med. IT-Netzwerkes betrachten. Die Erfahrung zeigt, dass das Verständnis gerade auch der Anwender für komplexe vernetzte Systeme deutlich steigt, wenn sie in das Risikomanagement eingebunden sind.
Die Norm nimmt also dem Betreiber (oberste Leitung) nicht die organisatorische Aufgabe ab, einen solchen Prozess zu initiieren und somit Personen, Mitarbeiter u. o. Externe zu beauftragen, ein solches Risikomanagement aufzubauen.
Sie schlägt grundsätzlich einen Risikomanagementprozess vor, der immer dann erfolgen muss, wenn ein Medizinprodukt in ein Netzwerk integriert wird. Dieser Prozess muss über die Nutzungsdauer bzw. Lebenszyklus eines Netzwerkes und bei allen Änderungen fortgeführt werden.
Diese Vorgehensweise über ein Risikomanagement stellt einen Paradigmenwechsel dar, durch den der Betreiber veranlasst wird, selber Fragen zur Sicherheit des Med. IT-Netzwerk zu stellen, die von den individuellen Gegebenheiten des jeweiligen Krankenhauses abhängen. Durch eine solche, systematische Vorgehensweise erkennen die beteiligten Personen, welche Prozesse, Schnittstellen u. a. Themen mögliche Gefährdungen und Risiken beinhalten.

Häufig wird Risikomanagement mit Problemmanagement verwechselt. Dies bedeutet, dass erst ein materieller Schaden und/oder schlimmer, ein Personenschaden auftreten müssen, bevor ein Betreiber zum Handeln veranlasst

wird. Ein geradezu klassisches Beispiel stellt der Malwareschutz im Bereich von Rechnern in der Medizintechnik dar. Häufig erfolgt keine rechtzeitige Ersatzbeschaffung alter Rechner und alter Betriebssysteme aus Kostengründen. Kommt es dann zu einem elektronischen Virenbefall, fällt die Funktionsfähigkeit einer Abteilung solange aus, bis das Problem behoben ist. In einem solchen Fall steht erfahrungsgemäß immer sehr schnell Geld zur Verfügung, um das Problem zu beheben.

Die DIN EN 80001-1 ist kein Norm für Problemmanagement, das kann sie nicht leisten. Ihre wesentliche Zielsetzung besteht darin, ein **prophylaktisches** Risikomanagement anzuregen und nicht erst dann, wenn eine Schaden bzw. Problem aufgetreten ist.
Sie ist auch nicht umfassend sondern verweist sinnvollerweise auf andere Normen bzw. läßt dem Krankenhaus, das diese Norm umsetzen will, auch die Freiheit, eigenständige Lösungen zu entwickeln und zu verwenden, die die drei Schutzziele Sicherheit, Schutz und Effektivität möglicherweise genauso einhalten.

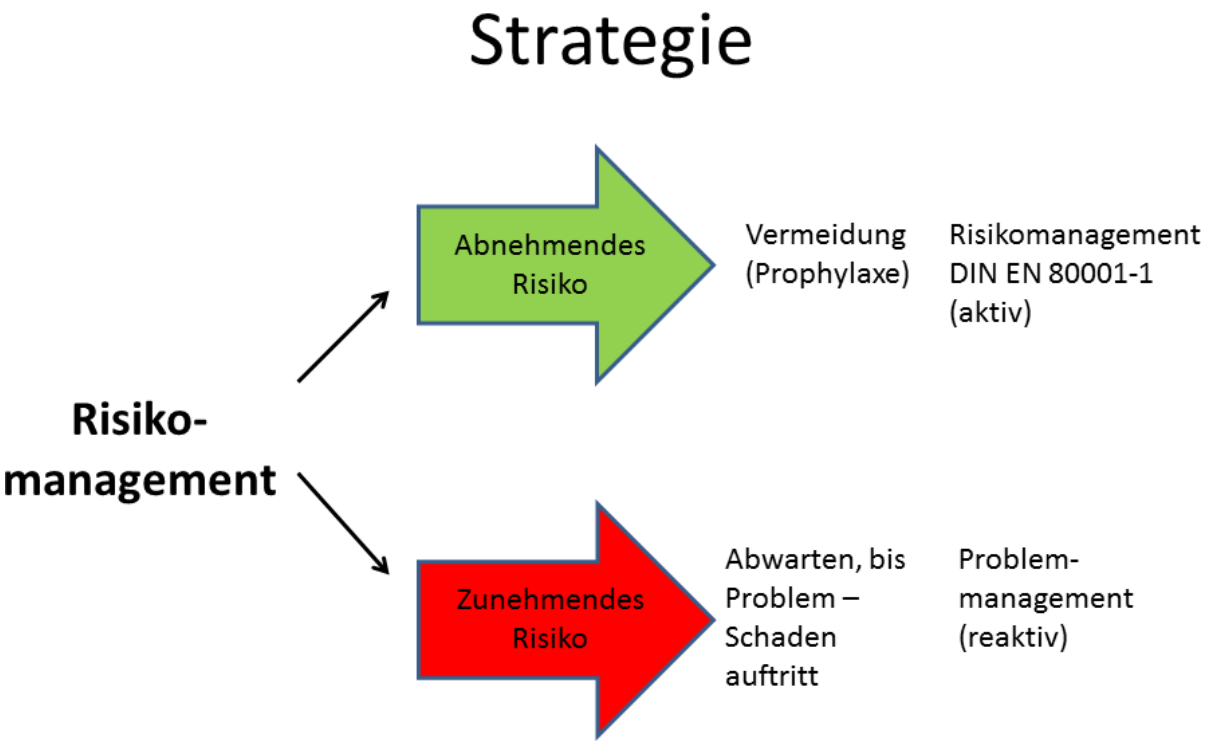

Bild 6: Mögliche Unternehmensstrategien im Umgang mit Gefährdungen und Risiken

Eine Voraussetzung, einen solchen Prozess überhaupt durchführen zu können, besteht darin, sich Kenntnisse im Risikomanagement z. B. nach der DIN EN ISO 14971 (Quelle 4) anzueignen, die immer mehr auch als Handwerkzeug für Betreiber angesehen wird. Nicht umsonst verweist bzw. referenziert die DIN EN 80001-1 auf die Norm 14971.

Da der Gesetzgeber über das MPG und auch über die Betreiberverordnung dies nicht so konkret einfordert bzw. relativ abstrakt hält (siehe § 2. Abs. 3 der MPBetreibV), fällt es in der Praxis durchaus schwer, diesen Prozess zu betreiben.

Immer wieder kommen Fragen auf wie:

- Wo steht das?
- Müssen wir das tun?
- Gibt es schon Gerichtsurteile dazu, nach denen wir dazu verpflichtet sind?

Normen können freiwillig angewendet werden, es besteht keine gesetzliche bzw. rechtliche Verpflichtung, insbesondere dann (noch) nicht, wenn sie noch keine anerkannten Regeln der Technik darstellen. Andererseits ist ein Betreiber aus haftungsrechtlicher Sicht gut beraten, wenn er sich mit den Anforderungen der DIN EN 80001-1 bereits jetzt auseinandersetzt und einen Risikomanagementprozess startet
Eine der Hemmnisse, sich mit dem Risikomanagement integrierter Medizinprodukte zu beschäftigen und einen solchen Prozess dauerhaft zu implementieren, besteht in der Sorge, dass diese Aktivitäten in Konsequenz Ressourcen, Personal und somit – möglicherweise nicht abschätzbaren – Aufwand bedeuten.

7. Ansätze und Vorgehensweise zur Umsetzung

Die Norm richtet sich bewußt an die sogenannte „Oberste Leitung“; mit dieser Formulierung ist immer die Geschäftsleitung und/oder der Vorstand eines Krankenhauses angesprochen und nicht die Fachabteilung Medizintechnik oder die IT. Die Leitung muss einen solchen Prozess starten, was voraussetzt, dass die Gefährdungssituation Med. IT-Netzwerke erkannt wird. (Siehe Bild 3)

Die Norm richtet sich bewußt nicht an die IT-Abteilung und/oder die Medizintechnik, weil die Beschäftigung mit der Norm und die Umsetzung sowohl Ressourcen als auch Prozessveränderungen erfordert, die nur die Geschäftsleitung bzw. der Vorstand eines Krankenhauses durchsetzen kann. Nur die Geschäftsleitung kann eine entsprechende Risikostrategie umsetzen, also definieren, wie mit Gefährdungen und Risiken umzugehen ist. Eine solche Strategie kann (Quelle 5) folgende Teilaspekte umfassen:

- Risiken vermeiden: Versuch, ein Risikoereignis möglichst nicht eintreten zu lassen, indem man die Eintrittswahrscheinlichkeit reduziert
- Risiken begrenzen: Auswirkungen begrenzen wie beispielsweise durch eine Versicherung
- Risiken abschwächen: Reduzierung der Eintrittswahrscheinlichkeit oder der Auswirkungen durch zusätzlichen Aufwand oder kreative Lösungen

- Risiken ignorieren: Die Wahrnehmung eines Risikos unabhängig von der möglichen Eintrittswahrscheinlichkeit und der Auswirkung wird ausgeblendet.

Vielfach findet man im Krankenhausbereich die Strategie, abzuwarten, ob und bis ein Problem auftritt. Solange keine Risiken/Probleme auftreten, ist die Motivation häufig niedrig, Risikomanagement zu betreiben. Dies zeigt sich am Beispiel elektronischer Viren. Seit der Jahrtausendwende ist bekannt, dass Malware (elektronische Viren) auch im Krankenhausbereich auftreten kann.
Wenn denn nun ein solcher Malware-Befall unerwartet auftritt und es keine vorbeugenden Maßnahmen gegeben hat, kann diese Situation zu einer erheblichen Beeinträchtigung und/oder Patientengefährdung führen (siehe Beispiel in Abschnitt 5), bis Maßnahmen umgesetzt sind, um die Malware zu entfernen.
Malwarebefall von Medizinprodukten kann zu einer akuten Gefährdung von Patienten durch Funktionsunfähigkeit von Medizinprodukten, aber auch zu Einnahmeverlusten führen, weil Patienten nicht behandelt werden können und/oder verlegt werden müssen.

Eine Risikoanalyse muss daher Maßnahmen beinhalten, mit denen man Risiken aktiv verfolgen kann. Erkannte Risiken verlieren ihr Gefährdungspotenzial, wenn man die Maßnahmen umsetzt, mit denen man diese Risiken abschwächen, reduzieren und/oder beherrschen kann. Ein Risikomanagement ist daher kein temporär begrenzter Prozess, sondern eine Daueraufgabe über den Lebenszyklus eines Med. IT-Netzwerkes.

Bei der Risikoanalyse sollte man sich zunächst auf die wesentlichen Gefährdungen beschränken, da ansonsten die Gefahr besteht, dass man sich in Details verliert und vielleicht wichtige Gefährdungen übersieht, die ein Risiko für Patienten auslösen können.
Dies bedeutet, dass ein Betreiber mit dem Prozess der Risikoanalyse mit vorhandenen Mitarbeitern und Ressourcen starten sollte, um z. B. kritische Risiken wie bei der Übertragung von Alarmen über das IT-Netzwerk zu erkennen und zu bearbeiten. (siehe Literaturangaben 6 und 7)
Im Laufe der Durchführung eines solchen Prozesses gewinnt der Betreiber an Erfahrung und wird möglicherweise die Vorteile eines konsequenten Risikomanagements erkennen, was dann idealerweise dazu führt, dass mehr Ressourcen für diesen Prozess zur Verfügung gestellt werden.

Der Versuch, die DIN EN 80001-1 möglichst schnell und hundertprozentig in allen Bereichen umzusetzen bzw. zu erfüllen, wird erfahrungsgemäß scheitern, wenn nicht Priorisierungen und somit eine Konzentration auf wesentliche Risiken erfolgen.
Es sollte daher gelten:

→ Keine Analyse bis zur Paralyse

DIN EN 80001-1 empfiehlt die Erstellung einer Risikostrategie. Darunter versteht die Norm eine beschreibende Definition, wie ein Betreiber mit Risiken generell und spezifisch vorausschauend sowie beim unerwarteten Auftreten von Risiken umgeht. Nach Ebert (Quelle 5 S. 82) betrachtet eine Risikostrategie immer alle Einflussfaktoren und versucht, allgemeingültige Regeln und Verfahrensweisen zu kommunizieren.

Aufgaben des Betreibers
Beschafft und integriert ein Betreiber vernetzbare Medizinprodukte in ein IT-Netzwerk, so verfügt er normalerweise bereits über eine Organisationsstruktur und (idealtypische) Prozesse, die eine solche Beschaffung und Integration ermöglichen und begleiten (sollten):

- Qualitätsmanagement: dient der Prozessbeschreibung
- Beschaffungsmanagement: beschafft Medizinprodukte unter standardisierten Bedingungen und Voraussetzungen
- Projektmanagement: schafft die planerischen, baulichen und technischen Voraussetzungen für die Integration vernetzbarer Medizinprodukte.

Dies bedeutet, dass wesentliche Elemente i. d. R. bereits vorhanden sind, auf die man das Risikomanagement nach DIN EN 80001-1 aufbauen kann. Mit anderen Worten, normalerweise verfügt ein Betreiber idealerweise bereits über Prozesse, die wesentliche Voraussetzungen bzw. Bestandteile eines Risikomanagements darstellen.

Das Risikomanagement nach DIN EN 80001-1 betrachtet konsequent die sich aus der Integration von vernetzbaren Medizinprodukten in ein IT-Netzwerk entstehenden Gefährdungen und daraus resultierende Risiken, aber nicht Geräterisiken, die der Hersteller bereits bewertet hat. Dies bedeutet auch, dass der Aufwand überschaubar wird, wenn man sich initial auf kritische Med. IT-Netzwerke konzentriert und dafür das Risikomanagement durchführt.

Da die „Mutter“-Norm DIN EN 80001-1 relativ abstrakt, auch sehr komplex ist und beileibe nicht alle Themen abdecken kann, erscheinen bzw. werden sogenannte Technical Reports erscheinen, die konkrete Themen behandeln wie Anforderungen an WLAN-Infrastruktur, Alarmsysteme u. a.

Folgende Technical Reports sind bereits erschienen bzw. werden zurzeit erarbeitet:

DIN IEC/TR 80001-2-1	Application of risk management for IT-networks incorporating medical devices - Part 2-1: Step by step risk management of medical IT-networks - Practical applications and examples
DIN IEC/TR 80001-2-2	Application of risk management for IT-

	networks incorporating medical devices -- Part 2-2: Guidance for the communication of medical device security needs, risks and controls
DIN IEC/TR 80001-2-3	Application of risk management for IT-networks incorporating medical devices - Part 2-3: Guidance for wireless networks
DIN IEC/TR 80001-2-4	Application of risk management for IT-networks incorporating medical devices – Part 2-4: General implementation guidance for Healthcare Delivery Organizations
DIN IEC/TR 80001-2-5	Application of risk management for IT-networks incorporating medical devices - Part 2-5: Guidance on distributed alarm systems (IEC 62A/816/NP:2012)

Tabelle 1: Überblick über Technical Reports TR 80001-2-X

Weitere TR sind in Planung bzw. können erarbeitet werden.

8. Chancen und Potenziale der Norm

Die wesentliche Bedeutung der Norm für einen Betreiber ergibt sich durch folgende Chancen und Potenziale:

- Reduzierung der Gefährdungen und Risiken Med. IT-Netzwerke
- Reduzierung haftungsrechtliche Probleme
- Reduzierung wirtschaftlicher Probleme durch unkalkulierbare Ausfälle (Erhöhung der Verfügbarkeit Med. IT-Netzwerke)
- Transparenz in Beschaffungsprozessen und in Instandhaltungsprozessen
- Verbesserte Abstimmungsprozesse durch Optimierung der internen Kommunikation zwischen Anwender Medizintechnik, IT und Einkauf
- Reduzierung Zeit- und Kostenaufwand bei Projekten
- Mögliche Standardisierung zur Vereinfachung des Aufwandes der Vernetzung von Medizinprodukten in das IT-Netzwerk
- Erfüllung des KonTraG: Ein Unternehmen muss die von ihm bereits eingegangenen und noch einzugehenden Risiken identifizieren, messen als auch steuern und regeln, wenn es seinen Bestand langfristig sichern will. Mit KonTraG wurde die Grundlage zur ganzheitlichen Betrachtung der Risiken im unternehmerischen Umfeld geschaffen.
- U. a.

Ein wesentlicher, noch unterschätzter Benefit besteht in der Prozessanalyse der bestehenden Abstimmungs- und Kommunikationsprozesse bei Beschaffungen von Medizinprodukten. DIN EN 80001-1 setzt voraus, dass im Rahmen eines

Projektmanagements alle Aspekte der Beschaffung, Installation und Integration im Vorfeld geklärt sind, bevor ein Auftrag erteilt wird. Häufig findet man in der Praxis, dass diese Abstimmungsprozesse nicht oder nicht vollständig erfolgen, sodass man nach Auslieferung, Installation und Übergabe eines Medizinproduktes feststellt, dass kostenintensive Nacharbeiten erforderlich sind, z. B. in der IT-Infrastruktur auf Grund veralteter Switches, PC u. a. Werden diese Themen im Vorfeld der Beschaffung in Hinblick auf die Anforderungen bzw. Schutzziele der DIN EN 80001-1 mit allen beteiligten Fachabteilungen geklärt, ersparen sich die Krankenhäuser nachträgliche Aufwendungen und auch Ärger.

Bild 7 zeigt prinzipiell, wie ein Beschaffungsprozess im Vorfeld der Auftragserteilung erfolgen sollte, indem der Nutzer sein Anforderungsprofil definiert. Diese Nutzeranforderungen werden dann von Medizintechnik und IT in ein technisches Anforderungsprofil umgesetzt und auf die Anforderungen der DIN EN 80001-1 geprüft. Wenn dann alle diesbezüglichen Fragen geklärt sind, kann die finale Abstimmung mit dem Nutzer erfolgen und die Beschaffung durchgeführt werden.

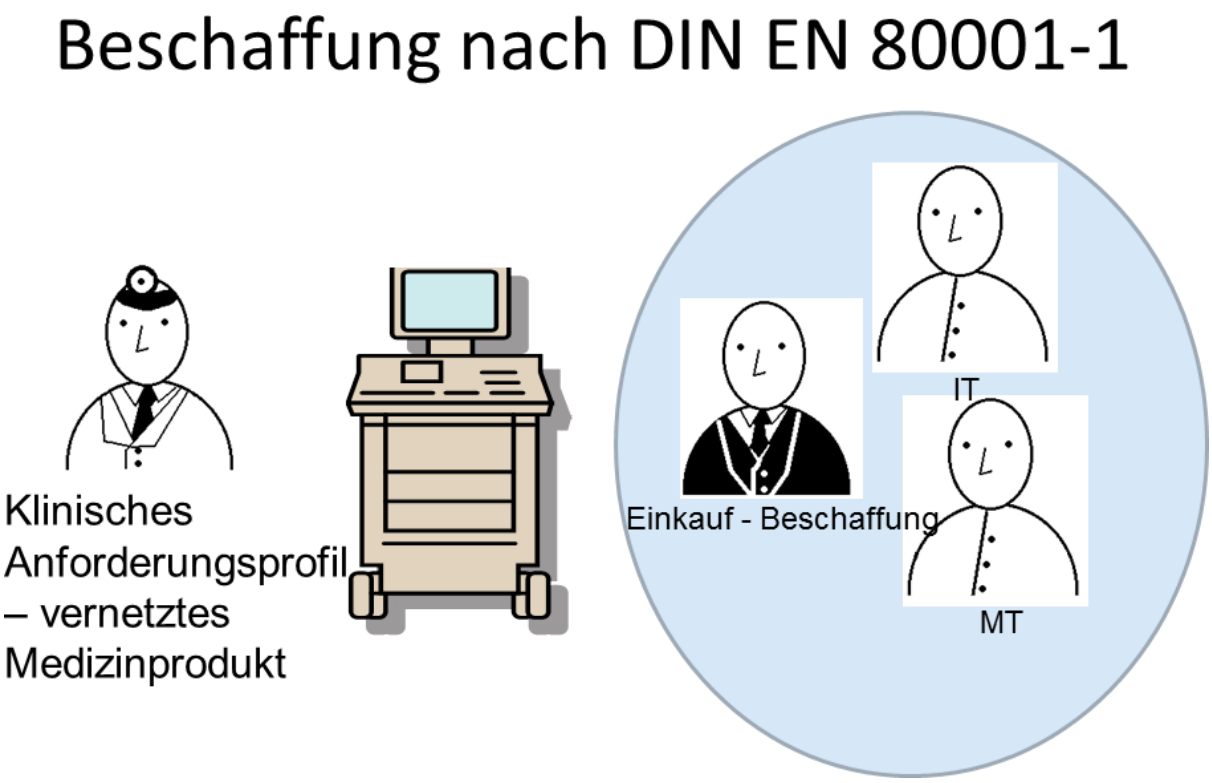

Bild 7: Prozessänderungen aufgrund der Anforderungen der DIN EN 80001-1

An diesen häufig nicht klar definierten innerbetrieblichen Schnittstellen und der nicht immer eindeutigen Kommunikation zwischen den Fachabteilungen (Problem der Zuständigkeit und der Information) verlieren Krankenhäuser immer noch viel Geld auf Grund nicht geklärter Voraussetzungen bzw. nicht abgestimmter Anforderungen. Die DIN EN 80001-1 bietet daher die Chance, derartige Probleme im Rahmen eines

eindeutigen Projekt- und Risikomanagements zu vermeiden und somit Beschaffungen effizient durchzuführen.

9. Wertung der DIN EN 80001-1

Die DIN EN 80001-1 ist ein notwendiger, wichtiger Ansatz und Impuls für den Betreiber, sich um die Sicherheit, den Schutz und die Effektivität seiner zunehmend vernetzten Unternehmens-Infrastruktur als kritischen Erfolgsfaktor zu kümmern. Sie ist auch die erste Norm als Regel der Technik, die sich direkt an Betreiber vernetzter Medizinprodukte richtet.
Das Dilemma der Grundnorm DIN EN 80001-1 besteht darin, dass sie nicht nur abstrakt formuliert sondern sehr komplex gestaltet ist.
Das Risikomanagement mit der Risikoanalyse nach DIN EN ISO 14971 ist im Krankenhausbereich noch wenig bekannt und auch als Organisations-Handwerkzeug in den Technik-Abteilungen noch wenig verbreitet. Gerade IT-Abteilungen tun sich mit dem Risikomanagement für ihre Arbeit schwer und wünschen sich daher häufig konkrete, abzuarbeitende Checklisten.
Die DIN EN 80001-1 stellt somit einen Paradigmenwechsel dar, weil der Betreiber Verfahren selber definieren muss, was zu tun ist. Diese Vorgehensweise erfordert Aufwand, wenn man Risikomanagement konsequent umsetzen will. Dieser Aufwand besteht u. a. darin, nicht nur ein neues Arbeitsmittel zu erlernen sondern auch darin, sehr umfangreiche individuelle Dokumentationen zu erstellen und diese auch zu pflegen.
Definiert man Komplexität mit der Höhe des Aufwandes und der Fülle von Maßnahmen, dann bedeutet das bezogen auf die DIN EN 80001-1, dass man bei einer angenommenen idealtypischen Umsetzung zukünftig Mitarbeiter für die ständige Nacharbeit und Pflege der erstellen Risikodokumentation für jedes Med. IT-Netzwerk über dessen Lebenszyklus einsetzen muss.
So wichtig die Norm auf Grund von Vorkommnissen mit vernetzten Med. IT-Netzwerken und somit ihre Umsetzung im Krankenhaus ist, so verhalten ist die Resonanz auf die unübersehbare Komplexität und Umfang der Aufgaben, die aus der Norm heraus resultieren. Es besteht daher durchaus die Gefahr, dass die Norm auf Grund dieser erkennbaren Komplexität nicht oder nur beschränkt wahrgenommen wird.

Dies liegt auch daran, dass der Umfang und die möglicherweise geforderte Vollständigkeit der Risikomanagementdokumentation nicht definiert sind. Es obliegt dem Betreiber, Umfang und Detailtiefe des Risikomanagements und damit der Dokumentation selber festzulegen.
Mit anderen Worten, Umfang und Inhalt des geforderten Risikomanagements und der daraus resultierenden Dokumentation sind zunächst nicht überschaubar. Somit sind der dafür erforderliche Aufwand und die entstehende Kosten schwer zu kalkulieren. Der Nutzen und Benefit erschließen sich nicht unmittelbar, direkt und auch nicht sofort in konkret fassbaren monetären Einsparungspotenzialen. Diesen Befürchtungen stehen aber durchaus nutzbare Chancen und Potenziale gegenüber.

Der entscheidende Aspekt liegt darin, ein Risikomanagement als Unternehmensprozess zu beginnen und nicht darin, eine formalisierte Risikodokumentation aufzubauen.

10. Empfehlung zum Umgang und zur Umsetzung der DIN EN 80001-1

Was sind der Nutzen und Benefit eines Risikomanagements über die Integration von vernetzbaren Medizinprodukten in ein IT-Netzwerk?
Solange nichts passiert, ist es oft schwierig, zugunsten von Risikomanagement zu argumentieren. Die Motivation, ein Risikomanagement durchzuführen, kann sich aus folgenden Überlegungen heraus ergeben:

- Der Betreiber kann auf Probleme, mögliche Gefährdungen und Risiken frühzeitig reagieren.
- Wenn mögliche Gefährdungen frühzeitig erkannt werden, wird der Blick für weitere Gefährdungen geschärft.
- Gefährdungen können reduziert und alternative Lösungen rechtzeitig geplant werden.
- Es sind bereits Probleme und Gefährdungen mit vernetzten Medizinprodukten aufgetreten, z. B. Malwarebefall.
- u. a.

Das Risikomanagement sollte sich daher zunächst auf die wichtigsten Gefährdungen und Risiken konzentrieren. Der Versuch, alle möglichen Gefährdungen und Risiken auch nur ansatzweise zu analysieren und bearbeiten, erzeugt einen immensen Aufwand, der letztendlich in eine (motivatorische) Sackgasse führen kann. Die Vermeidung von Gefährdungen stellt vorbeugenden Schutz im Sinne der Sorgfaltspflicht dar.

Die Konzentration auf die wichtigsten Gefährdungen ermöglicht es dem Betreiber auch, zunächst im Rahmen der bestehenden Möglichkeiten und vor allem vorhandenen Ressourcen, wichtige Risiken weitgehend zu beherrschen. Solche konkreten Risiken bestehen z. B. in der zunehmenden Nutzung des IT-Netzwerkes für die Alarmübertragung. Idealerweise startet man mit einem überschaubaren Projekt in Form eines kleinen Med. IT-Netzwerkes und lernt dabei die Vorgehensweise und die Methoden eines Risikomanagementprozesses.

Wenn dann der Betreiber im Laufe des Prozesses feststellt bzw. durch Erfahrung die Erkenntnis gewinnt, das Art und Umfang des Prozesses ausgeweitet werden müssen, dann sollte dies auch durch entsprechende Ressourcen z. B. für weitere Qualifikation und Personal erfolgen.
Auf der anderen Seite ist es nicht zu empfehlen, nur auf Grund der Komplexität und der weitgehenden Abstraktheit des erheblichen Arbeitsaufwandes die Norm zur Seite zu legen und keinen Risikomanagementprozess für Med. IT-Netzwerke zu starten.

Die Gefährdungen von Med. IT-Netzwerken werden weiter zunehmen, genauso wie die Nutzung des Med. IT-Netzwerk zunimmt.

Die Empfehlung besteht daher darin, die Chancen und Potenziale für das Unternehmen zu nutzen, die bei einer systematischen und überschaubaren Beschäftigung mit der Norm und den Technical Reports zu heben sind und somit mit vorhandenen Ressourcen zu starten.

Literatur und Quellenangaben

1. DIN EN 80001-1:2011 Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten
2. DIN EN 60601-1:2007-07 Medizinische elektrische Geräte – Teil 1: Allgemeine Festlegungen für die Sicherheit einschließlich der wesentlichen Leistungsmerkmale
3. http://ec.europa.eu/health/medical-devices/files/revision_docs/proposal_2012_542_de.pdf, letzter Zugriff 30.10.2012
4. DIN EN ISO 14971; 2009-10 Medizinprodukte - Anwendung des Risikomanagements auf Medizinprodukte
5. Ebert, C.; Risikomanagement kompakt, Spektrum Akademischer Verlag, 2006, ISBN 978-3-8274-1646-9
6. Gärtner, A.; http://www.e-health-com.eu/fileadmin/user_upload/dateien/Downloads/Gaertner_Normentechn._Anforderungen_an_Patientenueberwachung_und_Alarmierung_Teil1.pdf, letzter Zugriff 03.11.2012
7. Gärtner, A.; http://www.e-health-com.eu/fileadmin/user_upload/dateien/Downloads/Gaertner_Patientenueberwachung-Teil_2_Verteilte_Alarmsysteme_und_Risikomanagement_Gaertner_Patientenueberwachung_Teil2.pdf, letzter Zugriff 03.11.2012

Stand 04.11.2012

Verfasser
Armin Gärtner
Ingenieurbüro für Medizintechnik
Ö. b. u. v. Sachverständiger für Medizintechnik und Telemedizin
Edith-Stein-Weg 8
40699 Erkrath
Armin.gaertner@t-online.de