# Allgemeine und spezielle Sicherheitsziele

Die Themen Sicherheit und Risiko rücken immer dann in den Mittelpunkt des öffentlichen Interesses, wenn durch Fehler in Geräten oder technischen Systemen Menschen zu Schaden gekommen sind. Gefahren und Unfälle können durch menschliches Versagen ausgelöst werden, aber auch durch technische Defekte in Systemen unterschiedlichster Art. Systeme die nicht vor Missbrauch geschützt werden oder auch andere sicherheitstechnischen Schwächen aufzeigen, sind nicht sicher und stellen ein erhöhtes Risiko für Personen dar. [Löw, Pabst & Petry 2010, S. 9]

Benutzer von technischen Geräten haben verständlicherweise sehr hohe Erwartungen an die Sicherheit von Systemen und die Reduzierung der Risiken und Defekten. Hersteller wollen sichere Produkte kostengünstig entwickeln durch Unfälle vermeiden und die Kundenzufriedenheit erhalten. [Löw, Pabst & Petry 2010, S. 10]

In den vergangenen Jahren ist der Der Anteil der sicherheitsbezogenen, elektronischen Steuerungen und der Software in den verschiedenen Produkten stark angestiegen. Daraus ergibt sich natürlich eine wachsende Komplexität der Systeme und Anforderungen an die Sicherheit der Geräte. In aktuellen Kraftfahrzeugen finden sich schon bis zu 80 verschiedene elektronische Steuergeräte die für Sicherheit der Passagiere sorgen. Diese Entwicklung spiegelt sich jedoch in fast allen Bereichen wieder, unteranderem auch bei Medizingeräten. Im Bereich der Medizintechnik spielt das Thema Sicherheit und Zuverlässigkeit eine sehr wichtige Rolle. Die Software in diesen Chips, die zu einem sicheren Betrieb der Geräte beiträgt, muss dann jedoch stabiler und zuverlässiger funktionieren als etwa das Betriebssystem eines heutigen Laptops, das den Betrieb ab und zu durch einen Neustart unterbrich t, wenn es meint, überlastet zu sein. [Löw, Pabst & Petry 2010, S. 10]

Um Anforderungen an Sicherheiten von Produkten erfüllen zu können, ist die Anwendung von Sicherheitsnormen dringend erforderlich. Diese Normen beschreiben Standards, welche von der Mehrzahl der Fachleute als korrekt anerkannt wird und sich auch in der Praxis gut bewährt hat. Die Anwendung der Regeln unterstützt zusätzlich die nachweisbare Erfüllung der Sicherheitsanforderungen an Produkte. [Löw, Pabst & Petry 2010, S. 11]

# Normen für die Sicherheit von Medizinprodukten

Einen Stand der Technik widerspiegelndes Dokument definiert sich als Norm. Eine Norm regelt und erleichtert somit durch Festlegungen allgemeine und wiederkehrende Anwendungen, wie zum Beispiel Herstellungsprozesse, Prüfverfahren, sowie Produkteigenschaften. Sie können sich somit sowohl auf Gegenstände als auch auf Verfahren beziehen. [Rölleke 2010, S. 605]

Normen haben für sich genommen keinerlei Gesetzeskraft. Ihre Anwendung für Produkte, Hersteller, Betreiber und Anwender ist somit freiwillig. Erst durch Rechtsakte können Normen Verbindlichkeit erlangen, etwa wenn auf sie in privaten Verträgen oder in Gesetzen und Verordnungen Bezug genommen wird. [Rölleke 2010, S. 606]

Nun wollen wir auf Normen in Bezug auf Medizinprodukte näher eingehen. Ein Medizinprodukt ist ein einzelnes oder mit anderen Medizinprodukten verbundenes Instrument, Apparat oder Vorrichtung, welche einschließlich der für ein einwandfreies funktionierendes Medizinproduktes eingesetzte Software, die vom Hersteller zur Anwendung für Menschen mittels ihrer dafür vorgesehenen Funktionen benutzt wird. Die Einhaltung grundlegender Anforderungen bei medizinischen Produkten ist nach der jeweiligen Europäischen Richtlinie zu erfüllen. [Rölleke 2010, S. 606]

Für alle Medizinprodukte gilt die „DIN EN ISO 14971“. Da diese Norm, als Prozessstandard noch die größte Produktnähe aufweist, wollen wir sie an dieser Stelle etwas näher darauf eingehen. Die Norm „DIN EN ISO 14971“ wurde spezifisch für die Herstellung von Medizinprodukten entwickelt und behandelt sich mit dem Erkennen, Bewerten und Minimieren von Risiken, die natürlich in der erster Linie Patienten betreffen könnten. [Rölleke 2010, S. 607] Das Risiko lässt sich, neben subjektiv geprägten Parametern, auch durch folgende 2 Faktoren charakterisieren:

* Wahrscheinlichkeit des Auftretens eines Schadens
* Auswirkung des Schadens

Die Risikomanagementnorm „DIN EN ISO 14971“ kann ebenfalls Prozesse zur Identifizierung und Minimierung von Gefährdungen festlegen, die von Medizinprodukten ausgehen können. Einen Risikobereich vertretbar konkretisieren ist pauschal jedoch nicht möglich. [Rölleke 2010, S. 608]

Wie schon zuvor erwähnt beschreibt die Norm „DIN EN ISO 14971“ eine Risikomanagementnorm bzw. ein Verfahren. Die Abbildung 1 zeigt den, die in der ISO 14971 festgelegten, Risikomanagementprozess. Es gibt 4 Schritte für das Risikomanagement, welche zu beachten sind. [Rau 2010, S. 129]

* Risikoanalyse (risk analysis)
* Risikobewertung (risk evaluation)
* Risikokontrolle (risk control)
* Postproduktionsinformationen (post-production information)

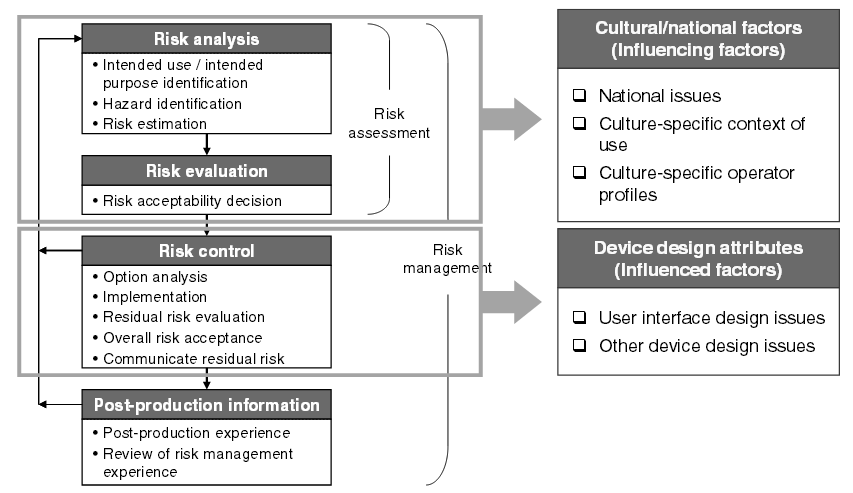


Abb. 1. Riskomanagement and Faktoren für kulturübergreifende Gestaltung von Medizinprodukten [Rau 2010, S. 129]

# Definition von Informationssicherheit

Der weiter verbreitete Begriff der IT-Sicherheit erfüllt nicht mehr die Anforderungen einer ganzheitlichen Betrachtungsweise, da Geräte aus dem mobilen Bereich (wie in etwas Smartphones) nicht als IT-Systeme bzw. IT-Geräte verstanden werden und dadurch oft übersehen werden. Aus dieser Gegebenheit heraus, ist es normgerechter den Begriff Informationssicherheit zu verwenden. [Vogel, Gruetz 2010, S. 163]

Unter dem Begriff Informationssicherheit versteht man im Wesentlichen folgende Punkte:

* Vertraulichkeit

Die Informationen werden nur den dazu befugten Personen zugänglich gemacht.

* Verfügbarkeit

Die Informationen sind in angemessener Zeit aufrufbar.

* Integrität

Die Informationen bleiben richtig und vollständig.

* Zurechenbarkeit

Die Änderungen der Informationen kann dem Urheber der Änderungen zugerechnet werden.

* Authentizität

Der Systembenutzer oder das System selbst ist tatsächlich derjenige bzw. dasjenige für den er oder es sich ausgibt.

Informationssicherheit dient der Aufrechterhaltung des Geschäftsbetriebs. In weiterer Folge werden dadurch auch die Geschäftsrisiken minimiert und die Rendite und Geschäftschancen maximiert. Informationssicherheit ist somit der Schutz von Informationen vor einer Vielzahl von unternehmerischen Bedrohungen. [Vogel, Gruetz 2010, S. 163]

Die Informationssicherheit unterstützt somit das Unternehmen und darf nicht als Hindernis angesehene werden. Welche Sicherheitsziele nun gelten, also beispielsweise welches Maß an Vertraulichkeit bzw. Verfügbarkeit für die Informationen gelten soll, sollte jedes Krankenhaus verbindlich und hausweit gültig in den Sicherheitslinien festlegen. Folgende Ziele könnten in die Sicherheitslinien festzuschreiben sein:

* Unternehmenswichtige IT-Systeme sind hoch verfügbar
* Alle Systeme werden von einem Zugriff durch Unbefugte geschützt
* Die Anforderungen an die ärztliche Schweigepflicht werden eingehalten
* Kosten für die Geschäftsprozesse werden optimiert
* Schadensfälle durch nicht gesicherte IT-Systeme werden unterbunden

[Vogel, Gruetz 2010, S. 163]

# Angriffsarten und Angriffspfade

Immer mehr klassische Medizingeräte werden durch neuere innovative Geräte ersetzt, deren Funktionalität durch Software gesteuert wird und die zum Austausch von Daten über das LAN (Local Area Network) oder WLAN (Wireless Local Area Network) kommunizieren. Diese Geräte wachsen in die IT eines Krankenhauses hinein und unterliegen somit auch deren Gefahrenpotential. In den letzten Jahrzehnten waren in fast allen Häusern die Bereiche IT und Medizintechnik klassisch getrennt. In den letzten Jahren werden doch immer öfters herkömmliche PCs zur Steuerung bzw. Auswertung der Daten von Medizingeräte. Auch fordert das Krankenhauspersonal erfasste Daten möglichst überall im Haus verfügbar zu haben. Hierbei wird oft auf eine gemeinsam genutzte LAN-Kabel-Infrastruktur zurückgegriffen. Dabei ergeben sich jedoch folglich einige Sicherheitsprobleme. [Vogel, Gruetz 2010, S. 162]

Die Medizintechnik, die bisher quasi, in einer sicheren Umgebung arbeiten konnte, hatte bisher keinerlei bösartige Ein- und Angriffe waren zu erwarten, da es sich meist um nicht vernetzte Geräte handelte. Diese Geräte waren zusätzlich auch noch mit proprietären Betriebssystemen ausgestattet oder in abgeschlossenen Netze ohne Zugang zur Außenwelt, geschweige denn zum Internet. Auf der anderen Seite haben wir die moderne IT, die seit Jahren mit Viren und Trojanern, mit Fehlern in Betriebssystemen und Software leben muss. Dadurch hat sich ein reichhaltiges Wissen zur Gefahrenabwehr angehäuft. [Vogel, Gruetz 2010, S. 162]

# Sicherheitsangriffe

Aus der Gegebenheit heraus, dass in Krankenhäuser dieselben bis sehr ähnliche IT-Infrastrukturen wie in anderen Unternehmen zum Einsatz kommen, ergeben dieselben klassischen IT-Sicherheitsprobleme und Angriffsarten.

* Routing Protocoll Injection

Hierbei wird unbefugt die Routingtabelle von Gatewaysystemen verfälscht

* Denial-of-Service-Angriffe

DoS-Angriffe unterscheiden sich in einem Punkt von anderen Angriffsarten. Bei dieser Art des Angriffs will der Angreifer nicht Zugang zum Netzwerk, sondern der Angriff hat den Zweck das System so stark zu überlasten, dass eine normale Nutzung nicht mehr möglich ist.

* IF-Spoofing Angriff

Hierbei wird unter Vortäuschung einer falschen IP-Adresse Aktionen gegen fremde Systeme gestartet. Durch die Identitätsverschleierung ist es oftmals schwierig den Verursacher zeitnah zu identifizieren.

* Password Cracking Angriffe

Dies stellt wohl die gebräuchlichste Form von Angriffe auf IT-Systeme dar. Es wird versucht Zugänge auf dem Zielsystem und die zugehörigen Passwörter zu ermitteln.

* Man-in-the-middle-Angriff

Dies ist eine Angriffsart bei der sich eine initialisierende Kommunikationsbeziehung, bei der sich der Angreifer logisch genau zwischen den Partner befindet. Es wird dem Angreifer somit möglich sein, Daten mitzulesen und ggf. auch zu manipulieren. Die Sicherheit kann in diesem Zusammenhang erhöht werden, wenn sich beide Partner einer starken Authentifizierung beim Verbindungsaufbau unterziehen müssen.

[Laszlo 2004, S. 14]

# Literaturverzeichnis

[Löw, Pabst & Petry 2010] Peter Löw, Roland Pabst, Erwin Petry: Funktionale Sicherheit in der Praxis, 2010, dpunkt Verlag, S. 1-15.

[Vogel, Gruetz 2010] Norbert Vogel, Rüdiger Gruetz: IT-Sicherheit in Kliniken, 2010, Vieweg + Teubner, S. 161-179.

[Rölleke 2010] Dr. T. Rölleke: Stellenwert und Verbindlichkeit von Normen für die Sicherheit von Medizinprodukten, 2009, Springer-Verlag, S. 605-609.

[Laszlo 2004] Marc Laszlo: Security Risk Management - Kostenbetrachtung bei der Untersuchung von IT-Risiken, 2004

[Rau 2010] P. L. Patrick Rau: Cultural Diversity - New Challenge to Medical Device Use Safety for International Markets, 2013, Springer Berlin Heidelberg, S. 127-136.