EHEALTHCOM
Magazin für Health-IT, vernetzte Medizintechnik und Telemedizin

Aufgabenstellungen der novellierten MPBetreibV an Betreiber, Medizintechnik und IT für vernetzbare Medizinprodukte

Expertenbeitrag von Armin Gärtner

Einleitung

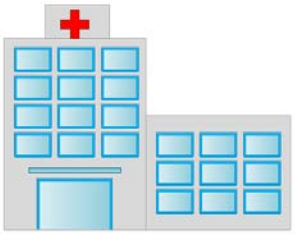
Da immer mehr Medizinprodukte zweckbestimmt vernetzt werden können, stellt sich die Frage, wie die Medizinprodukte-Betreiberverordnung den sicheren Betrieb von vernetzbaren Medizinprodukte mit Betriebssystemen, IT-Netzwerken und Gefährdungen durch Malware regelt.

Am 01.01.2017 erschien die in weiten Teilen novellierte Medizinprodukte-Betreiberverordnung mit zahlreichen Neuerungen, aber auch weitgehenden Änderungen bisheriger Paragrafen. Der folgende Beitrag setzt sich mit Bedeutung der novellierten Verordnung für vernetzbare Medizinprodukte auseinander, die in das IT-Netzwerk einer Gesundheitseinrichtung integriert werden, um Daten wie z.B. medizinische Bilder und Befunde auszutauschen. Der Beitrag erläutert die z. T. sehr abstrakten bzw. vagen Anforderungen und ihre beispielhafte Umsetzung in das Prozessmanagement einer Gesundheitseinrichtung.

1. Betreiber-Definition der MPBetreibV

Eine der wesentlichen Neuerungen der MPBetreibV stellt die Legaldefinition des Betreibers dar, welche bisher gefehlt hat. § 2 Ab. 2 definiert nun den Betreiber einer Gesundheitseinrichtung eindeutig als jede juristische oder natürliche Person, die für den Betrieb der Gesundheitseinrichtung verantwortlich ist, in der Medizinprodukte durch dessen Beschäftigte betrieben oder angewendet werden.

§ 2 Abs. 2 Betreiber-Definition



- Betreiberverantwortung:
- Geschäftsleitung/Vorstand

- § 3 Betreiberpflichten
- **Betreiber muss sicheres und ordnungsgemäßes Anwenden von Medizinprodukten gewährleisten!**

Bild 1: Betreiberdefinition und Pflichten

Der Betreiber muss eine sichere und ordnungsgemäße Anwendung von Medizinprodukten gewährleisten. Dies gilt nicht nur für einzelne Medizinprodukte sondern auch für Medizinproduktesysteme und für Kombinationen im Rahmen des § 4 Abs. 4.

Auch wenn die Verordnung der zunehmenden Vernetzung von Medizinprodukten mit der IT-Infrastruktur der Gesundheitseinrichtungen nach wie vor nicht durch konkrete Anforderungen Rechnung trägt, läßt sich dennoch aus der vorliegenden aktuellen Fassung ableiten, dass der Betreiber auch die IT-Sicherheit vernetzbarer Medizinprodukte sicherstellen und somit gewährleisten muss. Dies bedeutet z. B., vernetzbare Medizinprodukte vor Gefährdungen durch Malware aus dem Netzwerk zu schützen, Betriebssysteme auf einem aktuellen Patchzustand zu halten und a. m. Die seit 2016 und 2017 zunehmend auftretenden Ransomware bzw. Crypto-Trojaner wie Locky, Jaffa, Wannacry u. a. nutzen zunehmend Sicherheitslücken von Betriebssystemen von vernetzten Rechnern und gefährden somit auch vernetzbare Medizinprodukte.

Bild 2: IT-Sicherheit vernetzter Medizinprodukte

Mit § 2 Abs. 2 wird klargestellt, dass grundsätzlich der Vorstand bzw. die Geschäftsleitung eines Krankenhauses die Verantwortung für den Betrieb und die Anwendung (und somit auch für die Instandhaltung) von Medizinprodukten trägt und nicht die Organisationsabteilungen Medizintechnik und/oder IT des Betreibers. Dies gilt in gleicher Weise für Arztpraxen, Rehabilitations- und Pflegeeinrichtungen.

Da der Vorstand bzw. die Geschäftsleitung die daraus resultierenden Detailaufgaben natürlich nicht selber wahrnimmt bzw. wahrnehmen kann, werden die jeweiligen Aufgaben in der innerbetrieblichen Organisation auf spezifische Fachabteilungen wie Einkauf, Medizintechnik, Betriebstechnik und IT über Dienstanweisungen und Stellen-/Funktionsbeschreibungen übertragen. Mit anderen Worten, wenn eine Geschäftsführung bzw. ein Vorstand diese Verantwortung und Aufgabenstellung ernst nimmt, muss die Geschäftsführung die Anforderungen der MPBetreibV in entsprechende Prozesse in der Gesundheitseinrichtung umsetzen und die diesbezüglichen Aktivitäten auch regelmäßig auf Wirksamkeit überwachen.

2. Aufgabendelegation an MT und IT

Die in § 2 Abs. 2 beschriebene Verantwortung eines Vorstandes bzw. einer Geschäftsleitung in Form von Tätigkeiten für den Betrieb und die Anwendung von

Medizinprodukten in der Gesundheitseinrichtung wird in § 3 „Pflichten des Betreiber“ sogar noch ausführlicher beschrieben und gefordert:

(1) Der Betreiber hat die ihm nach dieser Verordnung obliegenden Pflichten wahrzunehmen, um ein sicheres und ordnungsgemäßes Anwenden der in seiner Gesundheitseinrichtung am Patienten eingesetzten Medizinprodukte zu gewährleisten.

Diese Formulierung kann als Konkretisierung des § 14 des Medizinproduktegesetztes angesehen werden, nach dem Medizinprodukte nicht betrieben und angewendet werden dürfen, wenn sie Mängel aufweisen, durch die Patienten, Anwender und Beschäftigte sowie Dritte gefährdet werden können.

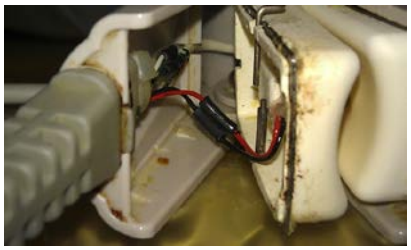
Da § 14 den Begriff des Mangels nicht weiter definiert bzw. nicht ausführt und auch die (Medizinprodukte-)Verordnungen mit Ausnahme der Medizinprodukte-Sicherheitsplanverordnung (MPSV) dazu keine weiteren Definitionen enthalten, werden aus technischer Sicht folgende Defekte, fehlende Eigenschaften wie IT-Sicherheit und fehlende Gebrauchstauglichkeit unter dem Oberbegriff Mangel subsummiert wie

- Mechanischer Mangel (z. B. Gehäusedefekt)
- Elektrischer Mangel (z. B. Überschreiten des Gehäuseableitstroms)
- Hygienischer Mangel (nicht korrekt aufbereitete Instrumente)
- Mangelnde IT-Sicherheit (z. B. Sicherheitslücken in nicht gepatchten oder veralteten Betriebssystemen wie Windows XP in vernetzbaren bzw. vernetzten Medizinprodukten)
- Mangel an Gebrauchstauglichkeit (z. B. Ein/-Ausschalter und Stand-by Schalter liegen dicht neben einander).

Mängel?

Mechanik

Hygiene



Elektrik

IT-Sicherheit

Bild 3: Mängel von Medizinprodukten nach § 14 MPG

Dies bedeutet, dass ein Betreiber Prozesse definieren und umsetzen muss, mit denen vernetzbare Medizinprodukte (mängelfrei) sicher und ordnungsgemäß beschafft, instandgehalten und angewendet werden können.
Um dies für vernetzbare Medizinprodukte zu gewährleisten, müssen Medizintechnik und IT (mit dem Einkauf) vor der Beschaffung solcher Medizinprodukte die diesbezüglichen Fragen zur IT-Sicherheit und zur dauerhaft sicheren Integration in das IT-Netzwerk der Gesundheitseinrichtung klären und bei der Instandhaltung berücksichtigen.

3. Beschaffung vernetzbarer Medizinprodukte – Fragen zur IT-Sicherheit

Wenn ein Anwender im Rahmen einer Beschaffung im Anforderungsprofil die Vernetzung eines zu beschaffenden Medizinproduktes vorsieht, dann sind vor der Beauftragung wesentliche Fragestellungen zur Instandhaltung und zur IT-Sicherheit mit den anbietenden Herstellern zu klären.
Definiert man IT-Sicherheit vernetzbarer Medizinprodukte als frei von unvertretbaren Risiken für Patienten, Anwender und Dritte gemäß § 14 des MPG, so sollten folgende diesbezügliche Fragestellungen (ohne Anspruch auf Vollständigkeit) mit den Herstellern soweit wie möglich geklärt und am besten vertraglich vereinbart werden wie

- Begründung für die bestimmungsgemäße Anbindung an IT-Netzwerke zum Datenaustausch: Inwiefern trägt die Vernetzung zum Erreichen der Zweckbestimmung bei?
- Angabe der Bezeichnung und Version eines Betriebssystems wie z. B. von Microsoft
- Offene Betriebssysteme oder „embedded“ Versionen
- Angabe zum Patchzustand bei der Auslieferung auf dem Übergabeprotokoll
- Angaben zu Lizenzübergabe bei Betriebssystemen und Produkten, z. B. von Microsoft und anderen Herstellern
- Angaben zum richtlinienkonformen Patchmanagement des verwendeten Betriebssystems (Vermeidung der Eigenherstellung nach § 12 MPG durch Patchen in eigener Verantwortung)
- Angaben zur (erlaubten oder vorgesehenen) Verwendung von Anti-Malwaresoftware
- Art der Integrierbarkeit, ggf. Möglichkeit zur Virtualisierung
- Zugangsschutz (Passwörter und USB-Anschlüsse, auch für besondere Betriebszustände wie z. B. Demo-Modus oder Service-Betrieb)
- Nachweise über IT-Sicherheit des angebotenen Medizinproduktes (Wie definiert der Anbieter „IT-Sicherheit“, wie weist er das nach, was hat man unternommen, um IT-Sicherheit zu gewährleisten, Penetrationstests u. a.)
  u. a. Fragestellungen.

Die in den letzten anderthalb Jahren aufgekommenen und immer häufiger auftretenden, ausgeklügelten Crypto-Trojaner nutzen insbesondere Sicherheitslücken von Betriebssystemen aus. Dies betrifft vor allem alte sowie ältere aber auch moderne Betriebssysteme, deren nachträglich festgestellten Sicherheitslücken nicht laufend durch Patches aktualisiert werden.
Um somit vernetzbare Medizinprodukte zu schützen und bzw. zu verhindern, dass Crypto-Trojaner u. a. Malware bekannte, nicht gepatchte Sicherheitslücken ausnutzen und somit die Verfügbarkeit dieser Medizinprodukten kompromittiert, muss die Gesundheitseinrichtung vor der Beschaffung die wesentliche Frage des Patchens von Betriebssystemen vernetzbarer Medizinprodukte mit den anbietenden Herstellern unbedingt klären. Dies bedeutet, dass ein Hersteller offen legen muss, ob und unter welchen Voraussetzungen eine Gesundheitseinrichtung ein Betriebssystem eines vernetzten Medizinproduktes patchen kann und darf, ohne die Richtlinienkonformität zu tangieren. Ansonsten verbleibt immer die Unsicherheit, ob das Patchen eines Betriebssystems eines Medizinproduktes als Eigenherstellung nach § 12 MPG mit allen Konsequenzen anzusehen ist.

Es empfiehlt sich, unbedingt auch das Thema der „Instandhaltung“ von vernetzbaren Medizinprodukten nach § 7 MPBetreibV mit Betriebssystemen und Applikationssoftware in Form von Patchmanagement und Upgrades/Updates (Recht, Pflicht, Möglichkeit) vor der Beschaffung zu klären.

Die Klärung dieser Fragestellung vor der Produktentscheidung und -beschaffung wird unter dem Aspekt der IT-Sicherheit vernetzter Medizinprodukte immer wichtiger und entscheidender.

4. Zulässige Kombination von Medizinprodukten mit anderen (IT-)Produkten

Auch wenn die MPBetreibV nach wie vor keine konkreten Anforderungen bzw. Beschreibung an die Vernetzung mit der IT-Infrastruktur einer Gesundheitseinrichtung enthält, so definiert sie doch in zwei Paragrafen Anforderungen, die einzuhalten sind, wenn Medizinprodukte mit anderen Produkten und/oder mit anderen Gegenständen wie der IT-Infrastruktur kombiniert werden. Es handelt sich dabei zum einen um den Paragrafen 4 Abs. 4 und zum anderen um den Paragrafen 4 Abs. 6.

Insbesondere Paragraf 4 Abs. 4 beschreibt die rechtlichen Anforderungen, nach denen **zulässigerweise** Medizinprodukte mit Zubehör, Software und anderen Gegenständen wie vor allem mit IT-Produkten kombiniert werden dürfen. Eine Kombination darf dann zulässigerweise vorgenommen werden, wenn ein Medizinprodukt für die Kombination mit einem anderen (IT-)Produkt unter Berücksichtigung der Zweckbestimmung geeignet ist und ein Nachweis der Eignung für die Sicherheit von Patienten, Anwender, Beschäftigten oder Dritten erbracht werden kann.

Gerätekombination nach § 4 Abs. 4

(4) Miteinander verbundene Medizinprodukte sowie mit Zubehör einschließlich Software oder mit anderen Gegenständen verbundene Medizinprodukte dürfen nur betrieben und angewendet werden, wenn sie zur Anwendung in dieser Kombination unter Berücksichtigung der Zweckbestimmung und der Sicherheit der Patienten, Anwender, Beschäftigten oder Dritten geeignet sind.

Der vorstehende Paragraf enthält also zwei Anforderungen, die vor der Kombination eines Medizinproduktes mit einem (IT-)Produkt = anderer Gegenstand nachzuweisen sind:

1. Kombination unter Berücksichtigung der Zweckbestimmung
2. Nachweis der Eignung für die Sicherheit von Patient, Anwender, Beschäftigten oder Dritten

4.1. Anforderung an eine Kombination

Paragraf 4 Abs. 4 beschreibt technikneutral die zweckbestimmte Kombination von Medizinprodukten mit anderen Produkten. Diese Kombinationen können zusammengestellt werden aus der

- Kombination eines Medizinproduktes mit einem anderen Medizinprodukt (Beispiel Überwachungsmonitor wird mit Narkosebeatmungsgerät kombiniert)
- Kombination eines Medizinproduktes mit Zubehör (Beispiel: Beatmungsgerät wird mit Schläuchen eines anderen Herstellers kombiniert)
- Kombination eines Medizinproduktes mit Software (Beispiel: Ein Ultraschallgerät wird mit einer endoskopischen Dokumentationssystem – Software kombiniert)
- Kombination eines Medizinproduktes mit anderen Gegenständen (Beispiel: Ein Medizinprodukt wie ein Ultraschallgerät wird mit einem PC und/oder über die IT-Infrastruktur einer Gesundheitseinrichtung einem Server kombiniert).

Die vorgenannten Kombinationen gelten nicht nur für einzelne Medizinprodukte sondern auch für Medizinproduktesysteme, die aus mehreren Medizinprodukten zu einem System zusammengesetzt werden.

Folgende Formen von Software können mit einem Medizinprodukt gemäß § 4 Abs. 4 kombiniert werden:

- Software Medizinprodukt (z. B. Patientendatenmanagementsysteme, PDMS, PACS)
- Applikationssoftware (z. B. Software für Ultraschallbildgebung, Geburtshilfe u. a.)
- Dokumentationssoftware (z. B. Krankenhausinformationssysteme KIS)
- Antimalware-Software (Antiviren-Software)
- Software-Agenten zur Überwachung der Verfügbarkeit von vernetzbaren Medizinprodukten
- Teilen von Betriebssystemen wie Ablageordnern für das Ablegen generierter Daten

Unter anderen Gegenständen gemäß § 4 Abs. 4 sind üblicherweise Nicht-Medizinprodukte zu verstehen wie beispielsweise:

- Rufanlage für den Schwesternruf nach VDE 0834
- Personal Computer und/oder Notebooks
- Tablets und/oder Smartphones
- Galvanische Trenner und / oder Datenkonzentratoren
- IT-Netzwerk (kabelgestützt oder über eine Funk-Infrastruktur, wie z. B. WLAN, Bluetooth)

§ 4 Abs. 4: andere Gegenstände

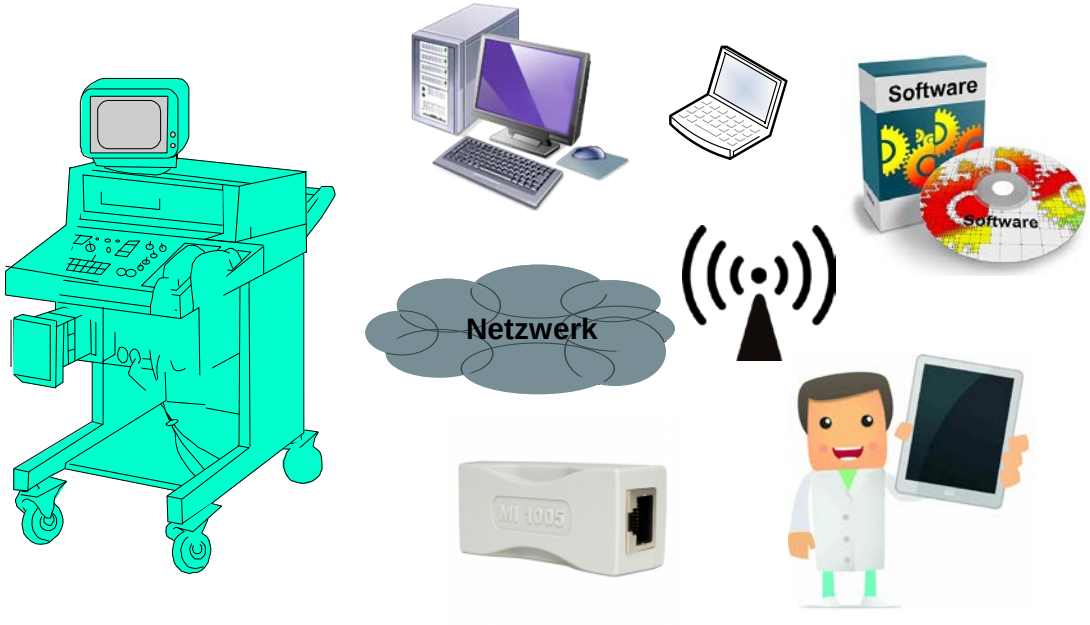


Bild 4: Anbindung MP an andere Gegenstände

Dabei vermeidet der Verordnungsgeber eine Festlegung bzw. Präzisierung des Begriffes „andere Gegenstände“, sodass der Betreiber selber entscheiden kann, ob er beispielsweise eine kabelgestützte oder WLAN-gestützte Infrastruktur verwendet. Dies setzt voraus, dass die Kombination eines Medizinproduktes mit einem IT-Produkt wie PC dafür geeignet ist, wobei die Zweckbestimmung des Herstellers zu berücksichtigen ist.
Dies bedeutet, dass der Hersteller für ein Medizinprodukt wie ein bildgebendes Ultraschallgerät nicht nur entsprechende Schnittstellen wie USB, Netzwerkanschluss, RS-232 o. a. Schnittstellen physikalisch eingebaut hat sondern auch in der erweiterten Zweckbestimmung in Form der Gebrauchsanweisung die Anbindung an datenverarbeitende Systeme beschreibt.

Dazu muss sich der Hersteller des Kapitels 14.13 der DIN EN 60601-1 bedienen, das inhaltlich Angaben enthält, wie eine Verbindung von einem Medizinprodukt zu anderen Geräten durch ein Netzwerk und/oder Datenverbund gestaltet werden muss. Diese Angaben muss der Hersteller in der Gebrauchsanweisung bzw. technischen Beschreibung mitliefern; in der Praxis zeigt sich, dass dies nicht immer der Fall ist.

Wenn dies so erfolgt und in den Unterlagen eines Herstellers zu einem Medizinprodukt enthalten ist, dann kann eine IT-Abteilung einer Gesundheitseinrichtung im Rahmen der Zweckbestimmung zulässigerweise das

Medizinprodukt mit anderen IT-Gegenständen bzw. dem IT-Netzwerk für einen Datenaustausch kombinieren.

4.2. Nachweis der Eignung der Kombination für die Sicherheit (Risikomanagement)

Paragraf § 4 Abs. 4 der Verordnung fordert vom Betreiber, immer die Eignung der Sicherheit einer solchen Kombination (wie mit IT-Produkten und/oder dem IT-Netzwerk eines Krankenhauses) nachzuweisen. Diesen Nachweis führt man sinnvollerweise, indem man die Unterlagen aller kombinierten Produkte durchsieht, die Zweckbestimmung und Angaben der Hersteller zu zulässigen Kombination oder aber Ausschlüssen zusammenstellt und dann ein Risikomanagement über die möglichen Kombinationen durchführt.
Das Risikomanagement betrachtet sämtliche Gefährdungen, die in Verbindung mit der analysierten Gerätekombination für Patienten und Anwender auftreten können bzw. beschreibt Maßnahmen zu deren Reduzierung.
Sinnvollerweise führt man alle diese Unterlagen und das Risikomanagement in Form einer Technischen Dokumentation zusammen.

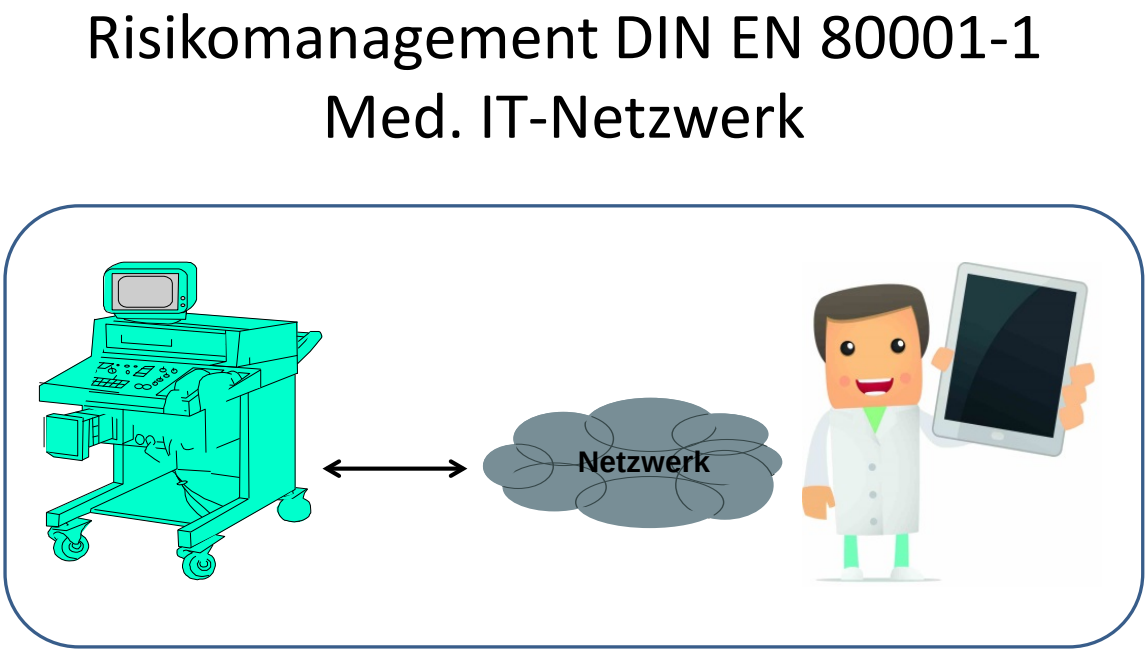


Bild 5: DIN EN 80001-1 für vernetzte Medizinprodukte

Da § 4 Abs. 4 keinerlei Angaben zu Form, Inhalt und Umfang des Risikomanagements beinhaltet, empfiehlt es sich, bei der Vernetzung von Medizinprodukten mit dem IT-Netzwerk einer Gesundheitseinrichtung die Norm DIN

EN 80001-1 heranzuziehen. Da die DIN EN 80001-1 nur die Netzwerkanbindung betrachtet, ist es sinnvoll, für eine Gerätekombination ohne Netzwerkanbindung die Risikomanagementnorm DIN EN 14971 zu nutzen.

Dabei zu beachten ist § 4 Abs. 6, der darüber hinaus fordert, die Sicherheit „in der jeweiligen Kombination“ nachzuweisen. Das wird eine wiederkehrende Aufgabe für solche Medizinprodukte sein, die ortsveränderlich sind und an verschiedenen Schnittstellen ins IT-Netzwerk integriert werden können sowie für den Fall, dass verschiedene Kombinationen von Medizinprodukten und sonstigen Produkten/Geräten je nach Anwendungsfall gewählt werden können.
Darunter fällt auch ein temporärer Einsatz von Sicherheitslösungen wie z. B. regelmäßig geplanter Einsatz (z. B. Scan) von Antiviren-Software, Netzwerk-Komponenten-Erkennungsdiensten, IDS oder IPS-Produkten (Intrusion Detection System bzw. Intrusion Prevention System). Mitunter hilft an dieser Stelle nur ein geeignetes IT-Event-Management.

4.3. Einweisungsverpflichtung von Kombinationen nach § 4 Abs. 3

Der Verordnungsgeber hat auch die Verpflichtung zur Einweisung neu geregelt. Waren in der bisherigen Fassung der MPBetreibV nur Medizinprodukte gemäß Anlage 1 einweisungspflichtig, so sind nun gemäß § 4 Abs. 3 der Verordnung prinzipiell alle Medizinprodukte einzuweisen, es sei denn, sie sind selbsterklärend oder aber es handelt sich um bauartgleiche Medizinprodukte, für die bereits eine Einweisung erfolgt ist. Im Zweifel ist die Eignung zur Selbsterklärung nachzuweisen.
Auch wenn der Verordnungsgeber aus unbekannten Gründen Gerätekombinationen nach § 4 Abs. 4 nicht ausdrücklich in die Einweisungsverpflichtung mit einbezogen hat, so ergibt sich eine solche Verpflichtung sinngemäß aus den Forderungen des § 4.

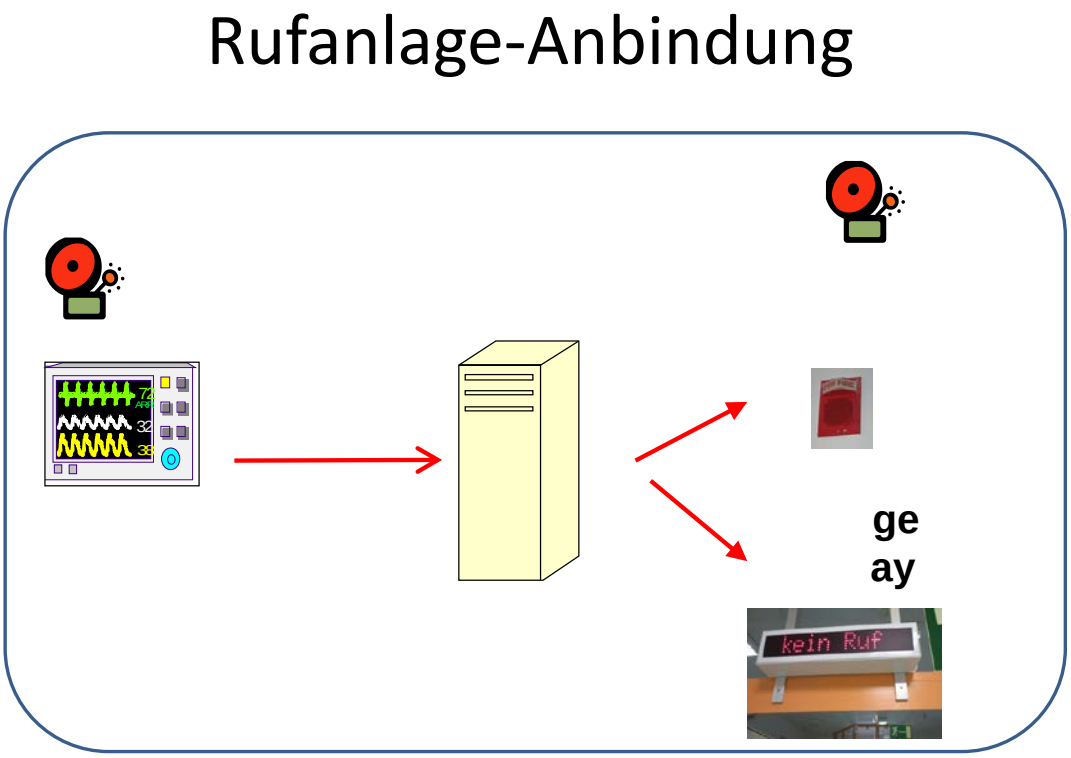


Bild 6: Anbindung Medizinprodukt Anlage 1 an anderen Gegenstand

Dementsprechend ist eine Gesundheitseinrichtung gut beraten, auch Gerätekombinationen einzuweisen, wenn diese aus Medizinprodukt(en) und anderen Gegenständen wie (IT-)Produkten bestehen. Dies ist insbesondere dann der Fall, wenn Medizinprodukte z. B. mit Rufanlagen zu sog. Verteilten Alarm- oder Informationssystemen kombiniert werden, bildgebende Medizinprodukte medizinische Daten auf Server im IT-Netzwerk schicken, Informationen z. B. über den Workflow erhalten und schicken, u. a. komplexe Integrationsprojekte wie die Anbindung der aktiven Medizinprodukte einer Intensivstation an ein PDMS.

4.4. Funktionsprüfung

Auch wenn die MPBetreibV keine Einweisung für Kombinationen gemäß § 4 Abs. 4 verlangt, so schreibt sie dennoch mit § 4 Abs. 6 dezidiert für solche Kombinationen eine Funktionsprüfung vor:

Abs. 4 (6) Der Anwender hat sich vor dem Anwenden eines Medizinproduktes von der Funktionsfähigkeit und dem ordnungsgemäßen Zustand des Medizinproduktes zu überzeugen und die Gebrauchsanweisung sowie die sonstigen beigefügten sicherheitsbezogenen Informationen und Instandhaltungshinweise zu beachten. ***Satz 1 gilt entsprechend für zur Anwendung miteinander verbundene Medizinprodukte, für Zubehör einschließlich Software oder andere***

Gegenstände, die mit Medizinprodukten zur Anwendung verbunden sind, sowie für die jeweilige Kombination.

Mit diesem Paragrafen hat der Verordnungsgeber zwei wesentliche Anforderungen festgelegt:

1) Der Anwender (Ärzte, Pflegepersonal) müssen sich vor der Anwendung von der Funktionsfähigkeit und dem ordnungsgemäßen Zustand des Medizinproduktes (und im Sinne dieses Paragrafen auch von Systemen und Kombinationen) überzeugen.

2) Damit Anwender eine Funktionsprüfung einer Kombination durchführen können, muss der Betreiber sicherstellen, dass auch Kombination von Medizinprodukten mit anderen Produkten, Software und/oder Gegenständen eingewiesen werden. Dies gilt somit auch für vernetzbare Medizinprodukte in der Vernetzung mit dem IT-Netzwerk.

Zu einer Funktionsprüfung und zu einer Einweisung von vernetzten Medizinprodukten und vernetzten Medizinprodukte-Systemen bzw. Kombinationen gehören daher aus Sicht des Verfassers auch Hinweise und Informationen zu einem sicheren Umgang bezüglich IT-Komponenten und bezüglich IT-Sicherheit.
Diese Sicherheitshinweise sollten in einer IT-Sicherheitsschulung den Mitarbeitern einer Gesundheitseinrichtung (regelmäßig) vermittelt werden. Ein vollständiger Funktionsnachweis kann für den Anwender u.a. eine nicht zu leistende Aufgabe darstellen. Hier sind die Hersteller gefragt, z. B. durch Funktionsprüfroutinen (z. B. Selbsttests) geeignete Hilfen anzubieten.

5. Instandhaltung von (vernetzbaren) Medizinprodukten nach § 7 MPBetreibV

Der Verordnungsgeber hat die Anforderungen an den Nachweis der Sicherheit von Kombinationen von Medizinprodukten mit anderen Gegenständen (wie IT-Produkten) und deren Einweisung im Paragraf 4 beschrieben. Diese Anforderungen für Gerätekombinationen setzt sich aber merkwürdigerweise nicht in der gleichen Klarheit im Paragrafen 7 „Instandhaltung von Medizinprodukten“ fort. Die Anforderungen gelten nur für Medizinprodukte; eigentlich würde man erwarten, dass der Verordnungsgeber die Anforderungen an Instandhaltungen auch für die immer zahlreicher vorhandenen Kombinationen und Systeme in Gesundheitseinrichtungen entsprechend formuliert.

§ 7 Abs. 1 fordert, dass erforderliche Inspektionen und Wartungen durchzuführen sind, um den sicheren und ordnungsgemäßen Betrieb von Medizinprodukten fortlaufend zu gewährleisten. Es ist davon auszugehen, dass der Verordnungsgeber auch vernetzbare Medizinprodukte in die Forderung nach Instandhaltung mit einbezieht.

Dieser Schluss wird auch deswegen gezogen, weil § 11 der Verordnung sicherheitstechnische Kontrollen für Gerätekombinationen fordert, wenn der Betreiber Medizinprodukte der Anlage 1 der Verordnung mit anderen Medizinprodukten, Software und/oder anderen Gegenständen kombiniert.

5.1 Begriffe der Instandhaltung nach DIN 31051

Zu den in § 4 Abs. 1 der MPBetreibV erwähnten anerkannten Regeln der Technik gehört auch die DIN 31051 „Grundlagen der Instandhaltung“. Sie beschreibt die Grundmaßnahmen der Instandhaltung und deren Zusammenhänge für Produkte im Sinne von mechanisch-technischen Geräten.
Sie enthält allerdings keine Definition und Begriffe für die „Instandhaltung“ von Geräten mit Software wie Betriebssystemen und Applikations-Software, sodass diese Norm nur indirekt für die „Instandhaltung“ vernetzter Medizinprodukte heranzuziehen ist.

5.2 Unterscheidung Instandhaltung Medizintechnik – Verfügbarkeit IT

Das Medizinproduktegesetz und die darauf basierenden Verordnungen sind nach wie vor mit dem Fokus auf mechanisch-technische Geräte in Form von Medizinprodukten geschrieben und berücksichtigen die weitgehende Ausstattung und Vernetzung von Medizinprodukten mit Software, Betriebssystemen und IT-Netzwerken nur sehr technikneutral bzw. rudimentär.
Auch die MPBetreibV ist aus Sicht der klassischen Instandhaltung von mechanisch-technischen Produkten geschrieben, sodass auch die entsprechenden Regeln der Technik, die für die Instandhaltung herangezogen werden müssen, weitgehend nur medizinische elektrische Geräte (ME-Geräte) und Systeme (ME-Systeme) beschreiben.
Während die Medizintechnik von Instandhaltung in Form von Wartungen, Prüfungen und Instandsetzungen mechanisch oder elektrisch defekter Geräte spricht, verwendet die IT-Welt die folgenden Begriffe wie

- IT-Betrieb
- Verfügbarkeit bzw. Wiederherstellung der Verfügbarkeit
- Upgrades/Updates bzw. Releasewechsel
- Migration von Software und Betriebssystemen
- Instandhaltung von Hardwarekomponenten durch Austausch, oft nicht durch identische Komponenten möglich (Verfügbarkeit)

5.3 Instandhaltung von vernetzbaren Medizinprodukten nach § 7 MPBetreibV

Überträgt man die Begriffe der Instandhaltung der Medizintechnik auf vernetzbare Medizinprodukte bzw. Gerätekombinationen aus Medizinprodukten und IT-Produkten, so lassen sich aus folgende Anforderungen (ohne Anspruch auf

Vollständigkeit) definieren, um durch Instandhaltung eine sichere und ordnungsgemäße Anwendung zu gewährleisten:

- Regelmäßige Prüfung der elektrischen Sicherheit von IT-Komponenten
- Regelmäßiges Patchen von Betriebssystemen zur Vermeidung von Sicherheitslücken (offene Betriebssysteme, nicht embedded)
- Schutz vor Malware bzw. Antimalware
- Präventiver und korrektiver Austausch von Festplatten u. a. Komponenten
- Überwachung von vernetzten Medizinprodukten durch Netzwerkmanagement mit Software-Agenten
- Upgrade/Update von Software
- Betriebssystemwechsel durch Migration
- Betriebssystem-Upgrade (z. B. von Windows 7 auf Windows 10)
- Virtualisierung und Hochverfügbarkeit von Software als Medizinprodukt (Verschieben einer virtuellen Maschine im laufenden Betrieb auf eine andere physikalische Hardware)

Häufig ist bei der „Instandhaltung“ vernetzbarer Medizinprodukte unklar, ob der Betreiber bzw. eine IT-Abteilung derartige Aktivitäten an solchen Medizinprodukten durchführen kann und / oder darf. Dabei geht es um die Fragestellung, ob ein Betreiber bei einem Betriebssystemwechsel von z. B. Windows 7 auf Windows 10 ein vernetzbares Medizinprodukt soweit ändert, dass eine Neubewertung der Konformität nach der Medizinprodukte-Richtlinie durchgeführt werden muss.

Mit anderen Worten, die IT-Abteilungen stellen häufig die Frage, mit welchen Maßnahmen sie die Grenze der „zulässigen“ Instandhaltung von vernetzbaren Medizinprodukten gemäß MPBetreibV durch eine wesentliche Änderung zur Eigenherstellung nach 12 MPG überschreiten.

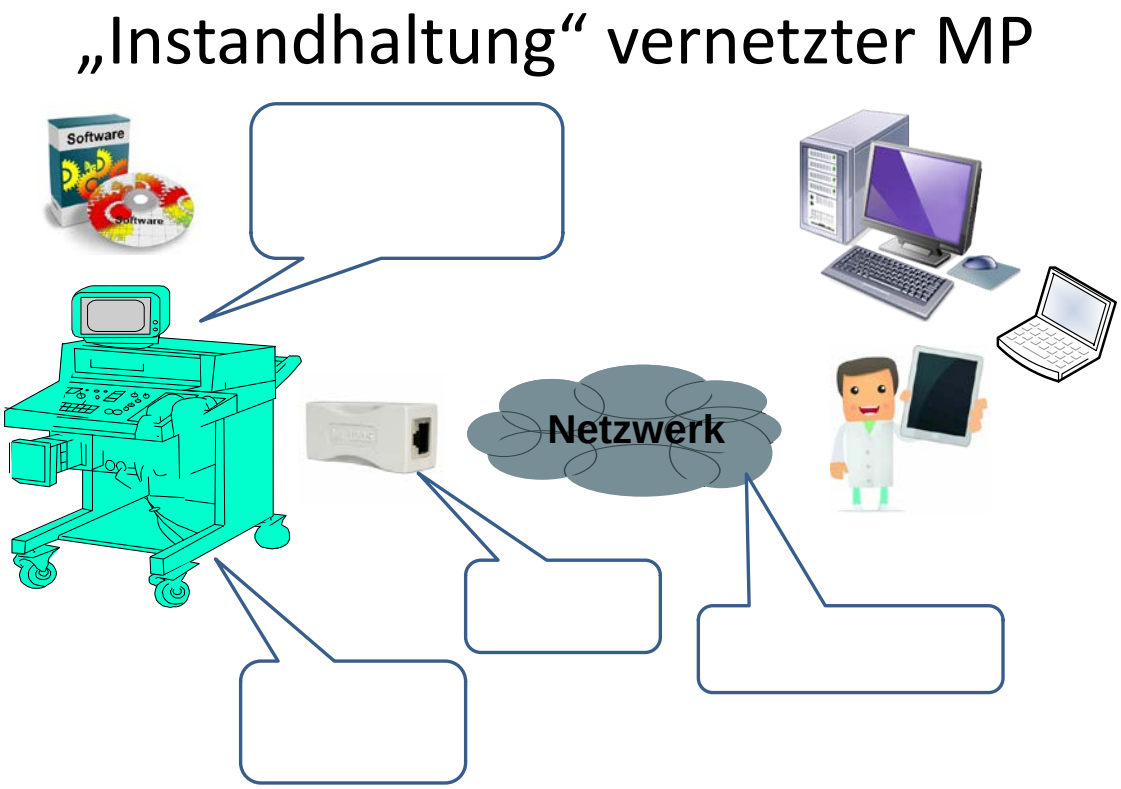


Bild 7: Instandhaltung vernetzter Medizinprodukte

Um diese u. a. Fragestellungen handlungssicher zu beantworten, müssen diese Fragen vor der Beschaffung mit dem oder den Hersteller(n) geklärt werden. Hier sei insbesondere auf den § 7 der MPBetreibV verwiesen, nach die Instandhaltung von Medizinprodukten unter Berücksichtigung der Angaben des Herstellers durchzuführen sind, der diese Angaben dem Medizinprodukt beizufügen hat.

IT-Abteilungen sollten unbedingt diese Anforderungen des § 7 Abs. 1 der MPBetreibV in Form der vorgenannten beispielhaften Fragen der „Instandhaltung“ von vernetzbaren Medizinprodukten mit den anbietenden Herstellern vor der Beschaffung klären. Allerdings ist in der Praxis häufig festzustellen, dass Hersteller diese Regelung nicht kennen und auch nicht auf sich beziehen, mit der Begründung, dass die Verordnung ja Aufgaben und Pflichte der Betreiber gemäß § 2 Abs. 2 regelt und daher nicht für Hersteller gelte.

6. STK an (vernetzten) Medizinprodukten und Gerätekombinationen

Mit der novellierten MPBetreibV hat der Verordnungsgeber nicht nur dem Betreiber die Festlegung von Fristen und Inhalten sicherheitstechnischer Kontrollen übertragen sondern auch diese Kontrollen auf bestimmte Gerätekombinationen erweitert. Wenn ein Medizinprodukt, das in Anhang 1 der Verordnung aufgeführt wird, mit anderen Medizinprodukten, Zubehör, Software oder anderen Gegenständen kombiniert wird,

dann ist für eine solche Kombination eine sicherheitstechnische Kontrolle inhaltlich zu definieren und mindestens alle zwei Jahre durchzuführen, unter voller Berücksichtigung der berufsgenossenschaftlichen Unfallverhütungsvorschriften.

Wenn also beispielsweise ein Beatmungsgerät auf einer Intensivstation über ein IT-Netzwerk an ein klinisches Informationssystem wie einem Patientendatenmanagementsystem (PDMS) angeschlossen ist, dann fällt diese Kombination unter die Pflicht zur Durchführung einer sicherheitstechnischen Kontrolle nach § 11 MPBetreibV. Das ist nachvollziehbar, wird es doch zunehmend möglich, einzelne, speziell analytische und auswertende Tätigkeiten von Medizinprodukten in eine angeschlossene Software zu verlegen.
Die gleiche Anforderung ergibt sich, wenn eine Spritzenpumpe als Produkt des Anhang 1 der Verordnung an eine Rufanlage angeschlossen wird. Auch für diese Kombination muss der Betreiber Inhalte und Fristen für eine sicherheitstechnische Kontrolle nach § 11 der Verordnung festlegen und durchführen (lassen).

7. IT-Sicherheit vernetzbarer Medizinprodukte

Die seit dem Jahr 2016 zunehmend auftretenden sogenannten Crypto-Trojaner (Ransomware) haben dazu geführt, dass die IT-Infrastruktur von Gesundheitseinrichtungen massiv beeinträchtigt wurde, indem Server und medizinische Datenbestände in erpresserischer Weise durch eingeschleuste Schadsoftware verschlüsselt wurden. Damit war die Verfügbarkeit der medizinisch und pflegerisch genutzten IT-Infrastruktur in den betroffenen Einrichtungen nicht mehr gegeben, wodurch sich massive Einschränkungen in der Versorgung von akut erkrankten Patienten bzw. in Notfällen ergaben.
Auch wenn es bisher (noch) keine gezielten Hackversuche auf in Betrieb befindliche vernetzte Medizinprodukte gegeben hat, ist damit zu rechnen, dass derartige Attacken kommen werden und dass Malware in Zukunft auch vernetzbare Medizinprodukte befällt, insbesondere, wenn diese über ältere Betriebssysteme und/oder nicht laufend durch Patches aktualisierte Betriebssysteme verfügen. Ein Hersteller solcher Medizinprodukte muss angeben, wie ein Betreiber mit diesen Gefährdungen umgehen soll und muss.
Um derartige Attacken und damit verbundene Ausfälle und mögliche Gefährdungen für die Patientenversorgung soweit wie möglich zu vermeiden, muss ein Betreiber die Forderung der MPBetreibV, einen sicheren und ordnungsgemäßen Betrieb und Anwendung von vernetzbaren Medizinprodukten zu gewährleisten, entsprechende Maßnahmen ergreifen, um die IT-Sicherheit vernetzbarer Medizinprodukte laufend zu verbessern und zu aktualisieren.

Trotz der zunehmenden Vernetzung von Medizinprodukten mit der IT-Infrastruktur und der daraus resultierenden Fragestellungen zur Instandhaltung und IT-Sicherheit hat der Verordnungsgeber dieser Entwicklung in der Novellierung der MPBetreibV zum 01.01.2017 leider nicht berücksichtigt.

8. Zusammenfassung und Empfehlungen

Auch wenn die novellierte MPBetreibV keine konkret formulierten Anforderungen für vernetzte Medizinprodukte und Gerätekombinationen mit IT-Vernetzung beinhaltet, so ergeben sich dennoch eine Reihe von Konsequenzen für die Beschaffung und Instandhaltung vernetzbarer Medizinprodukte und Kombinationen.
Die zentrale Forderung der Verordnung an den Betreiber, eine sichere und ordnungsgemäße Anwendung von (vernetzten) Medizinprodukten zu gewährleisten, muss der Betreiber (Vorstand, Geschäftsleitung) durch entsprechende Prozesse, Organisationsstrukturen und Aufgabenstellungen an den Einkauf, die Medizintechnik und IT einer Gesundheitseinrichtung umsetzen. Dies beinhaltet auch die Notwendigkeit, die Mitarbeiter bezüglich dieser Themen permanent und laufend weiterzubilden sowie die notwendigen Ressourcen zur Verfügung zu stellen.

Das Thema der sogenannten Cyber-Sicherheit in Gesundheitseinrichtungen zeigt sehr deutlich, dass Betreiber der „Instandhaltung“, dem sicheren, mängelfreien Betrieb und damit der Verfügbarkeit von vernetzten Medizinprodukten deutlich mehr Aufmerksamkeit schenken müssen als bisher.
Dies läßt sich nur dadurch erreichen, dass MT und IT

1. konsequent in die Beschaffungsprozesse vor Auftragserteilung eingebunden sind und ein Vetorecht zur Ablehnung von als nicht sicher beurteilten Produkten haben,
2. die sichere Integration vernetzter Medizinprodukte als Projekt mit einem Risikomanagement durchführen und begleiten, und
3. bezüglich der „Instandhaltung“ vernetzter Medizinprodukte eng zusammenarbeiten.

Mit einem solchen Prozessmanagement kann ein Vorstand bzw. eine Geschäftsleitung eines Krankenhauses seine rechtliche Verpflichtung nach § 2 Abs. 2 und § 3 Abs. 1 der Verordnung erfüllen, eine sichere und ordnungsgemäße Anwendung von (vernetzbaren) Medizinprodukten zu gewährleisten.

Stand 15.08.2017

Anschrift des Verfassers
Armin Gärtner
Ingenieurbüro für Medizintechnik
Ö. b. u. v. Sachverständiger für Medizintechnik und Telemedizin
Edith-Stein-Weg 8
40699 Erkrath
E-Mail: armin.gaertner@t-online.de

Der vollständige Beitrag erscheint im Fortsetzungswerk MIT der TÜV Media GmbH in der 26 Ergänzungslieferung.

Diese Publikation ist ein Auszug aus dem gleichnamigen Beitrag des Fortsetzungswerkes Medizintechnik und Informationstechnologie digital - MIT - Konzepte, Technologien, Anforderungen - TÜV Media GmbH, Köln.
Die vollständige Fassung erscheint vrsl. in der 26 Ergänzungslieferung des Fortsetzungswerkes im Dezember 2017.