ZVEI: Die Elektroindustrie

Positionspapier

IT-Sicherheit in Medizintechnik und Krankenhaus-IT

Januar 2017

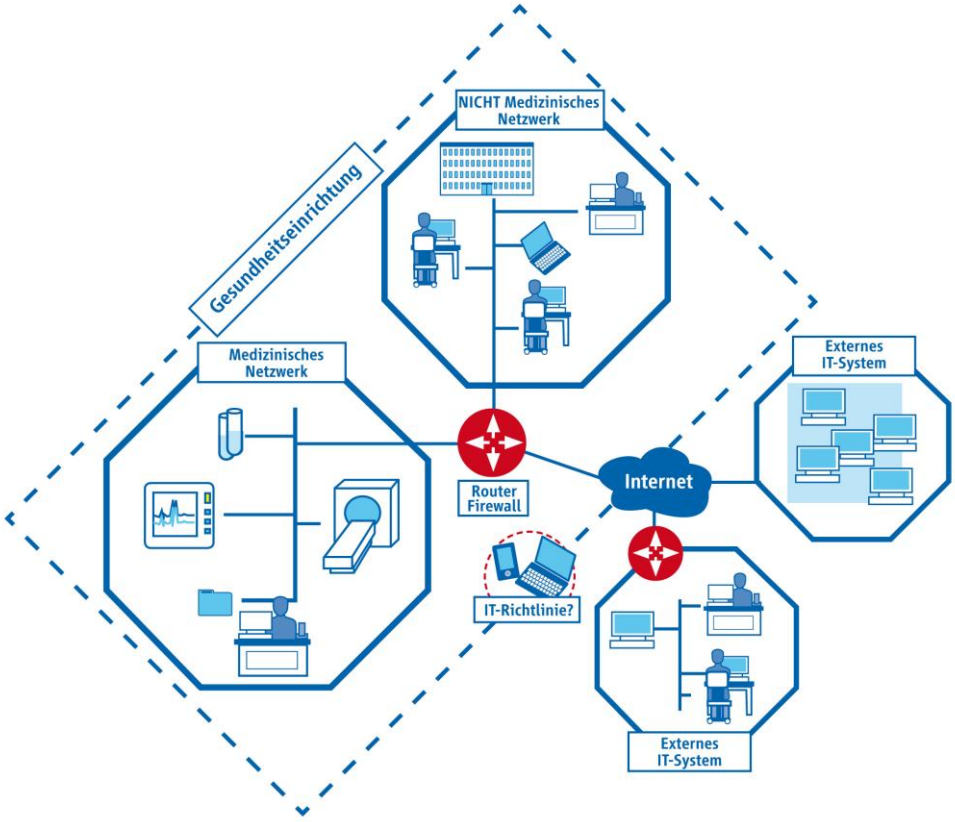
Zentralverband Elektrotechnik- und Elektronikindustrie

Daten und Systemsicherheit

Viele Unternehmen im Gesundheitswesen haben ihre Anlagen und Geräte automatisiert und vernetzt.

Die Vorteile liegen auf der Hand: Offenheit zwischen Administration und Leistungserbringung sowie verbesserte Transparenz und Durchgängigkeit der Datenströme können effizientere Leistungserbringungen ermöglichen. Diese Automatisierung und Vernetzung birgt allerdings auch Risiken, was sich bei der Betrachtung der verschiedenen Installationen in den unterschiedlichsten Umgebungen zeigt.

Typischerweise wird zwischen externen IT-Systemen, internen IT-Systemen sowie Systemen mit integrierten Medizinprodukten unterschieden.



Quelle: ZVEI

Interne IT-Systeme befinden sich grundsätzlich innerhalb der Gesundheitseinrichtung und sind mit dem IT-Netzwerk der Einrichtung verbunden. Dazu gehören Verwaltungssysteme, Archivierungssysteme und allgemeine Kommunikationssysteme (RIS, KIS, PACS).

Externe IT-Systeme befinden sich physisch nicht nur innerhalb der Gesundheitseinrichtung, sondern können an wechselnden Orten, also innerhalb oder außerhalb der Gesundheitseinrichtung und mit den unterschiedlichsten IT-Netzwerken, also auch am IT-System einer Gesundheitseinrichtung oder über ein Mobilfunknetzwerk, betrieben werden. Beispiele sind IT-Geräte mit Remotezugriff, portable Datenträger, externe Speichermedien und vergleichbare Geräte.

Zu den Systemen mit integrierten Medizinprodukten gehören u. a. PC-basierte Medizinprodukte, medizinische Software-Produkte oder andere aktive Medizinprodukte.

Allen ist gemeinsam, dass sie durch ihre Offenheit potentielle Einfallstore für Schadsoftware im Allgemeinen sind und diese aufgrund automatischer Vernetzung auch optimal weiter verbreiten können.

Dabei ist Schadsoftware jede Form von Software, die nicht gewünschte Auswirkungen auf das IT-System oder das Medizinprodukt hervorruft und damit zu einer Gefährdung von z. B. Patienten führen könnte.

Eintrittspforten für Schadsoftware

Schadsoftware kann auf verschiedenen Wegen in ein medizinisches Netzwerk gelangen. Häufig wird sie sogar durch den Anwender selbst eingebracht, z. B. über CDs/DVDs, USB-Speichermedien, E-Mail-Anhänge oder Internet-Verbindungen ohne ausreichenden Virenschutz. Besteht keine sichere Trennung des medizinischen Netzwerks von der übrigen IT-Infrastruktur oder zu externen Systemen, kann Schadsoftware auch von dort in das medizinische Netzwerk gelangen.

Um diesen Gefahren zu begegnen, ergreifen Betreiber häufig eigene Schutzmaßnahmen, ohne sich bewusst zu sein, dass gerade solche Maßnahmen das ordnungsgemäße Funktionieren der IT-Systeme gefährden können.

Unkontrollierte oder automatische, vom Medizinproduktehersteller nicht autorisierte Softwareupdates (z. B. für Virenschutz, Betriebssystem oder sonstige Anwendungssoftware) können die ins Netzwerk eingebundene Medizinprodukte in ihrer Funktion beeinträchtigen und somit möglicherweise Patienten gesundheitlich schädigen.

Gesetzlicher Hintergrund

Grundsätzlich dürfen in Europa nur Produkte in Verkehr gebracht werden, wenn sie die Anforderungen der anwendbaren EU-Richtlinien erfüllen (z. B. MDD, R&TTED, RED, LVD). Medizinprodukte dürfen in Europa entsprechend der MDD, Anhang I (1) nur in Verkehr gebracht werden, wenn ihre Anwendung unter den vorgesehenen Bedingungen und zum vorgesehenen Zweck die Gesundheit und die Sicherheit der Patienten, Anwender oder von Dritten nicht gefährdet. Dieser Grundsatz gilt dementsprechend in allen Mitgliedsstaaten der EU. Darüber hinaus gelten auch die jeweiligen Regelungen zur Produkthaftung und zum Schutz personenbezogener Daten (95/46/EG).

Verpflichtungen für Hersteller

Hersteller von Medizinprodukten, die für ihre Medizinprodukte die Verwendung in IT-Netzwerken erwarten oder vorhersehen, müssen bereits während des Designs mögliche Risiken, die an den Schnittstellen denkbar sind, hinsichtlich ihres Gefährdungspotentials bewerten und entsprechende Minimierungsmaßnahmen definieren und implementieren. Sollte dies technisch nicht möglich sein, dann muss der Anwender bzw. der Patient hinreichend über diese Gefährdungen informiert werden, z. B. in der Gebrauchsanweisung.

Verpflichtungen für Betreiber

Betreiber (z. B. Krankenhäuser, medizinische Einrichtungen, Arztpraxen) dieser Medizinprodukte und IT-Netzwerke sind verpflichtet, bereits bei der Installation und Inbetriebnahme sich über evtl. Gefährdungen aller Art bei den involvierten Herstellern (z. B. Netzwerkkomponenten, Software, Medizinprodukte) zu informieren und geeignete Maßnahmen in ihrer eigenen Organisation zu entwickeln, festzulegen und umzusetzen. Dazu gehören sowohl technische Maßnahmen als auch organisatorische Maßnahmen, z. B. die Festlegung und Implementierung von Richtlinien zur Nutzung der IT.

Maßnahmen zur Sicherung des Netzwerkes

Der Bedrohung des IT-Netzwerkes kann mit einer Vielzahl von Maßnahmen begegnet werden, ohne die gesetzlichen Vorgaben für Medizinprodukte zu verletzen bzw. Eigenhersteller im Sinne des MPG zu werden.

Die Maßnahmen gliedern sich in organisatorische Maßnahmen, Anpassung der Netzwerkarchitektur und Systemabsicherung. Beispiele dafür sind:

- Regelmäßige Schulung der Mitarbeiter, um durch das Aufzeigen von Risiken die Wahrscheinlichkeit für Schadsoftwarebefall zu reduzieren.
- Klare Strukturierung des Netzwerkes, um medizinische von nicht-medizinischen Netzwerkbereichen zu trennen. Die notwendigen Verbindungen sollten über wenige, aber gut gewartete Gateways erfolgen. Siehe Kasten rechts.
- Schutzsoftware (Virenscanner, Firewall etc.) auf nicht-medizinischen Systemen installieren, um deren Infektion und die nachfolgende Verbreitung von Schadsoftware im medizinischen Netz zu verhindern.
- Installation von Portblockern an den Schnittstellen zwischen einzelnen Systemen, z. B. USB, so dass nur zwingend benötigte Medien Zugang erhalten. Dies gilt auch für Medizinprodukte.

Als Maßnahmen für den sicheren Betrieb von vernetzten Medizingeräten schlagen wir insbesondere die Einrichtung getrennter, abgesicherter medizinischer Subnetze vor. Im Rahmen eines umfassenden Sicherheitskonzepts (etwa nach einem der folgenden Standards: ISO/IEC 27002 / ISO 27799 / IEC 62443 / IT-Grundschutz) für das klinische IT-Netzwerk sollten dabei für jedes „sichere medizinische Subnetz“ folgende Sicherheitsverfahren umgesetzt werden:

IDENTIFY: Erkennen von Schutzgütern in medizinischen Subnetzen
PROTECT: Schutz vor unerlaubten oder unerwünschten Szenarien
DETECT: Erkennen von unerlaubten oder unerwünschten Szenarien
RESPOND: Reaktion auf unerlaubte oder unerwünschte Szenarien
RECOVER: Wiederherstellung nach unerlaubten oder unerwünschten Szenarien

Für weiterführende Informationen verweisen wir auf das Positionspapier zu sicheren medizinischen Subnetzen.

- FMEAs oder einschlägige Risikomanagementprozesse als geeignete und bewährte methodische Ansätze nutzen.

Dies sind einzelne wesentliche Maßnahmen, die prinzipiell in jeder medizinischen IT-Umgebung umgesetzt werden sollten. Jedoch ist jede Infrastruktur anders, so dass eine individuelle Beratung zur Erarbeitung optimaler Lösungen erforderlich ist.

Hilfestellung für eine risikobewusste Integration der Medizinprodukte in das IT-Netzwerk gibt neben den Normen ISO/IEC 27001 (information technology – information security management systems) und ISO/IEC 29100 (information technology – security framework) auch die Norm IEC 80001-1. In der Norm IEC 80001-1 wird beschrieben, wie eine Risikoanalyse und die daraus abgeleiteten Maßnahmen das Risiko für Schadsoftwarebefall und -ausbreitung in einem IT Netzwerk minimieren kann bzw. wie Prozesse für den Ernstfall definiert werden. Wichtige Randbedingungen sind:

- Bei der Erstellung eines Maßnahmenkataloges müssen die gesetzlichen Anforderungen, beispielsweise der MPBetreibV, berücksichtigt werden.
- Die technischen Möglichkeiten sind immer im Zusammenhang mit dem Verwendungszweck und den gesetzlichen Anforderungen abzugleichen.

Zu beachten ist: jede Aktualisierung der Soft- oder Hardware von Medizinprodukten bedarf immer einer erneuten Verifikation und Validierung, bevor das Produkt wieder eingesetzt werden darf bzw. wieder in einem IT-Netzwerk betrieben werden darf.

Fazit

IT-Systeme und ihre Vernetzung sind sowohl aus dem Alltag, wie auch aus dem Gesundheitswesen nicht mehr weg zu denken. Damit können jedoch im klinischen Umfeld besondere Risiken und Gefährdungen für Patienten und Anwender sowie Dritte verbunden sein, die die besondere Aufmerksamkeit insbesondere der Betreiber erfordert.

Besondere Vorsicht ist geboten bei der Definition und Implementierung von Sicherheitskonzepten, die auf lokalen Regelungen und Initiativen beruhen. Die inhärente Sicherheit von Medizingeräten darf dadurch nicht abgeschwächt werden oder inkompatibel zu anderen Regelungen werden. Diese Sicherheitskonzepte müssen zunächst transparent und unter Einbeziehung aller betroffenen Parteien bzw. Organisationen konsensorientiert erarbeitet werden. Danach müssen sie regelmäßig gewartet, überprüft und wo notwendig verbessert werden, um den Anforderungen kontinuierlich zu genügen. Das erforderliche Sicherheitsniveau kann nur erreicht werden, wenn alle Beteiligten ihrer Verantwortung gerecht werden und ihre Punkte direkt und mit Mitspracherecht adressieren können.

Abkürzungen:

R&TTED Radio and Telecommunication Terminal Equipment (R&TTE) Directive (1999/5/EC)

RED Radio Equipment Directive (RED) (2014/53/EU)

LVD Low Voltage Directive (2006/95/EC) and (2014/35/EC)

MDD Medical Device Directive (93/42/EG)

MPG Medizinproduktegesetz

FMEA Fehler-Möglichkeits- und Einfluss-Analyse

ZVEI - Zentralverband Elektrotechnik-
und Elektronikindustrie e. V.
Fachverband Elektromedizinische Technik
Lyoner Straße 9
60528 Frankfurt am Main

Ansprechpartner:
Hans-Peter Bursig, ZVEI
Telefon +49 69 6302-206
E-Mail: bursig@zvei.org
www.zvei.org

4. Auflage Januar 2017

Das Positionspapier entstand unter der Federführung des Arbeitskreis Medical IT & Communication Systems – MICS im ZVEI-Fachverband Elektromedizinische Technik.