zvei
electrifying ideas

Positionspapier

Cybersicherheit von Medizintechnik in Gesundheitseinrichtungen

Verband der Elektro- und Digitalindustrie

1 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 ermöglichen eine effizientere Leistungserbringung. Diese Automatisierung und Vernetzung bergen allerdings auch Risiken, was sich bei der Betrachtung der verschiedenen Installationen in den unterschiedlichsten Umgebungen zeigt.
Typischerweise wird zwischen externen IT-Systemen und internen IT-Systemen unterschieden. Letztere können medizinische Netzwerke (IT-Systeme mit integrierten Medizinprodukten) enthalten.

Interne IT-Systeme befinden sich grundsätzlich innerhalb eines geschlossenen Netzwerkes der Gesundheitseinrichtung, welches sowohl lokale Netze als auch Anbindungen an Cloud-Lösungen umfassen kann. Dazu gehören Verwaltungssysteme, Archivierungssysteme, elektronische Patientenakten und allgemeine Kommunikationssysteme (RIS, KIS, PACS).

Externe IT-Systeme befinden sich außerhalb des geschlossenen Netzwerkes, können aber mit geeigneten Maßnahmen (z. B. VPN-Lösungen oder gesicherte Webanwendungen) Anbindung an das geschlossene interne Netzwerk erhalten. Beispiele dafür sind Medizingeräte mit Remotezugriff, Cloud-Services oder mobile Arbeitsplätze. Nicht übersehen werden sollte die Verwendung portabler Datenträger.

Medizinische Netzwerke können zahlreiche und verschiedenste Medizinprodukte enthalten. Dazu gehören u. a. medizinische Software-Produkte oder Medizintechnik (embedded oder PC-basiert) wie z. B. Überwachungsmonitore oder bildgebende Systeme.

Allen Bestandteilen ist gemeinsam, dass sie durch ihre Architektur potenzielle Einfallstore für z. B. Schadsoftware (= Malware) oder nicht autorisierte Zugriffe sind. Die Vernetzung ermöglicht zudem die Weiterverbreitung von Schäden sowie Folgeschäden im IT-System.
Besteht keine sichere Trennung des medizinischen Netzwerks von der übrigen IT-Infrastruktur oder zu externen Systemen, können unerwünschte Aktivitäten auch von dort erfolgen und damit das medizinische Netzwerk betreffen.

2 Mögliche Eintrittspforten

Malware 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 Schutz.
Ebenso kann jede einzelne Komponente in einem Netzwerk durch Verlust von Zugangsdaten, Kompromittierung oder Ausnutzung von Sicherheits-Schwachstellen den nicht autorisierten Zugang zu weiteren Komponenten eines Netzwerks ermöglichen.
Um diesen Gefahren zu begegnen, werden von Betreibern neben der Netzwerkabsicherung auch Maßnahmen an den Medizinprodukten vorgenommen.
Vom Medizinprodukthersteller nicht freigegebene Softwareupdates (z. B. für Virenschutz, Betriebssystem oder sonstige Anwendungssoftware) können die ins Netzwerk eingebundenen Medizinprodukte in ihrer Funktion beeinträchtigen und somit möglicherweise Personen gefährden.

3 Gesetzlicher Hintergrund

Grundsätzlich dürfen in Europa nur Produkte in Verkehr gebracht werden, wenn sie die Anforderungen der anwendbaren EU-Richtlinien erfüllen (z. B. MDR, R&TTED, RED, LVD, NIS2-D). Medizinprodukte dürfen in Europa entsprechend der MDR, 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 (ProdHaftG) und zum Schutz personenbezogener Daten (DSGVO).

4 Verpflichtungen für Hersteller

Hersteller von Medizinprodukten, die für ihre Medizinprodukte die Verwendung in IT-Netzwerken erwarten oder vorhersehen, müssen bereits während des Designs u. a. mögliche Risiken, die an den Schnittstellen denkbar sind, hinsichtlich ihres Gefährdungspotentials bewerten und

entsprechende Minimierungsmaßnahmen definieren und implementieren. Sollte dieses technisch nicht möglich sein, dann muss der Anwender bzw. der Patient hinreichend über diese Gefährdungen informiert werden, z. B. in der Gebrauchsanweisung. Der Hersteller gibt dem Betreiber vor, in welcher Systemumgebung das Medizinprodukt sicher betrieben werden kann.

5 Verpflichtungen für Betreiber

Betreiber dieser Medizinprodukte (IT-Netzwerkkomponenten und Software) sind verpflichtet, sich bereits im Rahmen der Installation und Inbetriebnahme über evtl. Gefährdungen aller Art aus der vom Hersteller zur Verfügung gestellten Dokumentation zu informieren. Daraus sind geeignete Maßnahmen in ihrer eigenen Organisation zu entwickeln, festzulegen und umzusetzen. Das umfasst sowohl technische als auch organisatorische Maßnahmen, z. B. die Festlegung und Implementierung von Richtlinien zur Nutzung der IT, über den gesamten Produktlebenszyklus.

6 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 MPDG zu werden.
Jede Infrastruktur ist anders und macht daher individuelle Lösungen erforderlich. Die zu ergreifenden Maßnahmen sind im Rahmen des festgestellten Schutzbedarfes einer Risikoanalyse geeignet zu adressieren. In jedem Fall ist die Vorgabe des Herstellers für die Integration der Medizinprodukte in ein IT-Netzwerk zu berücksichtigen.
Hilfestellung für eine risikobewusste Integration der Medizinprodukte in das IT-Netzwerk geben folgende Normen:

- ISO/IEC 27001 (Information technology – Information security management systems)
- ISO/IEC 29100 (Information technology – Security framework)
- IEC 80001-1 (Application of risk management for IT-networks incorporating medical devices)

Dabei beschreibt die Norm IEC 80001-1, wie eine Risikoanalyse mit den daraus abgeleiteten Maßnahmen das Risiko für Gefährdungen in einem IT-Netzwerk minimieren kann bzw. wie Prozesse für den Ernstfall definiert werden.

Diese Maßnahmen können sowohl organisatorisch als auch technisch sein, z. B. die Anpassung der Netzwerkarchitektur und die Systemabsicherung. Beispiele für gängige Maßnahmen, die prinzipiell in jeder medizinischen IT-Umgebung umgesetzt werden sollten, finden sich im Folgenden:

• Regelmäßige Schulung der Mitarbeiter, um durch das Aufzeigen von Risiken die Wahrscheinlichkeit für Gefährdungen zu reduzieren. • Klare Strukturierung des Netzwerkes, um medizinische von nicht-medizinischen Netzwerk-Bereichen zu trennen. Die notwendigen Verbindungen sollten über wenige, aber gut abgesicherte Gateways erfolgen (siehe Kasten rechts). • Schutzsoftware (Virenscanner, Firewall etc.) auf nicht-medizinischen Systemen installieren, um deren Infektion und die nachfolgende Verbreitung im medizinischen Netzwerk zu verhindern. • Installation von Portblockern an den Schnittstellen zwischen einzelnen Systemen, z. B. USB, sodass nur zwingend benötigte Medien Zugang erhalten. Dieses gilt auch für Medizinprodukte.	Eine klare Strukturierung für den sicheren Betrieb von vernetzten Medizingeräten kann z. B. durch getrennte und abgesicherte medizinische Subnetze erreicht werden. Im Rahmen eines umfassenden Sicherheitskonzepts 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 ZVEI-Positionspapier „Sichere medizinische Netze“.

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 bzw. wieder in einem IT-Netzwerk betrieben werden darf. Der Betreiber ist angehalten, den Vorgaben der Hersteller zu folgen, da diese in der Regel bereits die Verifizierung und Validierung der freigegebenen Anpassung durchgeführt haben.

7 Fazit

IT-Systeme und ihre Vernetzung sind nicht mehr weg zu denken, weder im Alltag noch in der Gesundheitsversorgung. 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 erfordern.
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 oder inkompatibel zu anderen Regelungen werden. Diese Sicherheitskonzepte sollten transparent sein und unter Einbeziehung aller betroffenen Parteien bzw. Organisationen gemeinsam erarbeitet werden. Diese müssen regelmäßig überprüft und, wo notwendig, verbessert werden, um den jeweils aktuellen Anforderungen zu genügen.
Das erforderliche Sicherheitsniveau kann nur erreicht werden, wenn alle Beteiligten an einem Strang ziehen.

Kontakt
Andreas Bätzel • Senior Manager Medizintechnik und Gesundheitsmarkt • Bereich Gesundheit •
Tel.: +49 69 6302 388 • Mobil: +49 162 2664 929 • E-Mail: andreas.baetzel@zvei.org

ZVEI e. V. • Verband der Elektro- und Digitalindustrie • Lyoner Straße 9 • 60528 Frankfurt am Main
Lobbyregister-Nr.: R002101 • EU Transparenzregister ID: 94770746469-09 • www.zvei.org

Datum: 16.05.2023