zvei
electrifying ideas

Positionspapier

Sichere medizinische Netze

Verband der Elektro- und Digitalindustrie

1 Vernetzung von Medizinprodukten

Vernetzte Medizinprodukte nutzen das klinische IT-Netzwerk zur Kommunikation, etwa von Aufträgen, Nachrichten, Bildern und Berichten. Fehlbedienung, Missbrauch, Schadsoftware und Angriffe können nicht nur diese Kommunikation, sondern – je nach Gerät – auch die wesentlichen Funktionen des Medizinprodukts stören. Durch derartige Zwischenfälle („Incidents“) kann unter Umständen eine Gefährdung eintreten, selbst wenn der Hersteller des Medizinprodukts während der Entwicklung in seiner Analyse diesbezügliche Maßnahmen berücksichtigt hat.

Trotz sorgfältiger Umsetzung regulatorischer Vorgaben können Hersteller solche Maßnahmen lediglich in einzelnen zu vernetzenden Medizinprodukten realisieren. Die Wirksamkeit solcher technischen Maßnahmen hängt jedoch immer von der Systemumgebung sowie der sachgerechten Nutzung ab. Nur Betreiber haben Einfluss auf die Betriebsabläufe und die Einrichtung zusätzlicher technischer sowie organisatorischer Maßnahmen.

Dieses Positionspapier soll Medizintechnikern oder Klinik-IT- Experten in der Funktion eines Netzwerk-Administrators helfen, um Medizinprodukte sicher zu vernetzen. Es beschreibt technologie-neutral betreiberseitige Schutz-Maßnahmen im Sinne der IEC 80001-1.

Das Wort Informationssicherheit (für Information Security) soll als Risikomanagement gegen unerlaubte bzw. ungewünschte Szenarien im klinischen IT-Netzwerk verstanden werden.

Die hier vorgeschlagene Strukturierung der für den Schutz der Netze notwendigen technischen und organisatorischen Elemente orientiert sich am „Cybersecurity Framework“ des amerikanischen National Standards Institute (NIST):

- Identifikation der Gefährdungen
- Schutz der IT-Werte
- Erkennung von Schadszenarien
- Reaktion auf Zwischenfälle
- Wiederherstellung

Die Betreiber wählen je nach eigener Priorisierung und abhängig von der Art der erkannten Schadszenarien eigene Schwerpunkte zur Implementierung aus.

2 Sicherheit im Betrieb

Die grundsätzliche Verantwortung der Klinikleitung für den sicheren Betrieb des Netzes ist in der Norm IEC 80001-1:2010 beschrieben. Jedoch fehlt dort eine abgestimmte, praktikable Liste von Maßnahmen.

Die unten angegebenen Maßnahmen unterstützen die Sicherheit im Betrieb. Alle technischen Maßnahmen können nur im Kontext von Sicherheitsprozessen (etwa nach einem der Standards: ISO/IEC 27001 und -2, ISO 27799, IEC 62443, BSI IT-Grundschutz) seitens der Betreiber wirksam werden. Neben den unten beschriebenen Maßnahmen legt beispielsweise ein Sicherheitsprozess nach ISO 27799 (als Konkretisierung der ISO/IEC 27002 für klinische IT-Netze) u. a. diese übergreifenden strategischen, organisatorischen und technischen Elemente fest:

Strategie

- Unternehmenspolitik für Informationssicherheit
- Personalpolitik, Personalauswahl, Vertragsgestaltung, Personalführung

Organisation

- Organisation der Informationssicherheit
- Compliance
- Beschaffung von IT
- Lieferantenmanagement
- Kontrolle und Verbesserung, Auditierung des Sicherheitssystems

Technik

- Analyse des Schadensausmaßes von Schadszenarien
- Informationssicherheitsverfahren

- Werkzeuge und Software für Informationssicherheit
- Physische Zugangsbeschränkungen (Gebäude, Räume, Berechtigungskonzept)

Weiterhin wird ein „Incident“-Management bestimmt, in dem die Zuständigkeiten und Verfahren zur Abwehr und Behandlung von unerlaubten bzw. unerwünschten Schadszenarien festgelegt sind, beispielsweise
- zur Planung von Schadensabwehr,
- zur Reaktion bei Zwischenfällen,
- zum Wiederherstellen.

3 Betrieb sicherer medizinischer Netze

Es folgen konkrete, gemäß NIST strukturierte Beispiele für Maßnahmen:

IDENTIFIZIEREN: Erkennen von Schutzgütern in medizinischen Netzen

- Katalogisierung: Der Betreiber erstellt ein Verzeichnis der Schützgüter (Daten, Server, Arbeitsplätze, Dienste, Anwendungen) inklusive zusätzlicher Angaben wie etwa zugehöriger Organisation, die für das jeweilige medizinische Subnetz wichtig sind.
- Klassifizierung gemäß Kritikalität: Der Betreiber dokumentiert für jedes katalogisierte Schutzgut zusätzlich die Kritikalität (etwa nach Reaktionszeiten oder nach Gefährdungspotenzial).

Die gewählte Kritikalitätskala kann sich orientieren an den Attributen Vertraulichkeit, Verfügbarkeit, Kapazitätsbedarfe, Wertschöpfungsbeitrag, Betriebsabläufe, klinische Relevanz usw.

Die Klassifikation sollte durch Kennzeichnungsmaßnahmen an Geräten und Bedienoberflächen dargestellt werden.

- Zuständigkeiten: Der Betreiber dokumentiert
  - Zuständigkeiten und Verfahren für Einrichtung und Betrieb des jeweiligen medizinischen Netzes.
  - Verträge zur Geheimhaltung oder den vertrauensvollen Umgang mit Daten und Geräten.

Beispiel: Die Rolle „Medizintechnik-Experte“ hat die Aufgabe, das radiologische Subnetz zu administrieren. Dieses Subnetz ist bis auf definierte, geschützte Schnittstellen abgeschlossen.

SCHÜTZEN: Schutz vor unerlaubten oder unerwünschten Szenarien

Mit den folgenden Maßnahmen können Betreiber die Wahrscheinlichkeit eines Schadszenarios ("incident") verringern.

Organisatorische Schutzmaßnahmen:
- Anforderungen und Strategie für Zugriffsschutz
- Information und Ausbildung des Personals
- Festlegungen zur Aufstellung von Geräten, Speichern und Konsolen (inkl. mobile Nutzung)
- Regelungen zum Umgang mit Daten und Geräten
- Entsorgungsregelung für Datenträger und Geräte mit Datenspeichern
- Benutzerverwaltung (Login, rollenbasierte Berechtigungen)
- Simulation von Angriffen
- Regelungen zum Einbringen, Lagern, Weiterleiten und Vernichten von Wechseldatenträgern
- Dokumentation der Verfahren, sowie der Konfiguration von Anwendungen, Systemen und Netzen, Wartungsverfahren und Wartungsaufgaben

Technische Schutzmaßnahmen:
- Einrichtung abgesicherter medizinischer Subnetze
- Abtrennung medizinischer Subnetze durch Firewalls
- Physischer Schutz durch geschützte und separierte Verkabelung und Aufstellung der Geräte
- Löschprozeduren für Datenträger und Geräte mit Datenspeichern
- Technischer Zugriffsschutz für Anwender (Rolle mit eingeschränkten Berechtigungen)

- Technische Einschränkung oder Schutz von Schnittstellen (USB, WLAN, NFC, etc.)
- Technische Einschränkung der Installation und Nutzung unbekannter Schnittstellen, Geräte sowie Software-Funktionen und -Dienste sowie IT-Werkzeuge
- Virtualisierung besonders exponierter Anwendungen wie etwa E-mail und Internet-Browser in sicheren Umgebungen („container“, „sand-box“, „secure compartment“, „virtual client“)
- Einschränkung der Kommunikation auf bekannte (authentifizierte) Knoten und Anwendungen, z. B. durch Verschlüsselung von Daten und Nachrichten
- Zeitnahe Aktualisierung der Komponenten, z. B. Plattformen, Middleware und Anwendungen, durch freigegebene Sicherheits-Updates

ERKENNEN: Erkennen von unerlaubten oder unerwünschten Szenarien

Organisatorische Maßnahmen helfen Betreibern, die Erkennung unerwünschter Aktivitäten in sicheren Netzen zu verbessern. Dies können beispielsweise sein:

- Führen einer Liste von verdächtigen Anomalien, die auf ein Schadszenario hindeuten
- Lernprozess zur Aktualisierung der verdächtigen Anomalien

Mit technischen Maßnahmen können Betreiber unerwünschte Aktivitäten in Netzen erkennen:

- Monitoring-Funktionen zur Erkennung und Bewertung von Schadszenarien (z. B. mittels Firewall, intrusion detection)
- Protokollieren von Ereignissen, Admin-/Anwender-Logfiles, Schutz der Logdateien
- Technische Möglichkeit zur Aktualisierung der Liste (und Regeln) der verdächtigen Anomalien

REAGIEREN: Reaktion auf unerlaubte oder unerwünschte Szenarien

Betreiber können mit organisatorischen Maßnahmen die schädliche Auswirkung unerlaubter oder unerwünschter Aktivitäten in sicheren Netzen begrenzen:

- Planung und Etablierung von Analyseverfahren (wie schwerwiegend ist der Zwischenfall?)
- Planung und Etablierung von Reaktionsverfahren (Sammeln von Beweisen, Eindämmen, Isolieren, Benachrichtigen)
- Prozessverbesserung durch Lernen von Analyse und Reaktion

Technische Verfahren unterstützen die organisatorischen Maßnahmen:

- Einrichtung technischer Begrenzung und Abwehrverfahren (Stop-All-Funktion der Firewalls)
- Einrichtung technischer Benachrichtigungswege über unabhängige Kommunikationskanäle

WIEDERHERSTELLEN: Wiederherstellung nach unerlaubten oder unerwünschten Szenarien

Durch technische Maßnahmen können Betreiber den Schaden nach unerlaubter oder unerwünschter Aktivität im sicheren Netz kompensieren.

Organisatorische Wiederherstellungsmaßnahmen:

- Spezifikation und Etablierung von Sicherungs- und Wiederherstellungsverfahren
- Präventive Übung der Wiederherstellung („Disaster Recovery“)
- Verbesserungsprozess für o. g. Verfahren

Technische Wiederherstellungsmaßnahmen:

- Skripte/Dienste zur Sicherung der identifizierten Datenbestände. Dabei sollte auf Schadcodes und korrumpierte Daten geprüft werden
- Maßnahmen zum Schutz archivierter Bestände, etwa durch Entzug der Schreibrechte
- Skripte/Dienste zur Wiederherstellung der gesicherten Datenbestände, wobei identifizierte Schadcodes und korrumpierte Daten nicht zurückgespielt werden dürfen
- Redundante Plattformen für kritische Anwendungen (cold stand-by)

4 Fazit

Die oben geschilderte Einrichtung sicherer medizinischer Netze ermöglicht dem Betreiber eine Balance zwischen Informationssicherheit und Leistungsfähigkeit. Es ist Aufgabe des Betreibers, bei den obigen Maßnahmen die Funktion der vernetzten Medizingeräte weiterhin zu gewährleisten. Maßgeblich dabei ist die Gebrauchsanweisung des jeweiligen Herstellers.

Obwohl technische Security-Maßnahmen (etwa in vernetzten Medizingeräten) die Reaktionsgeschwindigkeit und den Datendurchsatz reduzieren können, sollten sie nicht von Betreibern umgangen oder abgeschaltet werden.

Die obige Aufzählung kann niemals vollständig sein. Es kann zukünftig unvorhersehbare Angriffe oder neue Arten von Angriffen geben, die mit den oben gelisteten Maßnahmen nicht abgewehrt werden können, sodass zusätzliche Maßnahmen notwendig werden können.

Die geschilderten Maßnahmen sind kein Ersatz für einen umfassenden IT- Sicherheitsprozess des Betreibers, etwa gemäß ISO/IEC 27002 oder ISO 27799.

5 Referenzen

BSI: IT-Grundschutz-Standard 100-2: IT-Grundschutz Methodologie – Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 2008

Canavan J. E.: Fundamentals of Network Security, Artech House Publishers, Boston, 2001

NIST: Framework for Improving Critical Infrastructure Cybersecurity, NIST, also available at https://www.nist.gov/cyberframework/framework.pdf, 2018

ISO/IEC 27002:2022: Information technology – Security techniques – Code of practice for information security management. Genf, ISO, 2022

ISO 27799:2016: Health informatics – Information security management in health using ISO/IEC 27002. Genf, ISO, 2016

IEC 62443-3-3:2013: Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels, Genf, IEC, 2013

IEC 80001-1:2021: Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities, Genf, IEC, 2021

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