Positionspapier

Sichere medizinische Subnetze

Januar 2017

Zentralverband Elektrotechnik- und Elektronikindustrie

Vernetzung von Medizingeräten

Vernetzte Medizingeräte 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 Medizingerätes stören. Durch derartige Zwischenfälle („incidents“) kann unter Umständen sogar die Sicherheit des Medizingeräts gestört werden, auch wenn dessen Hersteller in der Gefährdungsanalyse diesbezügliche Maßnahmen im Entwicklungsprozess umgesetzt hat.

Obwohl wirksame regulatorische Mittel den Herstellern vernetzter Medizingeräte entsprechende Pflichten im Rahmen der Gefährdungsanalyse auferlegen, können Hersteller lediglich technische Maßnahmen in einzelnen zu vernetzenden Komponenten realisieren. Die Wirksamkeit solcher technischen Maßnahmen hängt dabei jedoch immer von der geeigneten Umgebung sowie der sachgerechten Nutzung – also von Personen und Prozessen – ab, worauf eben nur die Betreiber Einfluss haben.

Dieses Papier beschreibt die Maßnahmen, die ein Medizintechniker oder Klinik-IT-Experte in der Funktion eines Netzwerk-Administrators umsetzen kann, um Medizingeräte sicher zu vernetzen. Die vorliegende Spezifikation beschreibt dazu betreiberseitige Schutz-Maßnahmen im Sinne der IEC 80001. Sie bleibt dabei unabhängig von Plattformen und Herstellern und versucht weitgehend technologie-neutral zu sein.

Das im deutschen etwas ungenaue Wort Informationssicherheit (für Information Security) legen wir hierbei als Risikomanagement gegen unerlaubte bzw. ungewünschte Szenarien im klinischen IT-Netzwerk fest.

Die Struktur dieser Spezifikation orientiert sich am „Cybersecurity Framework“ des amerikanischen National Standards Institute (NIST), in dem die notwendigen technischen und prozessualen Elemente anhand der Zielsetzungen in die folgenden Schritte aufgeteilt sind.

- Identifikation der Gefährdungen
- Schutz der IT-Werte
- Erkennung von Schadszenarien
- Reaktion und Wiederherstellung nach Schadszenarien

Die Anwender wählen sich aus diesen Schritten je nach eigener Priorisierung und abhängig von der Art der erkannten Schadszenarien eigene Schwerpunkte zur Implementierung aus. Im einfachsten Fall ist diese Spezifikation als Checkliste verwendbar.

Sicherheitsprozess

Die grundsätzliche Verantwortung der Klinikleitung für den sicheren Betrieb des Netzes ist in der Norm IEC 80001-1:2010 geklärt. Ebenso legt der Hersteller des vernetzten Medizingerätes die Betreiberverantwortung für die Einwirkung des Netzwerks auf den sicheren Betrieb des Geräts nach IEC 60601-1, Klausel 14.13. fest. Jedoch ist eine abgestimmte, praktikable Liste von Maßnahmen zum Schutz des Medizingerätes in keiner dieser Normen beschrieben.

Die unten angegebenen Abwehrmaßnahmen können nicht den grundlegenden Sicherheitsprozess seitens der Betreiberorganisation ersetzen. Alle technischen Maßnahmen können nur im Kontext einer sicheren und verantwortlichen Benutzung der Geräte im Rahmen eines Sicherheitsprozess (etwa nach einem der Standards: ISO/IEC 27002, ISO 27799, IEC 62443, BSI IT-Grundschutz) seitens der Betreiber wirksam werden. Neben den unten beschriebenen Abwehrmaßnahmen legt beispielsweise ein Sicherheitsprozess nach ISO 27799 –

als Übersetzung der ISO/IEC 27002 für klinische IT-Netz – diese übergreifenden Elemente fest.

- Unternehmenspolitik für Informationssicherheit
- Analyse des Schadensausmaßes von Schadszenarien
- Organisation der Informationssicherheit
- Informationssicherheitsverfahren
- Werkzeuge und Software für Informationssicherheit
- Beschaffung von IT
- Personalpolitik, Personalauswahl, Vertragsgestaltung, Personalführung
- Lieferantenmanagement
- Physische Zugangsbeschränkungen (Gebäude, Räume, Berechtigungs-konzept)
- Compliance
- Kontrolle und Verbesserung, Auditierung des Sicherheitssystems

Weiterhin wird ein „Incident"-Management bestimmt, in dem die Zuständigkeiten und Verfahren zur Abwehr und Behandlung von unerlaubten bzw. unerwünschten, schädlichen Szenarien („incident") festgelegt sind.

- Zuständigkeiten & Verfahren zur Planung von Schadensabwehr
- Zuständigkeiten & Verfahren zur Reaktion bei Zwischenfällen
- Zuständigkeiten & Verfahren zum Wiederaufsetzen

Betrieb von sicheren medizinischen Subnetzen

Primäre Zielgruppe dieser Spezifikation sind Medizintechniker sowie klinische IT-Administratoren, die vernetzte Medizingeräte in einem sicheren medizinischen Subnetz betreiben möchten. Je nach Organisation ist es sinnvoll, ein oder mehrere, abgesicherte medizinische Subnetze einzurichten.

1. IDENTIFIZIEREN: Erkennen und Klassifizieren von IT-Schutzgütern

IT-Inventar: Der Betreiber erstellt ein Verzeichnis der IT-Assets (Daten, Server, Arbeitsplätze, Dienste, Anwendungen) die für das jeweilige medizinische Subnetz wichtig sind. Zur Klassifikation gehört auch die genaue Angabe von zugehöriger Organisation und Hinweise auf betriebliche Zuständigkeiten.

Beispiel für ein radiologisches Subnetz: Bildgebende Modalität, RIS-Server, evtl. KIS-Schnittstelle (ADT, ORU), RIS-Workstations.

Klassifikation gemäß Kritikalität: Der Betreiber dokumentiert Geräte und relevante IT-Anwendungen des jeweiligen medizinischen Subnetzes und klassifiziert sie anhand ihrer Kritikalität (etwa nach Reaktionszeiten oder nach Gefährdungspotenzial).

Beispiel: In einer dreistufigen Kritikalitätsskala (geplant/kritisch/real-time) wird die Radiologie als „zeitkritisch" bewertet, denn sie unterstützt auch die Notfall-Versorgung. Deswegen arbeiten alle Anwendungen und Geräte zeitkritisch (mittlere Stufe), lediglich die Modalität hat Gefährdungspotenzial.

Die Klassifikation ist durch Kennzeichnungsmaßnahmen an Geräten, Bedienoberflächen und technischen Bezeichnern dargestellt.

Zuständigkeiten: Der Betreiber dokumentiert

a) Zuständigkeiten und Verfahren für Einrichtung und Betrieb des jeweiligen medizinischen Subnetzes.
b) Verträge zur Geheimhaltung oder den vertrauensvollen Umgang mit Daten und Geräten.

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

2. SCHÜTZEN: Einschränkung des Zugriffs auf die relevanten Schutzgüter

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

- Abtrennung medizinischer Subnetze durch Firewalls
- Physischer Schutz der geschützte und separierte Verkabelung und Aufstellung der Geräte
- Löschprozeduren für Datenträger und Geräte mit Datenspeichern
- Technischer Zugriffsschutz für Accounts („Login“ mit eingeschränkten Berechtigungen)
- Technische Einschränkung der Installation und Nutzung unbekannter Schnittstellen, Geräte und Software-Funktionen sowie IT-Werkzeuge
- Virtualisierung besonders exponierter Anwendungen wie etwa Email und Internet-Browser in sicheren Umgebungen („container“, „sand-box“, „secure compartment“, „virtual client“)
- Technische Einschränkung oder Schutz von Schnittstellen (USB, WLAN, NFC, Filesharing etc.)
- Verschlüsselung von Daten und Nachrichten
- Einschränkung der Kommunikation auf bekannte (authentifizierte) Knoten und Anwendungen
- Systematische Aktualisierung der Sicherheits-Updates für Plattformen, Middleware und Anwendungen

3. ERKENNEN und Bewerten von unerlaubten oder unerwünschten Aktivitäten

Organisatorische Maßnahmen helfen Betreibern, die Erkennung unbeabsichtigter Aktivitäten in sicheren Subnetzen zu verbessern.

- Lernprozess zur Aktualisierung der verdächtigen Anomalien
- Pflege einer Liste von verdächtigen Anomalien, die ein Schadszenario anzeigen

Mit technischen Maßnahmen können Betreiber unbeabsichtigte Aktivitäten in Subnetzen erkennen:

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

4. REAGIEREN: Reaktion auf unerlaubte oder unerwünschte Szenarien

Betreiber können mit organisatorischen Maßnahmen die schädliche Auswirkung unerlaubter oder unbeabsichtigter Aktivitäten in sicheren Subnetzen begrenzen:

- Dokumentation von Analyseverfahren (wie schwerwiegend ist der Zwischenfall?)
- Dokumentation von Reaktionsverfahren (Sammeln von Beweisen, wie wird reagiert?)
- 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

5. WIEDERHERSTELLEN: Einrichten von Prozeduren zur Wiederherstellung von Daten und Funktionen des sicheren medizinischen Subnetzes nach einem Angriff

Durch technische Maßnahmen können Betreiber den Schaden nach unerlaubter oder unbeabsichtigter Aktivität im sicheren Subnetz kompensieren.

Organisatorische Wiederherstellungsmaßnahmen:

- Dokumentation von Sicherungs- und Wiederherstellungsverfahren
- Verbesserungsprozess für o. g. Verfahren
- Präventive Übung für schwerwiegende Ausfälle („Disaster Recovery“).

Technische Wiederherstellungsmaßnahmen:

- Skripte/Dienste zur Sicherung der identifizierten Datenbestände. Dabei sollten Schadcodes und korrumpierte Daten systematisch ausgelassen werden
- Maßnahmen zum Schutz archivierter Bestände, etwa durch Entzug der Schreibrechte
- Skripte/Dienste zur Wiederherstellung der gesicherten Datenbestände. Dabei sollten systematisch Schadcodes und korrumpierte Daten nicht aus dem Backup geholt werden
- Redundante Plattformen für kritische Anwendungen

Hinweise

Es ist Aufgabe des Betreibers, bei den obigen Maßnahmen die Funktion der vernetzten Medizingeräte weiterhin zu unterstützen. Maßgeblich dabei ist die Gebrauchsanweisung des jeweiligen Herstellers.

Obwohl technische Security-Maßnahmen (etwa in vernetzten Medizingeräten) die Reaktionsgeschwindigkeit und den Durchsatz 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.

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 http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, 2014

ISO/IEC 27002:2013: Information technology – Security techniques – Code of practice for information security management. Genf, ISO, 2013

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 80001-1:2010: Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities, Genf, IEC, 2010

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

2. Auflage Januar 2017

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