9 IT-Sicherheit bei Medizinprodukten

9.1 Einführung

9.1.1 Probleme mit der IT-Sicherheit

Die täglichen Meldungen über Probleme mit der IT-Sicherheit machen klar, wie bedroht auch vernetzte Medizinprodukte sind. So informiert die FDA über Infusionspumpen mit offenen SSL-Ports und über angreifbare Herzschrittmacher.

Doch es sind nicht nur diese plakativen Beispiele, die Sorgen bereiten. Auch die täglichen Nachlässigkeiten im Alltag gefährden die IT-Sicherheit:

- Eine Röntgenuntersuchung muss wiederholt werden, weil das Speichersystem wegen eines Hardwaredefekts nicht verfügbar ist.
- Pflegekräfte können nicht auf Patientendaten zugreifen, weil das Krankenhausinformationssystem neu gebootet werden muss.
- Ärzte verschicken dermatologische Bilder per WhatsApp, um diese gemeinsam zu befunden.
- Die Entwickler testen die Software mit einer Kopie der Produktionsdatenbank und erhalten dadurch Zugriff auf Patientendaten.
- Eine Datenbank lässt sich nach einem Hardwaredefekt nicht mehr aus dem Backup herstellen.

9.1.2 IT-Sicherheit: Begriffsdefinition und Ziele

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert die IT-Sicherheit als *»Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind«*.

Diese Definition offenbart die Ziele der IT-Sicherheit:

- Vertraulichkeit (Confidentiality)
- Integrität (Integrity)
- Verfügbarkeit (Availability)

Das Akronym CIA hilft, sich diese drei Ziele zu merken.

Im Kontext der IT-Sicherheit werden regelmäßig weitere (Schutz-)Ziele genannt:

- Autorisierung (Authorization)
- Authentifizierung bzw. Authentisierung (Authentication)
- Zurechenbarkeit (Accountability)
- Nicht-Abstreitbarkeit (Non-Repudiation)

Diese Ziele unterstützen jedoch vor allem die zuerst genannten Ziele:

- Vertraulichkeit,
- Integrität und
- Verfügbarkeit.

Abgrenzung IT Security und Safety

Die IT-Sicherheit (IT Security) hat jedoch nicht die Patientensicherheit (Safety) als direktes Schutzziel. Die Ziele Security und Safety können sogar im Konflikt miteinander stehen. Beispielsweise würde man durch das Entziehen von Zugriffsrechten die Vertraulichkeit und damit IT Security verbessern. Die Safety könnte aber darunter leiden, weil zum Behandeln notwendige Informationen nicht oder nicht schnell genug verfügbar sind.

Abgrenzung IT Security und Datenschutz

Der Datenschutz hat zum Ziel, die »Verletzung des Schutzes personenbezogener Daten« zu vermeiden. Darunter versteht man gemäß DSGVO:

> *»eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;«*

Beim Datenschutz geht es somit um personenbezogene Daten. Die IT-Sicherheit hat allerdings die Integrität und Verfügbarkeit **aller** Daten im Fokus. Dazu zählen genauso Softwareprogramme, Konfigurationsdaten und Logdateien.

9.1.3 Das STRIDE-Modell

Die Angriffe, die zur Kompromittierung der IT-Sicherheit führen, lassen sich in sechs Klassen unterteilen:

Angriffstyp	Erläuterung	Angegriffenes Schutzziel
Spoofing	Der Angreifer täuscht falsche Identität vor.	Authentifizierung bzw. Authentisierung
Tampering	Der Angreifer verändert Daten z. B. Zugangsdaten, Patientendaten.	Integrität
Repudiation	Der Angreifer bestreitet den Angriff.	Nicht-Abstreitbarkeit
Information disclosure	Der Angreifer gelangt an vertrauliche Daten.	Vertraulichkeit
Denial of service	Der Angreifer versucht, die Ressourcen (z. B. CPU, Bandbreite) aufzubrauchen, um die Verfügbarkeit der Dienste zu unterbinden.	Verfügbarkeit
Elevation of privilege	Der Angreifer erhöht selbst seine Rechte im System z. B. von einem normalen Anwender zum Administrator mit »Root-Rechten«.	Autorisierung

Tab. 9–1 *Klassen des STRIDE-Modells*

Das Akronym STRIDE bildet sich aus den Anfangsbuchstaben der Angriffstypen.

Hersteller sollten dieses Modell zur systematischen Untersuchung aller Angriffstypen nutzen, um entsprechende Gegenmaßnahmen zu ergreifen und so die IT-Sicherheit zu gewährleisten.

9.2 Regulatorische Rahmen

9.2.1 MDR und IVDR

Die MDR und IVDR stellen im Gegensatz zur MDD und IVDD explizite Forderungen an die IT-Sicherheit.

In Anhang I mit den »grundlegenden Sicherheits- und Leistungsanforderungen« haben die MDR und IVDR im folgenden Satz die Worte »einschließlich der Informationssicherheit« ergänzt:

> *»Bei Produkten, zu deren Bestandteilen Software gehört, oder bei Produkten in Form einer Software wird die Software entsprechend dem Stand der Technik entwickelt und hergestellt, wobei die Grundsätze des Software-Lebenszyklus, des Risikomanagements einschließlich der Informationssicherheit, der Verifizierung und der Validierung zu berücksichtigen sind.«* (Quelle: MDR Anhang I, Abschnitt 17.2)