Medical Device Regulation, In-vitro-Diagnostic Regulation

Die 10 häufigsten Sicherheitslücken in Medical Devices

Security Testing Medizinprodukte (Software und Hardware)[1]

Die europäische Medical Device Regulation (EU) 2017/745 (MDR) und die In-vitro-Diagnostic Regulation (EU) 2017/746 (IvDR) regeln die Überprüfung unter Sicherheitsaspekten von Software, Firmware, Microcode und mobilen Apps zur Steuerung medizinischer Geräte (hier generell als Software bezeichnet) wie z.B. Herzschrittmacher, Röntgengeräte, Tomografen, Ultraschallgeräte und auch Patientenverwaltungssoftware sowie Netze etc. Die Verordnungen sollen derzeit bis Mai 2020 (Medizinprodukte) und bis Mai 2022 (In-vitro Diagnostika) schrittweise in Kraft treten. Diese Regularien entsprechen Regelungen im internationalen Bereich (USA, Kanada, China, Japan etc.), so dass die sicherheitsrelevanten IT-Anforderungen und die Anforderungen an technische Datenschutzmaßnahmen z.B. MDCG 2019-16 und dem „Leitfaden zur Nutzung des MDS2 aus 2019: Sicherheit von Medizinprodukten“ der Allianz für Cyber-Sicherheit weltweit vergleichbar sind.

Medizinische Geräte und Systeme in Praxen und Krankenhäusern werden weit überwiegend vernetzt und sind – mehr oder weniger direkt – ans Internet angeschlossen, so dass IT-Sicherheitsmaßnahmen zum Schutz vor unberechtigter Einsichtnahme und Änderung von (Patienten-)daten zwingend erforderlich sind. Gleichermaßen muss sichergestellt werden, dass die die Geräte steuernde Software nicht verändert wird - beginnend bereits beim Bootprozess.

Erreicht werden sollen also insbesondere die (für Informatiker bekannten) Sachziele Vertraulichkeit, Integrität und Verfügbarkeit der Daten und Systeme. Stand der Technik (ISO 27034) ist ein Security Testing Process, der die Software entwicklungsbegleitend auf sicherheitsrelevante Fehler – Sicherheitslücken – überprüft. Ein solcher Prozess enthält die folgenden 6 Methoden:

- Security Requirements-Analysis - Riskanalysis
- Threat Modeling zur Analyse der Sicherheitsarchitektur
- Static Source Code Analyse – Code Reading des Quellcodes
- Penetration Testing des ausführbaren Codes
- Dynamic Analysis – Fuzzing des ausführbaren Codes
- Conformity Testing zur Identifizierung von Backdoors und Covert Channels

Jede Methode ist notwendig, weil sie die Identifizierung andersartiger Sicherheitslücken unterstützt.

Auf der Grundlage der Erfahrungen mit Security Tests seit 2016 lassen sich im Folgenden die 10 häufigsten und schwerwiegendsten Sicherheitslücken und Herausforderungen in Medizinprodukten nennen:

- **Datenschutz**. Unzureichend geschützte Patientendaten: Die sensiblen Daten müssen mit geeigneten technischen Maßnahmen vor unberechtigtem Zugriff und Manipulation geschützt werden. Mittels Verschlüsselung sind die Daten auch bei Datenübertragung und vor physischem Zugriff zu schützen.
- **Authentifizierung**. Unzureichende Authentifizierung vor dem Gerätezugriff: Um sicherzustellen das nur berechtigte Personen auf das medizinische Gerät (und die Daten) zugreifen, hat vor jeder Interaktion mit der Software oder dem Gerät eine Authentifizierung zu erfolgen.
- Generische/schwache **Standardkonfigurationen**: Die Wahl von Standardpasswörter für Geräte oder Applikationen muss auf starke, gerätespezifische Kennwörter setzen. Gleiche Passwörter für Geräte, die vielfach verkauft werden, senken massiv das Sicherheitsniveau.
- **Veraltete Softwareversionen**. Das Gesamtsystem muss betrachtet werden. Neben selbst entwickelten Anwendungen müssen die jüngsten Updates auch an das Betriebssystem sowie verwendete Libraries und Software von Drittanbietern ausgerollt werden.
- **Updateprozess**. Fehlende oder unzureichende Signaturprüfung: Um Authentizität und Integrität einer Softwareaktualisierung zu gewährleisten und onberechtigte Änderungen zu verhindern, muss eine Signaturprüfung vor Ausführung des Updates erfolgen.
- **Best Practices**. Zur Verschlüsselung, Passwortspeicherung etc. sollte auf Best Practice Methoden zurückgegriffen werden, anstatt eigene Lösungen zu entwickeln.
- **Zu enger Fokus**. Die von Drittanbietern bezogenen Funktionen müssen ebenfalls Sicherheits-überprüft werden. Beispielsweise gilt dies auch für HL7/DICOM Protokoll-Implementierungen, die typischerweise in Form von Third Party Libraries eingebunden werden.
- **Secure Coding Standards**. Beispielsweise sind bei der Programmierung in C/C++ entsprechende Best Practices umzusetzen. So sollten u.a. „Banned Functions“ nicht verwendet werden, da diese anfällig für Angriffe wie Buffer Overflows sind.
- **Never Trust User Input**. Unabhängig davon, ob Daten über das Netzwerk via HL7/DICOM oder lokal zur Verfügung gestellt werden, müssen Nutzerdaten vor der Verarbeitung validiert werden.

[1] Lars Ubbenhorst und Prof. Dr. Hartmut Pohl, softScheck GmbH

- **Least Privilege**. Anwendungen dürfen nur die Berechtigungen erhalten, die für den Betrieb des Systems unverzichtbar sind. Im Fall eines erfolgreichen Angriffs kann so das Schadensausmaß begrenzt werden.

In allen Fällen hat der jeweilige Hersteller – ausweislich einer Wiederholungsprüfung – die identifizierten Sicherheitslücken behoben, so dass die Software, Firmware, App oder der Microcode etc. nach dem Stand der Technik als sicher bezeichnet werden kann und damit die Anforderungen der Medical Device Regulation bzw. der In-vitro-Diagnostic Regulation erfüllt.