Sichere Software für Medizinprodukte[1, 2]

EU-Anforderungen an medizinische Geräte und Software der
Medical Device Regulation (MDR) und der **In-vitro-Diagnostika Regulation (IVDR)**

Bereits im Mai 2017 traten die vom EU-Parlament beschlossenen - für alle EU-Staaten unmittelbar wirksamen - Verordnungen für Medizinprodukte in Kraft. Hierbei handelt es sich um die **Medical Device Regulation** (MDR) und die **In-Vitro-Diagnostika Device Regulation** (IVDR)[3]. Diese beiden Verordnungen lösen die bisherigen Medizinprodukte-Richtlinien MDD, AIMD und IVD ab. In beiden Verordnungen wird auch das Thema der Software-Sicherheit und generell der IT-Sicherheit adressiert, um ein höheres Sicherheitsniveau für Patienten zu erreichen:

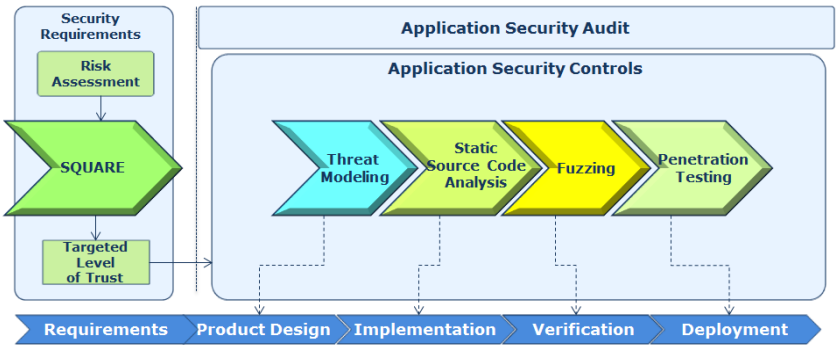
Ein IT-Angriff (Virus, direkter Angriff) auf lebenserhaltende Geräte und Systeme z.B. im Krankenhaus, Labor, Praxis kann Geräte direkt stören, Mess-Ergebnisse verfälschen und auch völlig abschalten! Fällt ein medizinisches Gerät aus, können Patienten vielleicht ja noch aufgenommen aber oft gar nicht mehr behandelt werden. Mit Ransomware werden Daten der Geräte (z.B. Patientendaten) so manipuliert (z.B. verschlüsselt), dass die Geräte nicht mehr korrekt arbeiten mit der Folge, dass Patienten falsch behandelt werden.

Darüber hinaus können Patientendaten kopiert, manipuliert oder gelöscht werden. Mit stark zunehmender Häufigkeit auch, um zu erpressen. Dazu gehören Labordaten die nicht anonymisiert, sondern nur pseudonymisiert sind, und daher den betroffenen Patienten ja durchaus zugeordnet werden können.

Einschlägig ist hier außerdem die **EU-Datenschutz-Grundverordnung (EU-DSGVO)**[4] mit ihrer Meldepflicht von Angriffen und Vorfällen. Abgesehen von strafrechtlicher Verfolgung können Bußgelder festgesetzt werden in Höhe von bis zu 20 Mio. Euro bzw. bis zu 4% des gesamten weltweit erzielten Konzern-Jahresumsatzes.

Für die Software- und Geräte-Entwicklung fordert die MDR ausdrücklich, IT-Sicherheit auf dem „Stand der Technik“. Dies erfordert Maßnahmen wie die Anwendung und Einhaltung des Grundschutzes des Bundesamts für Informationssicherheit (BSI) mit technischen Richtlinien und internationalen Normen wie die ISO 15408, IEC 62443, ISO 27034 oder auch die UL 2900-2-1.

So fordert die ISO 25010 Qualitätseigenschaften für Software-Security wie Vertraulichkeit, Integrität und Authentizität. Um dies zu erreichen sind Security Tests unverzichtbar, um potentielle Angriffspunkte (Sicherheitslücken) zu identifizieren. Angriffe sind dann erfolglos, wenn die Angriffspunkte identifiziert, behoben, korrigiert und gepatcht sind. Dazu existiert die ISO 27034 Application Security. Diese Norm entspricht dem Stand der Technik und erhöht die Sicherheitsqualität der Software. Sie beinhaltet mehrere Methoden zur Identifizierung von Sicherheitslücken.



softScheck Security Testing Process (SSTP) gem. ISO 27034

---

[1] Sascha Böhm, Security Consultant, softScheck GmbH

[2] Prof. Dr. Hartmut Pohl, geschäftsführender Gesellschafter softScheck GmbH

[3] https://ec.europa.eu/growth/sectors/medical-devices/regulatory-framework_de

[4] https://www.datenschutz-grundverordnung.eu

Sankt Augustin 2. Mai 2018

Dabei werden diese 6 Methoden zur Identifizierung der Sicherheitslücken eingesetzt:

- SQUARE: Security QUALity Requirements Engineering – Risk Analysis
- Threat Modeling: Untersuchung des Security Designs auf Sicherheitslücken
- Static Source Code Analysis zur Quellcodeprüfung auf Sicherheitslücken – Code Reading
- Penetration Testing: Identifizierung bekannter Sicherheitslücken
- Dynamic Analysis – Fuzzing: Identifizierung von Sicherheitslücken durch Eingabe erfahrungsgemäß erfolgreicher Angriffsdaten
- Conformance Testing: Prüfung auf Übereinstimmung von Design und Implementierung sowie von Implementierung und ausführbarem Code

Jede dieser Methoden wird in jeweils einer bestimmten Entwicklungsphase (von Requirements bis zum ausführbaren Code) eingesetzt, sodass bereits während der Entwicklung kritische Sicherheitslücken behoben werden.

softScheck arbeitet im Kontext aktiver Medizinprodukte mit dem **Johner Institut** zusammen. Das Johner Institut unterstützt Medizinproduktehersteller dabei, die regulatorischen Anforderungen z.B. der MDR, der IVDR oder der FDA zu erfüllen und so sicherere Produkte schnell und gesetzeskonform in den Markt bringen zu können.

Sie erreichen mit dem „Security Testing Process“ (SSTP) also 4 Ziele:

- **Hohes IT-Sicherheitsniveau** der Entwicklungen in Software, Firmware, Microcode, Apps, Systems und Hardware: Angreifbare Sicherheitslücken werden von softScheck identifiziert.
- **Produkt-Lebensdauer** - **Zukunftssicherheit**: Software, Firmware, Microcode, Apps, Systems und Hardware entsprechen den nationalen und den europäischen Gesetzen und Verordnungen sowie den US Regelungen der FDA.
- **Kostengünstige Software-Entwicklung**: Sicherheitsrelevante Fehler werden bereits während der Entwicklung identifiziert und müssen nicht erst Kosten-aufwändig nach Auslieferung an den Kunden korrigiert und gepatcht und ggf. im Feld ausgetauscht werden.
- **Verkürzung** der **Time-to-Market** durch parallel zur Entwicklung durchgeführte Security Tests.

softScheck
we identify vulnerabilities others don't

Prof. Dr. Hartmut Pohl
Geschäftsführender Gesellschafter
softScheck GmbH Köln www.softScheck.com
Büro: Bonner Str. 108. 53757 Sankt Augustin

Tel.: +49 (2241) 255 43 - 0
Mobil: +49 (172) 9437 – 329
Fax: +49 (2241) 255 4 – 329
Hartmut.Pohl@softScheck.com