



SECURE FIRMWARE OVER-THE-AIR-UPDATE FÜR STERILISATOREN UND REINIGUNGSGERÄTE

Belimed AG ist ein führender Anbieter für Produkt- und Servicelösungen zur Sterilisation, Desinfektion und Reinigung von medizinischen und chirurgischen Instrumenten. Mit einer Cloud-Plattform können Kunden ihren Maschinenpark fernüberwachen. Belimed beauftragte konplan, eine Machbarkeitsstudie für ein neues Feature «Secure Firmware Over-the-air (FOTA)-Update» für das bestehende System auszuarbeiten. Ziel ist, dass Software-Updates systematischer, schneller und sicher ausgerollt werden können.

Secure Architecture mit Einbezug unterschiedlicher Blickwinkel

Bei der Ausarbeitung der FOTA-Studie nahm konplan mehrere Blickwinkel ein: die User-bezogene Sicht enthielt die Ausarbeitung des FOTA-Workflows unter Einbezug der Stakeholder. Die Technologie-bezogene Sicht bestand aus der Risikoanalyse mit Fokus auf End-to-End IT-Security und Security Technologien. Basierend auf dem Workflow erarbeitete konplan Security Anforderungen, den Architekturansatz inklusiv Datenflussdiagramm und integrierte die verwendeten Assets in ein Defense-in-Depth Konzept. Über das Threat Modeling wurden die Risiken in Bezug auf die CIA-Triade identifiziert und entsprechende Mitigationen erarbeitet. Das Modeling kombinierte die Ergebnisse aus unterschiedlichen Ansätzen: aus dem klassischen bottom-up STRIDE Modeling, aus den OWASP Top Ten Security Risiken und aus den «Common Weakness Enumerations» (CWE). Die identifizierten IT-Security Risiko-Mitigationen wurden im Anschluss mit Vorgaben aus der IEC 62443 (Cybersecurity for industrial automation and control systems) abgeglichen und die gesamte Systemarchitektur entsprechend aktualisiert.

Detaillierte Grundlage für die sichere Implementation

Mit der Studie erhielt Belimed eine umfassende Sicht zur Architektur- und Implementation des sicheren Firmware Over-the-air-Update Features in das aktuelle System. Dazu gehören: Workflow und Security-Anforderungen an das System, Secure Architecture mit Defense-in-Depth IT-Sicherheit, «Rezeptbuch» für die Umsetzung sowie ein Entwurf einer Dokumentenliste für Zulassungsbehörden.

Resultat

- Umfassende Sicht zum sicheren Firmware-Update & Compliance
- Secure Architecture

Methodik & Technologien

- Workflow modeling
- STRIDE
- OWASP Top Ten Risks
- Security Risk Analysis

Leistungsumfang

- Nachweis Machbarkeit
- Secure Architecture
- «Rezeptbuch» für die Umsetzung



6 Monate



2 Mitarbeitende – konplan



Analyse & Ideenfindung
Konzeption

Kunde

Belimed  Miele Group Member

