CyOne SECURITY

12. August 2020

Mit der Vernetzung steigt die Verletzlichkeit

Lukas Christen | Senior Security Consultant
Public

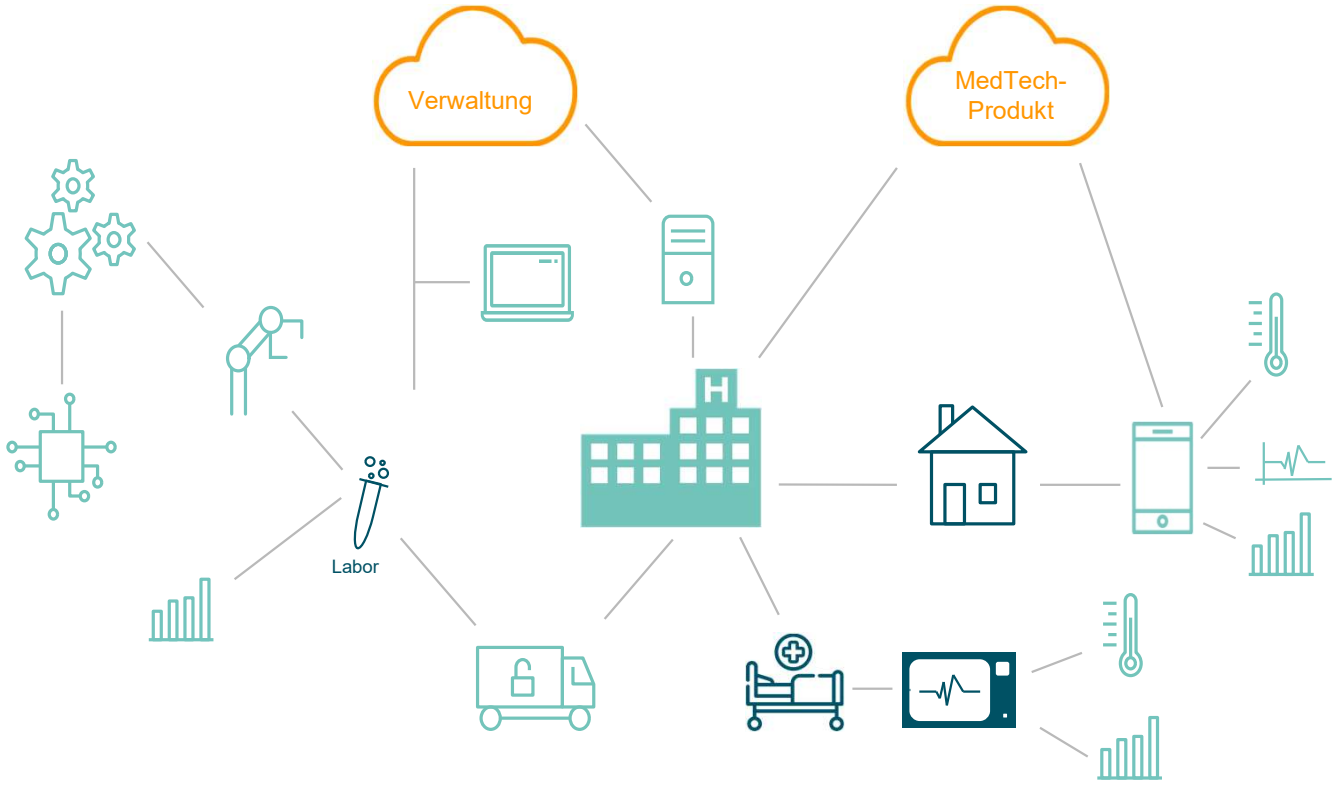
«If your product is successful,
it will be hacked»

Mike Muller, CTO ARM (2015)

«You Can’t Trust Big Data Unless You Can Trust the Little Data»

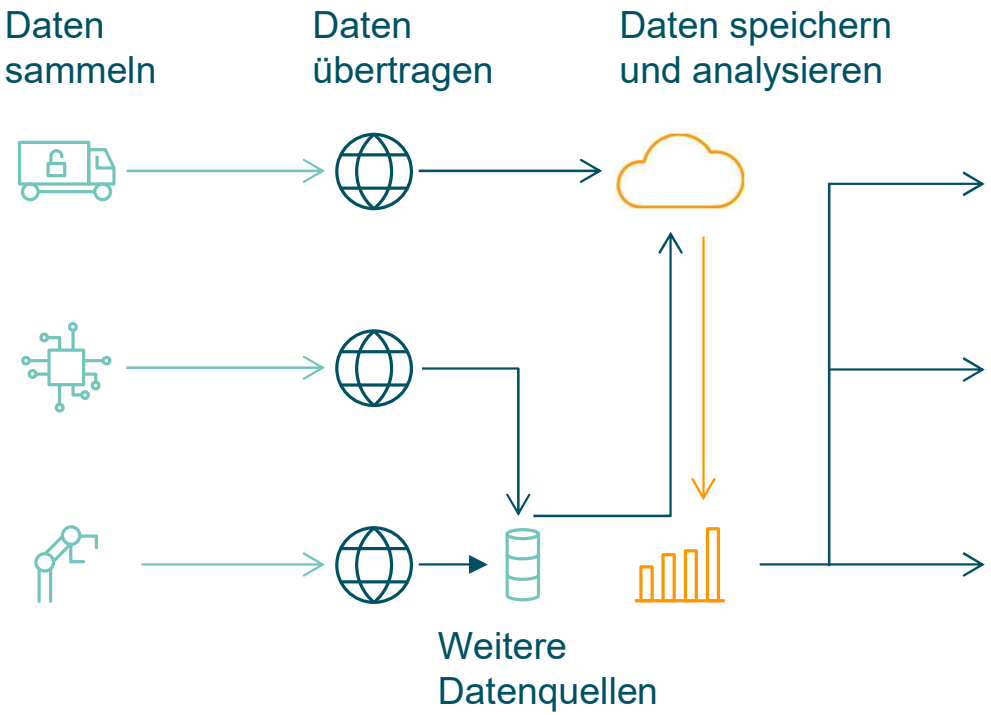
Mike Muller, CTO ARM (2015)

IoT – der Wirtschafts-Booster für Smart Healthcare



Bis **2023** sind weltweit **26,1 Milliarden Geräte vernetzt,** steigend bis auf **50 Milliarden.**

Welchen Mehrwert schafft IoT für die MedTech?



Verbessertes Kundenerlebnis

Schaffung von Wettbewerbsvorteil und Differenzierung

Effizientere Prozesse

Steigerung der Effizienz und Kosteneinsparung

Neue Geschäftsmodelle

Steigerung Unternehmenswachstum und Kundenbindung

Cybersecurity für Medizinprodukte – Einflussfaktoren

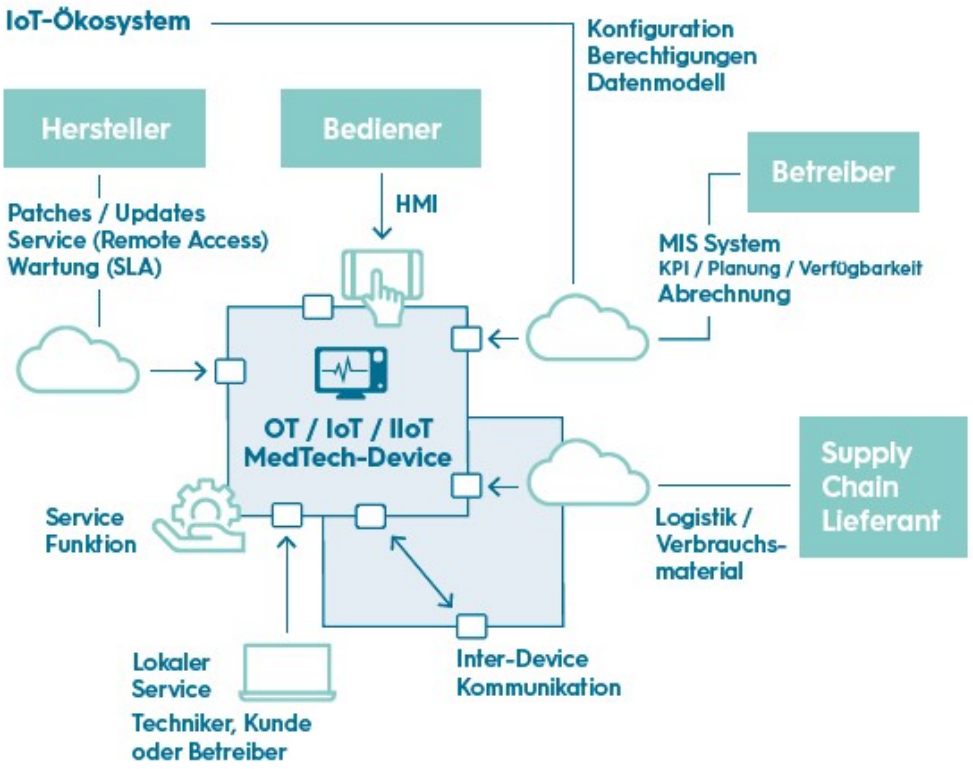
Jahr für Jahr werden **mehr Sicherheitslücken** in Standardsoftware-Komponenten wie Windows oder Oracle entdeckt.

Angriffe auf Netzwerke im Gesundheitswesen nehmen zu, d. h. für unsere Kunden besteht ein erheblich gestiegenes Risiko, Opfer von Datenpannen zu werden.

Neue Vorschriften der für die Sicherheit von Medizinprodukten und Daten zuständigen Behörden versuchen, das erhöhte Risiko nach Inverkehrbringen anzugehen.

Stark gestiegene Kundenforderungen nach Sicherheitskontrollen weltweit sind offensichtlich. In den USA spielen Sicherheitsfragen bei fast allen Ausschreibungen eine wesentliche Rolle.

Hohe Komplexität der vernetzten MedTech-Devices

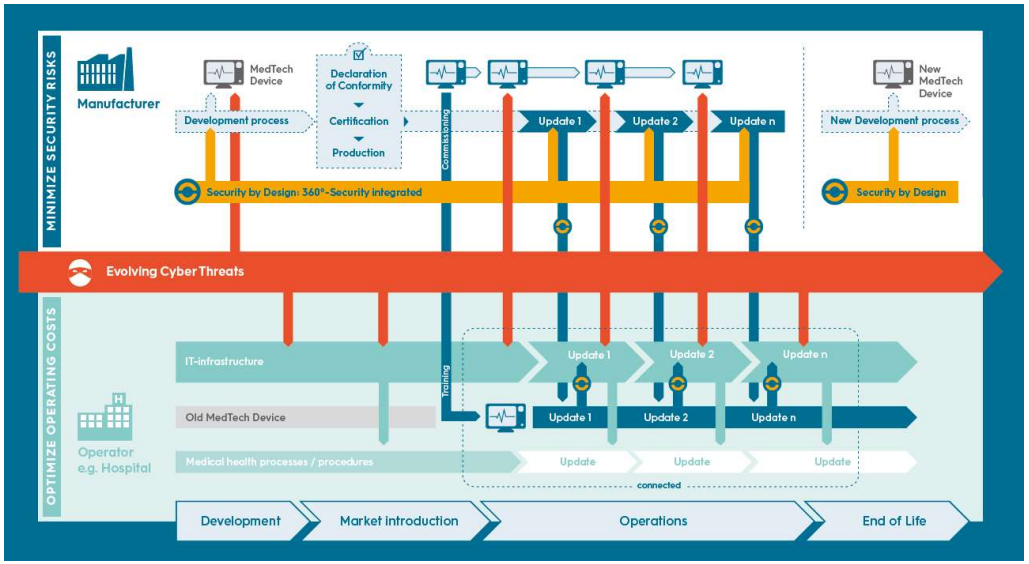


1 Integrativer Ansatz

2 Ganzheitliche IoT Security

3 Security by Design

Die Schlüsselfaktoren im IoT Product Life Cycle



Minimierung Sicherheitsrisiken

- Datensicherheit & Authentizität von Software
- Sicherstellen von Safety-Funktionen
- Anpassungen an Regulatorien und Cyber-Umfeld

Optimierung Betriebskosten

- Einfache sichere Integration
- Anpassungsfähigkeit an zukünftige IT Landschaft
- Erfüllen von regulatorischen Vorgaben
- Schutz gegen wandelnde Cyber-Bedrohungen

Anforderung Cybersecurity an das Med Tech Gerät

CyOne SECURITY

- Keine nicht unterstützte Standardsoftware auf neuen Geräten
- Regelmässige Sicherheitsupdates für die Betriebssysteme bereits eingesetzter Produkte
- Verwendung von Standardprotokollen zur Aktivierung von Schnittstellen
- Hoheit über Remote-Wartungsverbindungen muss bei den Krankenhäusern liegen
- Geräte müssen über Mechanismen verfügen, die mögliche Manipulationen erkennen können
- Schutz gegen Malware muss vorhanden sein
- Getestete Patches müssen in weniger als einem Monat bereitgestellt sein
- Dokumentation ist als Input für die Bewertung von Cyber-Risiken in Krankenhäusern wichtig
- Dokumentation ist für die kundenspezifische Konfiguration und Administration wichtig
- Hersteller stellt transparente Dokumentation für die Risikobewertung zur Verfügung

Abbildung der Forderungen in MDR und FDA

CyOne SECURITY

« Die Hersteller **legen Mindestanforderungen** bezüglich Hardware, Eigenschaften von IT-Netzen und **IT- Sicherheitsmaßnahmen einschließlich des Schutzes vor unbefugtem Zugriff fest**, die für den bestimmungsgemäßen Einsatz der Software erforderlich sind. (MDR, Anh. I, 17.4) »

« Gesundheitseinrichtungen treffen alle **technischen** und organisatorischen Maßnahmen, die notwendig sind, um bei netzwerkfähigen Produkten den **Schutz vor elektronischen Angriffen und Zugriffen** sicherzustellen. (MepV, Art. 72, Abs. 1) »

« **Electronic Records**
*information representation in digital form processed, **archived**, or distributed by a CS*

Persons who use open systems shall ensure the authenticity, integrity, and, as appropriate, confidentiality of electronic records from the point of their creation to the point of their receipt …
… ensure that the signer cannot readily repudiate the signed record as not genuine … (FDA, CFR21, part 11) »

« **Audit trails**
to record operator entries and actions that create, modify, or delete electronic records

- must be secure, computer-generated, time-stamped
- record changes shall not obscure previously recorded information.
- shall be retained (at least as long as that required for the subject electronic records)
- available for review (FDA, CFR21, part 11) »

«The assumption if being hacked at some point requires a solid mitigation strategy»

Mike Muller, CTO ARM (2015)

Massnahmen für Hersteller

Produkt

Sicherheit der Anwendung

- Langfristige Sicherheitsarchitektur
- Kryptologie und Sicherheitsmechanismen
- Cyber-Überwachung ermöglichen
- Software-Integrität / Secure Boot

→ Marktfähigkeit

→ Anpassungsfähigkeit

Wartung

Wartungsmöglichkeit

- Sicherere Zugänge für Wartung und Monitoring
- Geschützte Updates
  - Signiert (quanten-sicher?)
  - Downgrade-Schutz
- Reserve-Ressourcen

→ Widerstands-Fähigkeit

Entwicklung & Produktion

Infrastruktur und Prozesse

- Nachvollziehbarkeit von Releases
- Schwachstellen «tracken» (CVEs)
- Trennen von Test und Produktion
- Schutz langlebiger Schlüssel (HSM)

→ Update-Fähigkeit

Massnahmen für Betreiber

Analyse & Architektur

- Bedrohungsanalyse über Anwendungen und Umfeld
- Skalierbare und erweiterbare Sicherheitsarchitektur
- Sichere Produkte einsetzen

→ Implementierungs-Fähigkeit

→ «Defence in Depth» Umsetzung

Cyber-Überwachung

- Monitoring Geräte-Status
- Zentrales Logging
- Überwachen (SOC) und Auditing

→ Sicherheits-Update-Fähigkeit

→ Flexibilitätsfähigkeit

Prozesse

- Firmware-Updates
- Key- und Access-Management
- Security Reviews und Audits

→ Adaptions-Fähigkeit

Unsere Marktleistungen im IoT-Produktlebenszyklus

CyOne SECURITY

IoT-Produktlebenszyklus

Analyse / Konzept	Entwicklung	Zulassungen Compliance	Produktion	Bereitstellung Implementierung	Betrieb / Wartung	Migration
• Analyse Sicherheitsarchitektur und Anbindung IT nach Standards • Cyber-Risikobeurteilung • Sicherheitskonzept und -design	• Hardware • Software • Integration • Tests und Verifizierungen	• Validierung • Referenzumgebungen • Zertifizierung • Kundenvalidierung	• Fertigung • Logistik • Endmontage • Qualität • Konformität	• Erstkonfiguration • Installationprozesse • Systemintegration	• Betrieb • Überwachung • Verwaltung / Konfiguration • Updates / Upgrades • Reparatur / Support	• Migrationskonzept • Entsorgungskonzept • Ausserbetriebnahme

Kryptologische Herausforderungen

Sicherheitsprotokolle

Hardware-Design | **Hardware-Umsetzung**

Software-Design | **Software-Umsetzung**

Tests / Validierungs-verfahren

Sichere Fertigung

Sichere Logistik-prozesse

Reparatur und Support

Optionen für sichere Updates und Upgrades

System- und Netzwerkintegration

Betrieb und Wartung

Migration

Security by Design

Sichere MedTech.
Bit für Bit.

CyOne SECURITY

Lukas Christen
lukas.christen@cyone.ch
Telefon +41 41 748 85 76

cyone.ch