Öffentliche Präsentation

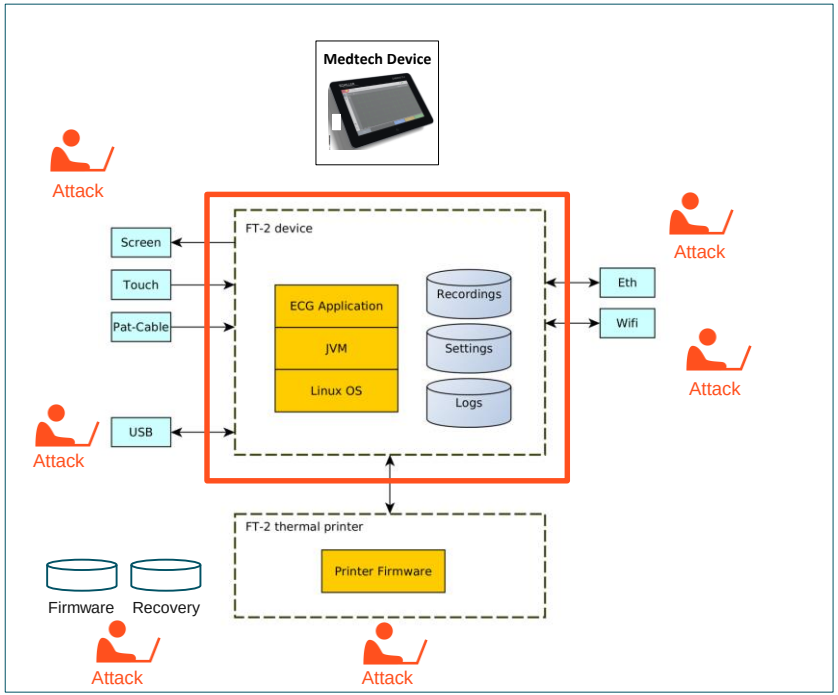
«Secure Healthcare Chain» Use Case eines Herstellers

01 – Externe Verwundbarkeitsanalyse

«unabhängige Expertenmeinung»

Verwundbarkeitsanalyse

Vernetztes Medtech-Gerät



Aufgabenstellung

Detektieren und dokumentieren von «relevanten» Verwundbarkeiten mit:

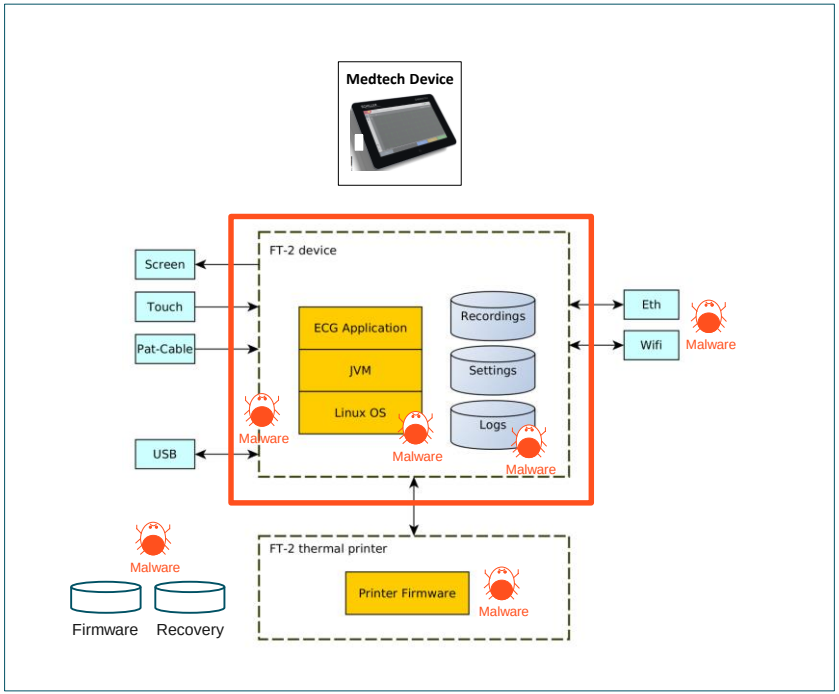
- Primären Fokus auf die Wifi- und Ethernet-Schnittstellen
- Sekundär auf USB und Thermal-Printer
- Benutzerinterface der ECG Applikation
- Recovery Image und Update Files

CyOne Security führte die Analyse mit einem «Whitebox»-Testansatz durch

Dazu wurden 16 verschiedene Angriffs-varianten ausgeführt (remote und lokal)

Relevante Verwundbarkeiten?

Vernetztes Medtech-Gerät

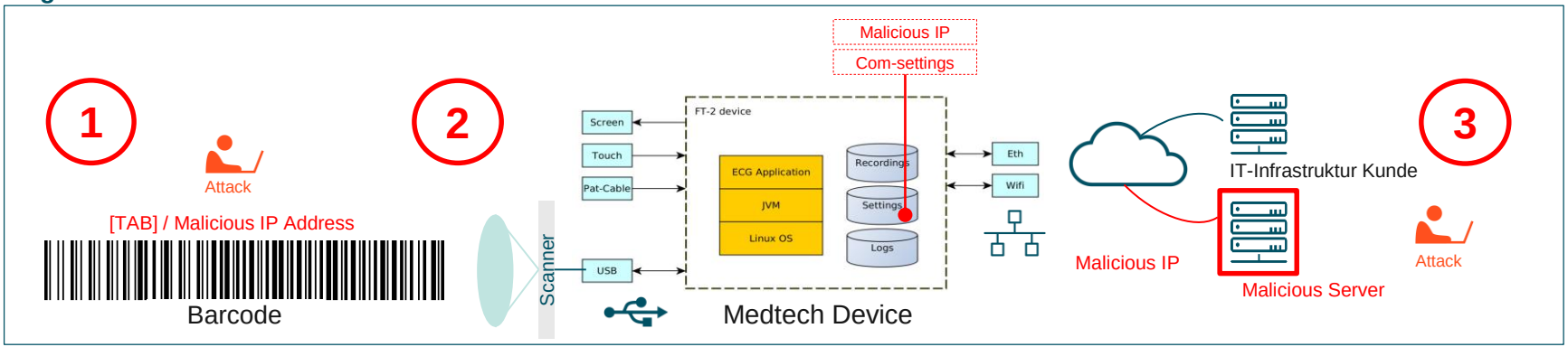


Was sind «relevante Verwundbarkeiten»?

- Angreifer kann diejenigen Daten stehlen, löschen oder manipulieren, welche direkt oder indirekt die Patientensicherheit gefährden können
- Dies während der Verarbeitung, Speicherung und Übermittlung
- Angreifer kann das Gerät übernehmen und Angriffe gegen die interne IT-Infrastruktur des Kunden (Betreiber) fahren
- Angreifer kann über einen Update oder Recovery-Prozess entsprechende Schadsoftware einschleusen

Ein Beispiel: Angriff via Barcode-Scanner

Angriffsszenario «Barcode Scanner»



Grundidee

1. Mit einem Generator wird ein Barcode erzeugt, welcher die Netzwerkeinstellungen des «Malicious Server» sowie die Anzahl Tabulatoren des entsprechenden Feldes enthält ([TAB]/IP-Adresse)
2. Mittels des vorhandenen Scanners wird der Barcode eingelesen und unter «Settings» die aktuelle Netzwerkeinstellung des Medtech-Geräts verändert (Angriffszeit < 2 Sekunden)
3. Das Medtech-Gerät kommuniziert neu mit «Malicous Server»

02 – Mehrwert des «Secure by Design» für Betreiber

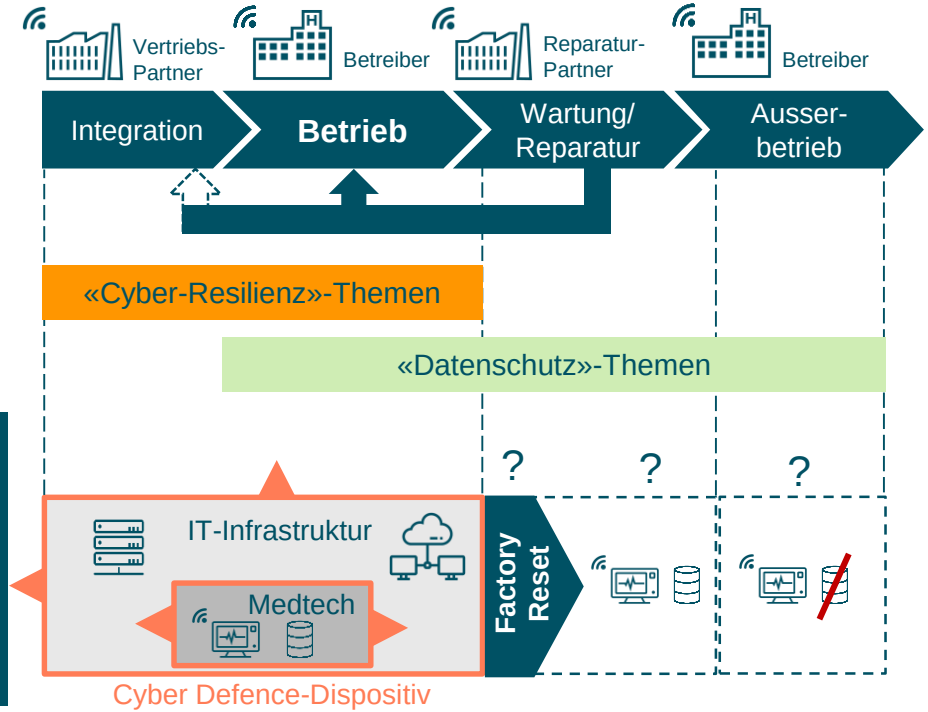
«eine sichere Healthcare Chain ist essentiell»

Herausforderungen der Betreiber

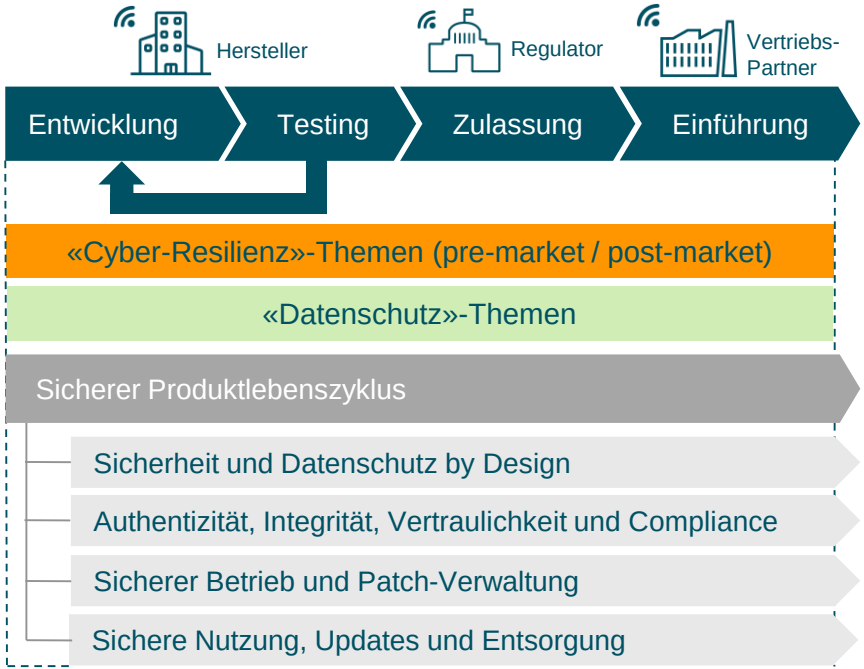
- Herausforderungen für Betreiber sind die sichere Integration und Betrieb, Wartung (inkl. Updates) und Reparatur und die Ausserbetriebnahme
- Prioritär steht das Thema «Cyber-Resilienz» der vernetzten Medtech-Geräte im Vordergrund
- Eher sekundär sind Schutz der kritischen Patientendaten für Betrieb, Wartung evtl. sogar Ausserbetriebnahme

Heute sehen wir:

- Ein zusätzliches Cyber Defence-Dispositiv infolge Konvergenz zwischen OT (Medtech) und klassischer IT
- Datenschutz während Wartung und Reparatur noch nicht optimal gelöst



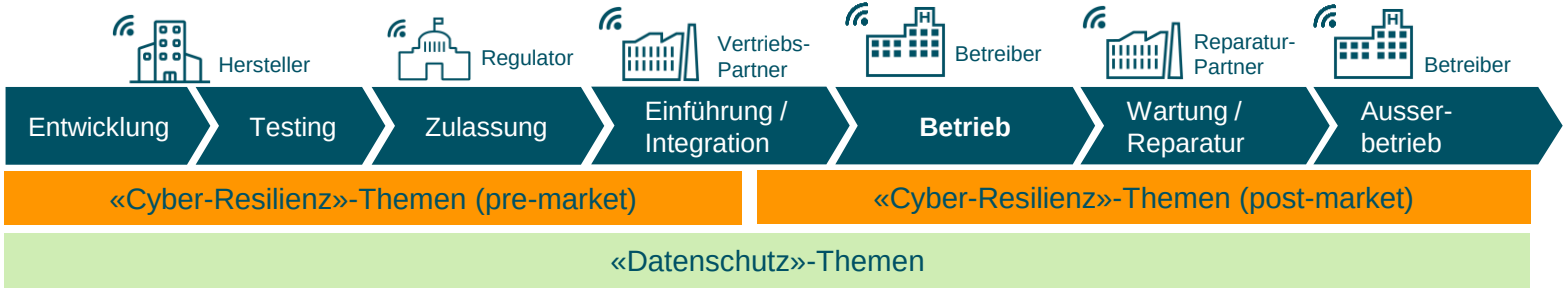
Hersteller: sicherer Produktlebenszyklus – «Secure by Design»



- Mit Blick auf den **ganzen** Produktlebenszyklus sollen Hersteller die «Cyber-Resilienz» und die «Datenschutz»-Themen integral betrachten
- Wichtige Punkte sind dabei:
  - Daten- und Benutzerauthentizität sowie Aspekte der Integrität, Vertraulichkeit und Nachvollziehbarkeit
  - Sicheres Patching und Update-Mechanismen für eine sichere Nutzung und einen sicheren Betrieb
  - Insbesondere der Datenschutz während Wartungs- und Reparaturzyklen inkl. Entsorgung muss auch gewährleistet werden

Sicherheitsmerkmale eines Produktes können und sollen gegenüber dem Kunden (Betreiber) als Verkaufsargument verwendet werden!

Vorteile «Secure Healthcare Chain» für Betreiber



Vorteile

- Einfachere Integration in existierende IT-Infrastruktur des Betreibers
- Reduktionsmöglichkeit des dezidierten Cyber-Abwehrdispositives und Überwachungsaufwandes – daraus resultierend geringere Betriebskosten
- Profitieren von regelmässigen Sicherheits-Updates
- Datenschutzaspekte sind während Wartungs- und Reparaturzyklen gewährleistet

Wir empfehlen Betreibern bei der Evaluation von neuen vernetzten Medtech-Geräten die «Secure by Design»-Aspekte mit zu berücksichtigen und bei den Herstellern aktiv einzufordern!

Sichere Schweiz.
Bit für Bit.

CyOne SECURITY

cyone.ch

BLOG Cyber Security

BLOG IoT Security