IOT SECURITY – ERFOLGSFAKTOR FÜR EINE MODERNE DIGITALE ARMEE

Vom Design bis zum Betrieb: 360°-Sicherheit konsequent integriert.

Das Internet of Things (IoT) vernetzt Dinge zu ganzen IoT-Ökosystemen: mit markanten Vorteilen und laufend neuen Einsatzmöglichkeiten im Behördenumfeld. Vernetzte Produkte und Systeme können aber auch zur Zielscheibe von Cyber-Angriffen werden – wenn Hersteller und Betreiber essenzielle Sicherheitsüberlegungen vernachlässigen.

CyOne SECURITY

Modularer Härtungsansatz: Die notwendige Differenzierung gegenüber zivilen Systemen

Skalierbare Sicherheitselemente decken die Vorgaben aus dem Sicherheitskonzept

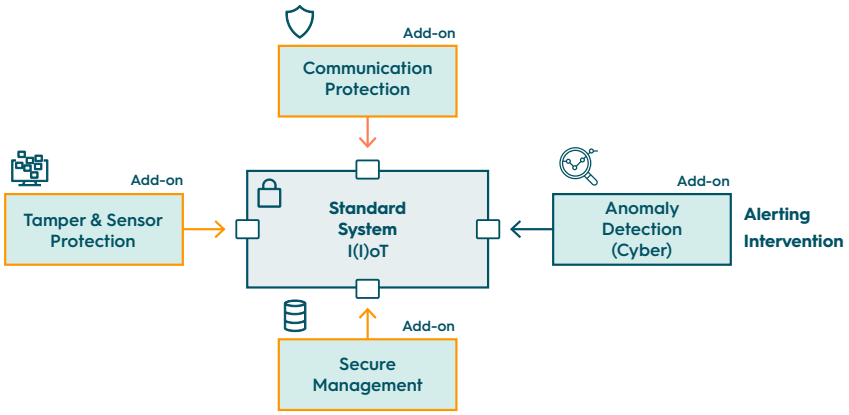
In der Projektphase kann auf die spezifischen Bedürfnisse aus dem Behördenumfeld eingegangen werden, und wo notwendig, Sicherheitselemente im Add-on-Prinzip hinzugefügt werden.

Skalierbarer Ansatz sichert Erfolg für Hersteller

Um als Hersteller nachhaltig Sicherheit im Behördenumfeld zu schaffen, darf nicht nur auf die Vernetzung einzelner Produktlösungen fokussiert werden, sondern auch auf die sichere Einbettung in die Umsysteme, sowie auf die partiell erhöhten Sicherheitsanforderung von Vertraulichkeit und Schutz vor Manipulation.

Wettbewerbsvorteil durch ganzheitliche IoT Security

Durch das Zusammenspiel aller Komponenten entsteht ein IoT-Ökosystem, in welchem die Sicherheit ein integraler Bestandteil sein muss. Die Sicherheit darf nicht nur auf die einzelnen Geräte beschränkt werden, sondern muss systemübergreifend betrachtet werden.

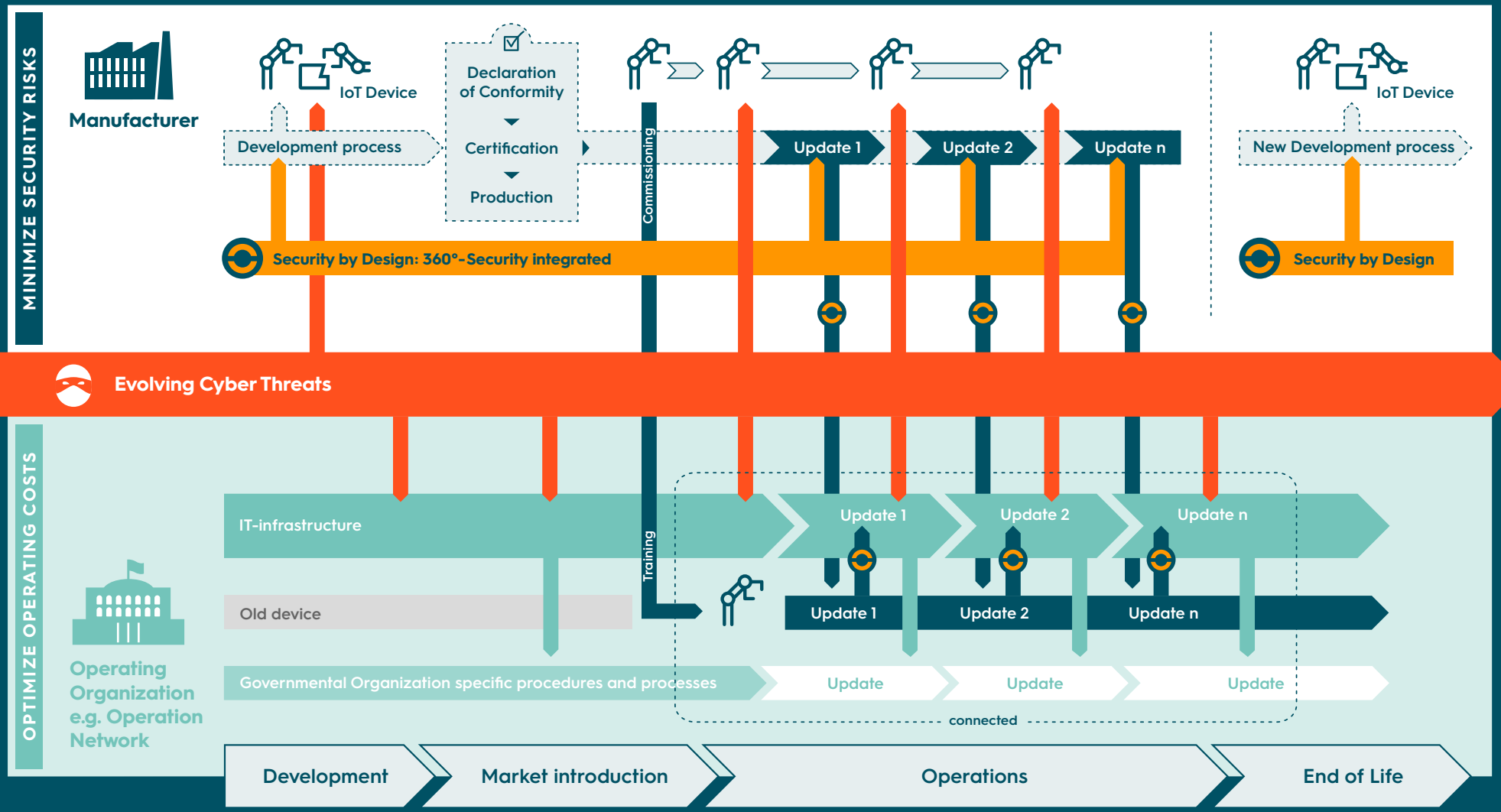


IoT Product Life Cycle 360°: Security integrated

Prävention, Adoption und Reaktionsfähigkeit

Intelligente Massnahmen minimieren Sicherheitsrisiken bei den Herstellern und optimieren die Betriebskosten bei den Betreibern.

Die Berücksichtigung aller Einflüsse wie Cyber-Bedrohungen, Digitalisierung, IT-Infrastruktur oder administrative Prozesse auf das Produkt ist essenziell – während des ganzen IoT Product Life Cycles!



Herausforderungen: Veränderung, Widerstand und Schutz

Vernetzte Produkte und Systeme werden während ihrem gesamten Lebenszyklus und ihrer Integration in Behördennetzwerke mit verschiedenen Herausforderungen konfrontiert.

Sie müssen deshalb:

1. mit den kontinuierlichen Veränderungen der hohen Sicherheitsvorgaben in redudanten Einsatznetzen schritthalten können.
2. sich innerhalb eines operativen und taktischen Prozessumfeldes behaupten.
3. sich gegen die sich dauernd weiterentwickelnden Cyber-Bedrohungen (auch von Seiten staatlicher Akteure) schützen lassen.

360°-Sicherheit: CyOne Security ist Ihr IoT Security-Experte

Sind die Sicherheitsanforderungen in der Produktentwicklung durch den ausgewählten Hersteller, sowie deren Implementierung von Projektbeginn an berücksichtigt und mit dem Sicherheitskonzept abgeglichen, können ein erfolgreicher Betrieb gewährleistet, Kosten minimiert und eine hohe Cyber-Resilience garantiert werden.

Sicherheitsdienstleistungen – für Hersteller und Betreiber

- Pentesting existierender Produkte und Systeme
- Überprüfen und analysieren von Sicherheitsarchitekturen
- Design der optimalen Sicherheitsarchitektur und Update-Fähigkeiten
- Design und Implementation kryptologischer Funktionen (z.B. Signieren von Updates)
- Datenseparation von klassifizierten Daten und geräterelevanten Systemdaten
- Design der richtigen IT-Sicherheitsarchitektur für die optimale Integration von vernetzten Produkten und Systemen
- Betreiben – sowohl für Betreiber als auch Hersteller – einer sicheren Update Plattform

Der Schutz Ihrer vernetzten Produkte und Systeme beginnt heute!

Machen Sie den ersten Schritt und analysieren Sie gemeinsam mit unseren IoT und Cyber Security-Experten Ihre aktuellen und zukünftigen Sicherheitsbedürfnisse.

→ Kontaktieren Sie uns für ein kostenloses Expertengespräch.

Reto Amstad
Senior Security Consultant
Direkt +41 41 748 85 16
reto.amstad@cyone.ch

Jetzt Blog abonnieren:
cyone.ch/blog-cybersecurity

CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

Telefon +41 41 748 85 00
info@cyone.ch
cyone.ch

CyOne SECURITY