ENTSCHEIDUNGS-CHECKLISTEN FÜR IHRE NACHHALTIGE ENTSCHEIDUNG

IoT Security «Make or Buy?»

Die Vernetzung schreitet unaufhaltsam voran. Produkte und Systeme werden Teil eines IoT-Ökosystems mit markanten Vorteilen und immer neuen Einsatzmöglichkeiten. Parallel zu dieser Entwicklung nehmen jedoch Cyber-Attacken auch auf IoT-Geräte rasant zu.

Hersteller und Betreiber sind zum einen gefordert, ihre Sicherheitssysteme auf den Prüfstand zu stellen. Zum anderen müssen IoT Security und Product Cyber Security von Anfang an in jedem Entwicklungsprojekt im Fokus stehen. Wie fit ist Ihr Unternehmen hinsichtlich Product Cyber-Risiken und IoT Security?

Lohnt es sich, die explizite «IoT und Product Cyber Security»-Fachkompetenz inhouse aufzubauen oder empfiehlt es sich, sie projektspezifisch einzukaufen? Die Frage, die sich deshalb jedes Unternehmen beantworten muss, lautet: «Make or Buy?»

Diese Entscheidungs-Checklisten helfen Ihnen bei der Entscheidungsfindung.

Schritt 1: Grundlagen schaffen.

Wenn Ihr innovatives IoT-Produkt gut funktioniert, eröffnet dies neue Möglichkeiten, vereinfacht Geschäftsprozesse und schafft Ihnen Wettbewerbsvorteile.

Im besten Fall resultiert daraus Unternehmenswachstum und die erfolgreiche Transformation in die Digitalisierung. Unabdingbare Voraussetzung für eine erfolgreiche Vernetzung ist die Sicherheit für Produkte und Systeme.

Mit der Beantwortung der nachfolgenden Fragen schaffen Sie sich die Grundlage für die Entscheidungsfindung.

→ **Nutzen Sie die nachfolgende Checkliste und erhalten Sie Antworten zu der Frage «Wie wichtig ist IoT Security und Product Cyber Security für uns und welche Grundlagen müssen wir schaffen?»**

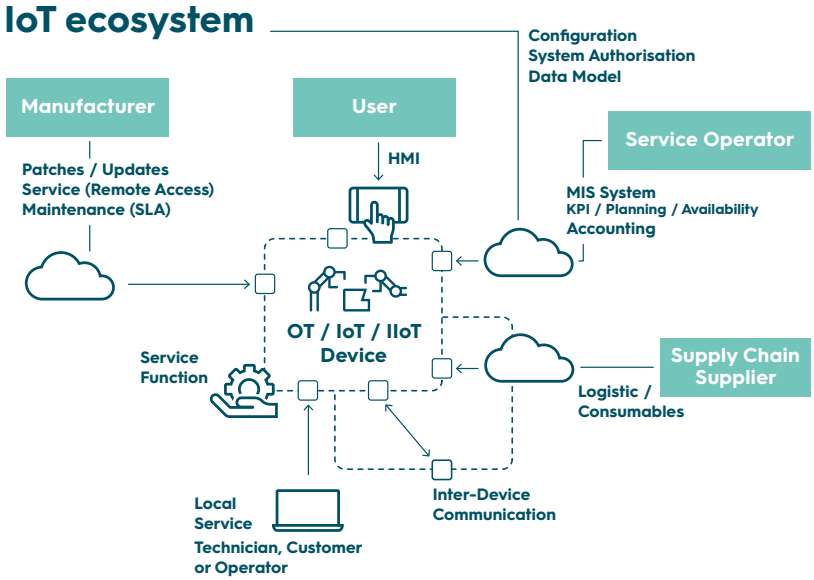
Ziele klären	**Ja**	**Nein**
IoT Security ist wichtig für unsere Produkte und Systeme hinsichtlich des weiteren Marktzugangs und zukünftiger IoT-Ökosysteme	☐	☐
IoT Security verschafft uns Wettbewerbsvorteile, sichert die Marktstellung und stimuliert das Unternehmens-wachstum	☐	☐
IoT Security hilft uns, unser positives Image auszubauen und Kundenverluste zu vermeiden	☐	☐
Unsere IoT-Produkte und -Systeme erfüllen die branchenspezifischen Sicherheitsanforderungen	☐	☐
Kosten prüfen	**Ja**	**Nein**
Wir kennen die Initial- und Personalkosten für den Kompetenzaufbau von IoT Security in Hard- und Software	☐	☐
Wir haben ausreichend personelle Kapazitäten, um IoT Security-Kompetenzen aufzubauen	☐	☐
Wir kennen den Return-on-Invest beim eigenen IoT Security-Kompetenzaufbau	☐	☐
Wir verfügen über genügend flüssige Mittel, um die Investitionen für den IoT Security-Kompetenzaufbau sicherzu-stellen	☐	☐
Durch den Aufbau von IoT Security-Kompetenz werden keine Investitionen in andere wichtige Projekte im Kern-geschäft blockiert	☐	☐
Vertraulichkeit definieren	**Ja**	**Nein**
Wir haben Prozesse und Reglemente für die Zusammenarbeit mit Projektpartnern bezüglich Wissens- und Infor-mationsschutz	☐	☐

Schritt 2: Sicherheitskomplexität verstehen.

A) IoT-Ökosystem

Wer als Hersteller nachhaltigen Mehrwert schaffen will, legt den Fokus nicht nur auf die Vernetzung einzelner Produktlösungen, sondern auch auf die Synergien im Betrieb eines IoT-Ökosystems mit der Sicherheit als integraler Bestandteil.

➜ **Mit der Beantwortung der nachfolgenden Fragen schaffen Sie sich einen Überblick über das intern vorhandene Verständnis und die Sicherheitskompetenzen in Bezug auf die Komplexität Ihrer vernetzten Produkte.**

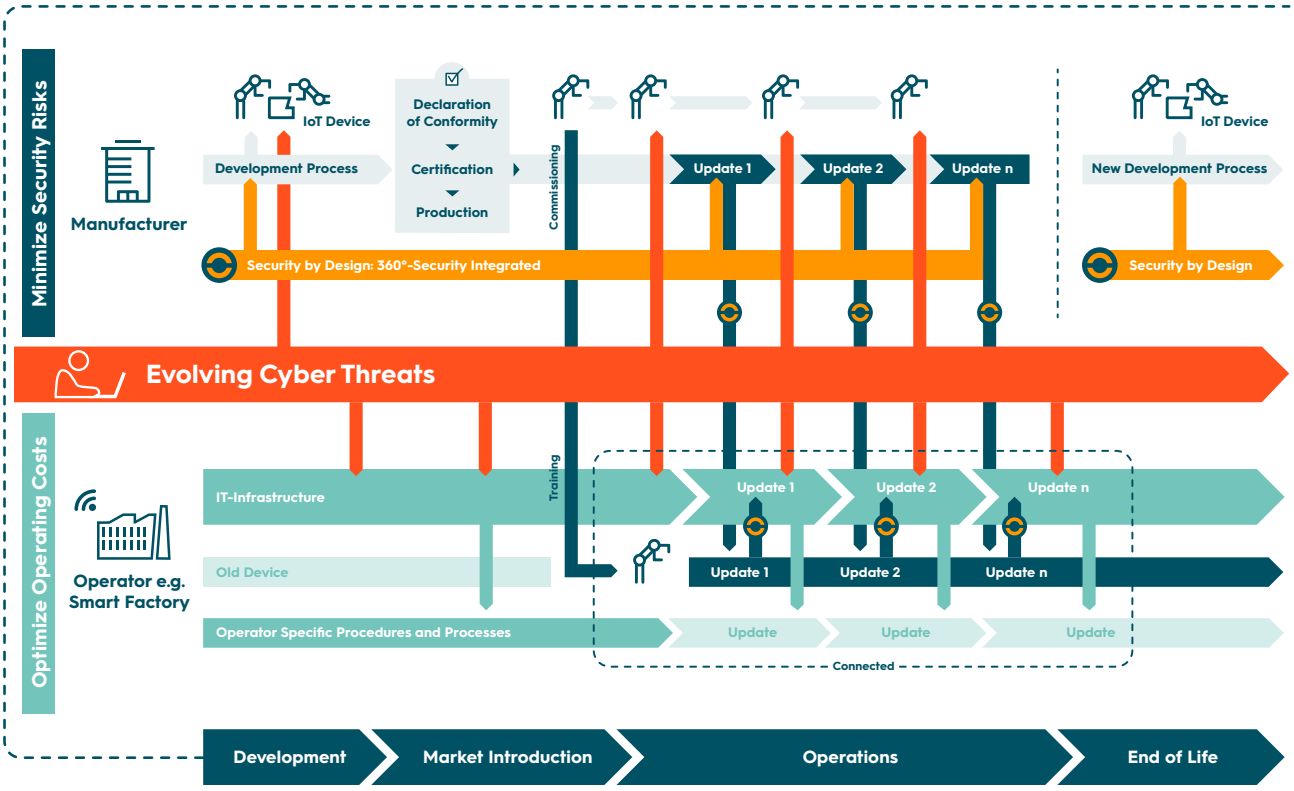


Sicherheitskomplexität	Ja	Nein
Verstehen wir die Sicherheitskomplexität unserer Produkte im IoT-Ökosystem?	☐	☐
Kennen wir die Sicherheitsrisiken unserer Produkte im IoT-Ökosystem?	☐	☐
Datensicherheit, Datentrennung, Datentransfer, Schnittstellen	**Ja**	**Nein**
Können wir den unterschiedlichen Stakeholdern Zugang zu ihren Daten verschaffen, ohne dass sie gegenseitig zu einer Schwachstelle für Angriffe werden?	☐	☐
Können wir die Datenhoheit der verschiedenen Stakeholder sichern?	☐	☐
Sind wir in der Lage, die externen Anbindungen sowie die Inter-Device-Verbindungen zu sichern?	☐	☐
Können wir sicherstellen, dass die digitalen Daten aus Prozessen nachvollziehbar und unveränderbar sind?	☐	☐
Sicherheitsstandards	**Ja**	**Nein**
Kennen wir die geforderten Sicherheitsstandards unserer Kunden und deren Branche?	☐	☐
Kennen wir die heutigen Cyber-Bedrohungen für unsere Geräte und die Bedrohungen aus dem Umfeld und wissen wir, wie wir diese minimieren können?	☐	☐
Können die Safety- und Compliance-Auflagen aus den Regulatorien erfüllt werden?	☐	☐
Sicherheitsanalyse	**Ja**	**Nein**
Haben wir die nötigen fachlichen Kompetenzen und personellen Ressourcen für regelmässige Sicherheitsanalysen?	☐	☐

B) IoT Security Product Life Cycle

Security by Design minimiert die Sicherheitsrisiken bei den Herstellern und optimiert die Betriebskosten bei den Betreibern. Es ist deshalb essenziell, alle Einflüsse – Cyber-Bedrohungen, Digitalisierung, IT-Infrastruktur oder administrative Prozesse – von Beginn an zu berücksichtigen.

→ **Über den gesamten IoT Security Product Life Cycle werden verschiedene Anforderungen an die Sicherheitskompetenz gestellt. Die nachfolgende Checkliste hilft Ihnen dabei, sich eine Übersicht zu verschaffen.**



IoT Security Product Life Cycle	Ja	Nein
Kennen wir den IoT Security Product Life Cycle unserer Produkte?	☐	☐
Sind uns die Sicherheitsanforderungen unserer Kunden über den gesamten Product Life Cycle bekannt?	☐	☐
Sicherheitsarchitektur	**Ja**	**Nein**
Ist die Datensicherheit und Authentizität der Gerätesoftware sichergestellt?	☐	☐
Kennen wir die notwendigen Sicherheitsvorkehrungen für Datensicherheit, Datentrennung, Datentransfer und Schnittstellen in der Sicherheitsarchitektur?	☐	☐
Lassen sich die Safety-Funktionen und damit das Verunmöglichen von Manipulationen garantieren?	☐	☐
Integration	**Ja**	**Nein**
Lässt sich das Produkt einfach und sicher in aktuelle und zukünftige IT-Landschaften beim Kunden integrieren?	☐	☐
Ist der Schutz vor sich wandelnden Cyber-Bedrohungen gegeben?	☐	☐
Lässt sich die installierte Basis den Regulatorien und dem Cyber-Umfeld anpassen?	☐	☐
Sicherheitsdesigns	**Ja**	**Nein**
Haben wir die notwendigen fachlichen Kompetenzen und personellen Ressourcen für nachhaltige Security-Designs in unseren Produkten?	☐	☐

Schritt 3: Sicherheitskompetenzen klären.

Vernetzte Produkte und Systeme werden während ihres Lebenszyklus und durch die Integration in die Unternehmensnetzwerke mit verschiedenen Herausforderungen konfrontiert. Sie müssen:

- Schritt halten mit den Veränderungen der Sicherheit im Unternehmensnetzwerk
- sich behaupten im operativ und regulatorisch geprägten Prozessumfeld
- sich schützen lassen vor Cyber-Bedrohungen, die sich ständig weiterentwickeln

Ein Unternehmen muss also über zahlreiche Sicherheitskompetenzen in Hardware und Software verfügen, die sich von der herkömmlichen Cyber Security für IT-Infrastrukturen unterscheiden.

➜ **In welchen Bereichen sind Sicherheitskompetenzen vorhanden und wie oft werden diese benötigt? Die nachfolgende Checkliste hilft Ihnen, die spezifischen Fachkompetenzen für IoT Security zu klären.**

Produkt	**Ja**	**Nein**
Ist die Sicherheitsarchitektur und die Auswahl der Verfahren langfristig angelegt?	☐	☐
Sind Kryptologie und Sicherheitsmechanismen updatebar?	☐	☐
Kennen und haben wir die relevanten Cyber-Überwachungsmöglichkeiten?	☐	☐
Haben wir Schutzmechanismen für die Plattform umgesetzt (Secure Boot)?	☐	☐
Sind die Prozessdaten geschützt und unveränderbar (Signaturen für Files)?	☐	☐
Sind Änderungen am Gerät / Prozess nachvollziehbar (Sicheres Log und starke Authentifizierung aller Änderungen)?	☐	☐
Wartung	**Ja**	**Nein**
Gibt es sichere Zugänge für Wartung und Monitoring?	☐	☐
Lassen sich Updates schützen?	☐	☐
Ist eine Signierung von Updates gegeben?	☐	☐
Ist Downgrade-Schutz vorhanden?	☐	☐
Entwicklung, Produktion und Prozess	**Ja**	**Nein**
Ist die Nachvollziehbarkeit von Releases gegeben?	☐	☐
Kennen wir die eingesetzten Libraries und Software-Elemente, sodass Schwachstellen getrackt werden? (CVE)	☐	☐
Lassen sich Test- und Produktionsumgebungen trennen?	☐	☐
Sind Schutz und allenfalls Updatefähigkeit langlebiger Schlüssel (HSM) möglich?	☐	☐
Sind Kompetenzen und Ressourcen vorhanden, um Sicherheitselemente zu verifizieren und deren Güte und Fähigkeit im Einsatzszenario zu beurteilen?	☐	☐
Time to Market	**Ja**	**Nein**
Haben wir genügend Zeit, um diese spezifischen Sicherheitskompetenzen intern aufzubauen?	☐	☐
Haben wir genügend Ressourcen, um Softwareteile auf ihre Sicherheit zu verifizieren?	☐	☐

«Make or Buy?»: Die entscheidende Frage.

Die Entscheidung «Make or Buy?» im Bereich der IoT Security und Product Cyber Security kann für Ihr Unternehmen nur von Ihnen gefällt werden. Zur Unterstützung finden Sie nachfolgend eine Übersicht einiger Pro- und Kontra-Argumente auf der Basis unserer langjährigen Expertise:

MAKE Inhouse IoT Security

Vorteile

+ Compliance-Vorgaben
+ Volle Kontrolle über Prozesse und Mitarbeitende
+ Informations- und Wissensschutz
+ Erweiterung des Security Know-how
+ Kein Einfluss von Drittpersonen

Nachteile

– Schwierig, Fachkräfte zu rekrutieren
– Lange Aufbauphase
– Fixe Personalkosten

BUY Outsourcing IoT Security

Vorteile

+ Branchenspezifische Umsetzung
+ Bedürfnis- und projektspezifischer Leistungsbezug
+ Profitieren von Referenzarchitekturen und -designs
+ Spezifisches, langjähriges IoT Security Know-how
+ Klar kalkulierbare Kosten
+ Fachpersonal für Analyse, Design, Engineering, Implementation
+ Fokussierung auf Core-Business
+ Flexible Reaktion auf Nachfrageänderung
+ Risikoverlagerung auf Partner
+ Externe Qualitätskontrolle

Nachteile

– Zusätzlicher Partner
– Teilen von Informationen und Wissen

IoT Security-Experten-Tipp

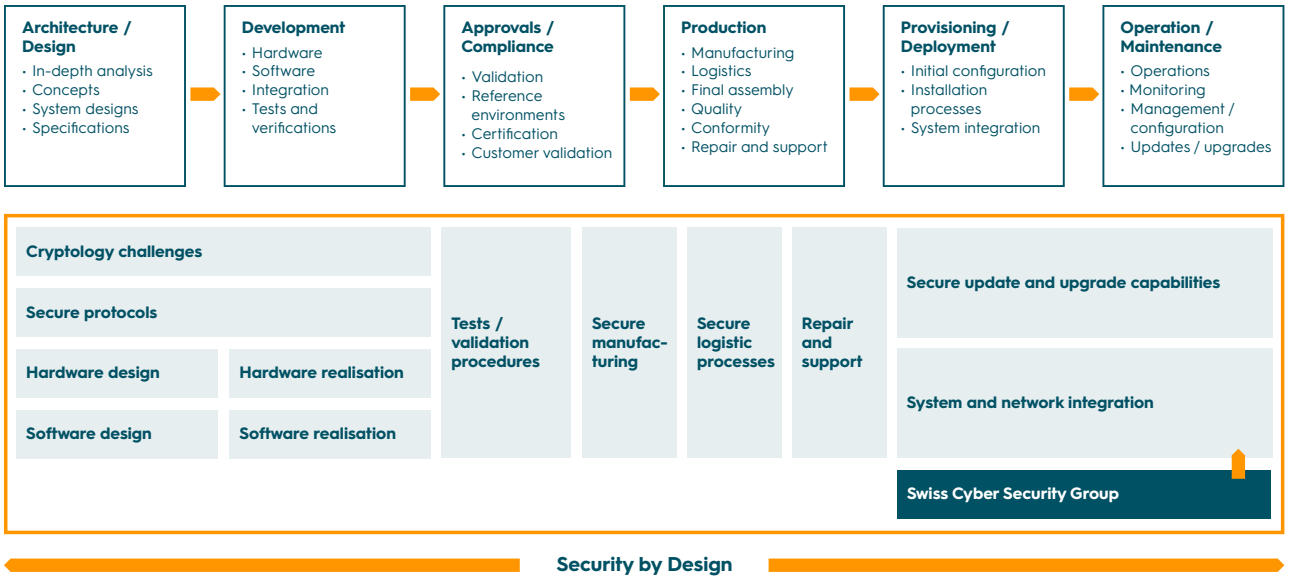
Die neuen digitalen Welten mit dem Internet of Things halten ein enormes Potenzial für alle Branchen bereit. Doch das IoT will seriös genutzt sein.

Dem effizienten Schutz vor Cyber-Attacken muss deshalb gemeinsam mit den Features, Functions und Big Data allererste Priorität eingeräumt werden.

Unser Tipp: Entscheiden Sie sich für eine nachhaltige IoT Security und Product Cyber Security und – als Konsequenz – für eine partnerschaftliche Zusammenarbeit mit CyOne Security: Dadurch schaffen Sie sich Zeit und Ressourcen für Ihre Kernkompetenz, innovative, vernetzte Produkte zu entwickeln und schlussendlich sparen Sie fixe Personal- und Betriebskosten.

Sie sichern sich damit auch tiefes, aktuelles Expertenwissen in IoT Security und Product Cyber Security sowie den Zugriff auf nachhaltige Sicherheitskonzepte und -lösungen.

→ **Profitieren Sie von den projektspezifischen IoT Security-Dienstleistungen der CyOne Security.**



Beginnen Sie heute und schützen Sie Ihre vernetzten Produkte und Systeme vor Cyber-Risiken.

Machen Sie den ersten Schritt: Suchen Sie das kostenlose Expertengespräch mit den CyOne Security-Experten und analysieren Sie gemeinsam die aktuellen und zukünftigen Sicherheitsbedürfnisse Ihrer vernetzten Produkte und Systeme.

→ **Kontaktieren Sie uns für ein kostenloses Expertengespräch.**

CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

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