



WISSENS-UPDATE

# Sicherheit – ein Must für jedes IoT-Projekt

Ivo Steiner | Sales Manager IoT Security | Steinhausen, 27. Dezember 2018

**IoT-Projekte verändern nicht nur die Prozesse einer Abteilung, sondern des gesamten Unternehmens. Häufig stellen sie gar das bisherige Geschäftsmodell infrage. Zudem bringen sie auch ganz neue Anforderungen an die Sicherheitsarchitektur mit sich, da durch die Vernetzung von Geräten und Maschinen neue Einfallstore für Cyber-Attacken entstehen. Sicherheit sollte bei IoT-Projekten deshalb oberste Priorität haben.**

Nur die wenigsten Unternehmen können die technologische Umsetzung von IoT-Projekten im Alleingang meistern. Serviceprovider und Spezialisten im IoT-Umfeld helfen nicht nur dabei, spezifische Probleme effektiv zu lösen, sondern auch, das Gesamtziel der Prozessoptimierung rasch zu erreichen. Idealerweise bringt der Partner Erfahrungen aus früheren IoT-Projekten mit und kennt sich auch im entsprechenden Markt- und Branchenumfeld aus.

## **Sicherheitsfragen Spezialisten überlassen**

Ein zentraler Punkt ist zudem die Sicherheit. Die wachsende Anzahl vernetzter Geräte macht Unternehmen anfällig für Cyber-Attacken – ein Punkt der in der IoT-Euphorie oft vernachlässigt wird. Es lohnt sich, einen separaten, erfahrenen Anbieter mit Sicherheitsfragen zu betrauen.

Hat man potenzielle Partner ins Auge gefasst, gilt es die vielversprechendsten IoT-Plattformen zu evaluieren. Grundsätzlich sollten sich die Auswahlkriterien an den prozessorientierten Herausforderungen beim Endkunden orientieren. Zudem ist es ratsam, eine flexible Lösung zu wählen, die sich schrittweise ausbauen lässt und Spielraum für Veränderungen bietet. Die Marktanforderungen ändern sich rasch. Agilität im Soft- und Hardwareumfeld sowie im Projektmanagement sind wichtige Schlüsselfaktoren.

Hat man sich für eine Software oder ein System entschieden, wird vor der eigentlichen Umsetzung ein Prototyp realisiert. Erfüllt der Prototyp die erforderlichen Kriterien, kann das Unternehmen mit der technischen und organisatorischen Umsetzung beginnen.

### **Erfolgsfaktoren bei der Umsetzung**

Erfolgreiche IoT-Projekte bedingen gemäss der eingangs erwähnten Studie von Cisco eine starke, technologieorientierte Kultur. Als wichtigste Erfolgsfaktoren nannten die befragten Unternehmen zudem die Kollaboration zwischen der IT- und Businessseite, die Beachtung des Themas in Führungsetagen und den internen Aufbau einer umfassenden IoT-Expertise. Zu Letzterem gehört auch, mit einem kompetenten Partner ein durchdachtes Sicherheitskonzept aufzustellen.

Die Geschäftsleitung erwartet in der Regel eine zügige Integration und einen schnellen Rollout. Deshalb sollte man sich realistische Ziele setzen. Es ist besser, in einem ersten Schritt einen Basisservice gut umzusetzen als an zu weit gegriffenen Konzepten zu scheitern. Dabei sollte immer die Zielgruppe im Blick behalten werden: Die Kunden und Mitarbeitenden, die sich mit dem neuen System anfreunden müssen. Ein Erfolgsfaktor ist somit auch die umfassende Schulung der Mitarbeitenden und gegebenenfalls auch der Kunden.

### **Mehrwert kontinuierlich überprüfen**

Ist der Basisservice erfolgreich implementiert, kann das Projekt stufenweise ausgebaut werden. Dabei gilt es drei Fragen im Blick zu behalten: Läuft das Projekt in die richtige Richtung? Können die internen Prozesse Schritt halten? Und hat der Endkunde tatsächlich den erhofften Mehrwert? Und ist die Datensicherheit gewährleistet? Wenn alle diese Fragen mit Ja beantwortet werden können, steht dem Ausbau des IoT-Projekts nichts im Weg.

### **CyOne Security ist der kompetente Partner für IoT-Sicherheit**

Bei der Entwicklung vernetzter Produkte und Systeme bleibt, wie oben beschrieben, die Sicherheit oft auf der Strecke, weshalb bisher erfolgreiche Sicherheitsansätze grundlegend überdacht werden müssen. Verfügbarkeit, Verhinderung von Zweckentfremdung und Wahrung der Datensicherheit sind zwingende Voraussetzungen für eine seriöse Nutzung des enormen Potenzials, das die neuen digitalen Welten für uns bereithalten.

Informations- und Datensicherheit ist bei jedem IoT-Entwicklungsprojekt ein substanzieller Bestandteil. Um die vernetzten Produkte und Systeme vor Cyber-Attacken zu schützen, bringt die CyOne Security AG tiefes Expertenwissen in Ciper- und Cyber-Security in die Sicherheitskonzepte und -lösungen ein, die auf der 360°-Sicherheitskompetenz von Product Security, System Security und Operational Security basieren.

## Beginnen Sie heute und schützen Sie Ihr Internet der Dinge vor Cyber-Risiken.

Machen Sie den ersten Schritt: Analysieren Sie gemeinsam mit unseren Experten Ihre aktuellen und zukünftigen Sicherheitsbedürfnisse Ihrer vernetzten Produkte, damit wir mit Ihnen über zielgerichtete Sicherheitslösungen diskutieren können.

**Kontaktieren Sie uns für ein kostenloses [Expertengespräch](#).**