CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

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

WISSENS-UPDATE

IoT-Sicherheit: Das Credo für Produktmanager lautet «Security by Design»

Erpressungsversuche oder Industriespionage schaden dem Geschäft und schwächen das Kundenvertrauen. Um das zu verhindern, muss Cyber-Sicherheit bei der Entwicklung von IoT-Geräten und -Lösungen für die Industrie oberste Priorität haben. Die Devise der Hersteller sollte lauten: «Security by Design». Was Produktmanager beachten müssen, damit ihre Produkte und Systeme sicher sind, erfahren Sie in diesem Wissens-Update.

Die Industriespionage ist mit dem Internet of Things (IoT) in eine neue Ära eingetreten. Durch die Digitalisierung und Vernetzung der Produktion stehen heute mehr Informationen denn je auf dem Spiel. Wer sich Zugang zu einer Produktionsanlage verschaffen kann, erhält detaillierte Daten zu Anlagensteuerungen, Maschinenparks, Produktionsdaten und letztlich auch Produkten. Bleibt der Datenklau unbemerkt, können Mitbewerber ein vergleichbares Produkt schneller und günstiger auf den Markt bringen oder die Marktleistung dem Markt besser anpassen.

Denkbar sind aber auch Erpressungsversuche von Cyber-Kriminellen, die sich Zugang zur Steuerung industrieller Anlagen verschaffen. Die Produktion steht dann so lange still, bis das Lösegeld bezahlt wird. Ein Angriff schwächt zudem das Kundenvertrauen, denn durch die zunehmende Vernetzung der Supply Chain stehen auch die Daten von Geschäftspartnern auf dem Spiel.

Diese Bedrohungsszenarien machen es deutlich: Hersteller von IoT-Geräten müssen Sicherheitsaspekten oberste Priorität einräumen.

IoT-Sicherheit als zentrales Verkaufsargument

Für die meisten Kunden aus der Industrie ist Cyber-Sicherheit schon heute ein zentrales Verkaufsargument. Doch längst nicht alle haben die Cyber-Risiken, die von IoT-Geräten ausgehen, erkannt. Das mag daran liegen, dass sich Industrieunternehmen zwar gewohnt sind, die Sicherheit der Information Technology (IT) sicherzustellen, wohingegen bei der Operational Technology (OT) – jenen Systemen also, mit denen die Produktion ausgeführt wird – Cyber-Sicherheit bislang kaum ein Thema war.

Beim Vertrieb von IoT-Geräten liegt es deshalb auch in der Verantwortung der Hersteller, das Thema Sicherheit einzubringen. Der Beratungsbedarf ist gross, der Markt ist unübersichtlich und eine Standardisierung liegt in weiter Ferne. Wer Kunden in diesem Dschungel von Lösungen die optimalen Technologien zum Aufbau eines sicheren IoT aufzeigen kann, verschafft sich einen entscheidenden Wettbewerbsvorteil.

Sichere Systemarchitektur durch «Security by Design»

Ein effizienter Schutz von IoT-basierten OT-Systemen beginnt bei der Produktentwicklung. Die Devise der Hersteller sollte deshalb lauten: «Security by Design». Diesen Fokus braucht es bereits bei der fachlichen Anforderungsanalyse. Die Systemarchitektur muss möglichst unempfindlich gegen Cyber-Angriffe sein und Schwachstellen müssen von Anfang an ausgemerzt werden. Dabei gilt es Angriffsvektoren zu identifizieren, aber auch künftige Risiken im Blick zu haben. So kann etwa die Funktion für sicheres Signieren und Kontrollieren eines Updatepakets die Cyber-Resilienz eines IoT-Geräts sicherstellen.

In der IT gibt der Sicherheitsstandard ISO 27001 den Rahmen für die Produktentwicklung vor. Im Bereich OT können sich Produktentwickler insbesondere an den von der International Society of Automation (ISA) erarbeiteten Normen IEC 62443 (ISA-99) und IEC 62264 (ISA-95) orientieren. Diese Standards für industrielle Kommunikationsnetze und Leitsysteme geben Anhaltspunkte für Risikoanalyse und Prozessdokumentation und zeigen beispielsweise die Mindestanforderungen an die Nutzungskontrolle oder die Systemintegrität auf. In Deutschland zertifiziert TÜV anhand dieser Vorgaben bereits Systeme für kritische Infrastrukturen.

Entscheidend für die Sicherheit einer IoT-Landschaft sind zunächst die Übertragungstechnologien, mit denen die Geräte vernetzt werden. Wo immer möglich sollten offene Industriestandards genutzt werden. Das ist insbesondere bezüglich Netzwerkschnittstellen und -protokollen von Bedeutung. Darüber hinaus sind bewährte Verfahren der Cyber-Sicherheit nötig. Dazu gehören digitale Signaturen für Software und Systeme, mehrstufige Authentifizierungsverfahren sowie eine durch kryptografische Methoden verschlüsselte Kommunikation. Besonderes Augenmerk gilt dabei der Geräteidentifizierung, -registrierung und -konfiguration.

Product und Security Lifecycle berücksichtigen

Eine industrielle IoT-Umgebung muss permanent überwacht werden – sowohl im Hinblick auf die Performance als auch in Bezug auf aktuelle und künftige Schwachstellen. Schliesslich ist das IoT-System einem ständigen Wandel unterworfen. Geräte werden hinzugefügt oder entfernt und laufend werden neue Applikationen und Funktionen in bestehende Systeme integriert. Somit müssen sich Entwickler auch damit beschäftigen, welche Angriffspunkte im weiteren Lebenszyklus entstehen könnten.

Im industriellen Kontext gilt es dabei stets die relativ lange Lebensdauer der Systeme zu berücksichtigen. Im Gegensatz zur IT, wo der Produktlebenszyklus drei bis fünf Jahre beträgt, liegt er im

Bereich OT bei fünf bis zwanzig Jahren. Hersteller von IoT-Geräten müssen für diesen Zeitraum die Bereitstellung von Updates garantieren, auch mit Blick auf funktionale Erweiterungen, die neue Sicherheitsfeatures verlangen. Somit ist der Produktlebenszyklus nicht allein von marktwirtschaftlichen und funktionstechnischen Faktoren abhängig. Vielmehr muss auch der gesamte Security Lifecycle in die Entwicklung einbezogen werden.

Ohne spezialisiertes Know-how geht es nicht – CyOne Security ist Ihr kompetenter IoT-Sicherheits-Partner

Aufgrund der hohen Sicherheitsanforderungen der Industrie und der wachsenden Komplexität der OT-Architektur ist es unerlässlich, mit Partnern zusammenzuarbeiten, die mit den Sicherheitsrisiken von IoT-Geräten vertraut sind.

Die CyOne Security unterstützt Produktmanager und Entwicklungsleiter dabei, das Prinzip «Security by Design» bei der Produktentwicklung von Beginn an zu berücksichtigen. Unsere IoT-Sicherheits-Experten kennen die aktuellen Bedrohungslagen und können die Entwicklung über den gesamten Security-Lifecycle hinweg einschätzen. Damit werden Produkte vom Markt besser akzeptiert und bleiben auch langfristig konkurrenzfähig.

Beginnen Sie heute, schützen Sie Ihre IoT-Geräte vor Cyber-Risiken und verschaffen Sie sich einen Wettbewerbsvorteil.

Machen Sie den ersten Schritt: Analysieren Sie gemeinsam mit unseren IoT-Sicherheitsexperten die aktuellen und zukünftigen Sicherheitsbedürfnisse Ihrer IoT-Geräte, damit wir mit Ihnen über zielgerichtete Sicherheitslösungen und -designs diskutieren können.

Kontaktieren Sie uns für ein kostenloses Expertengespräch.