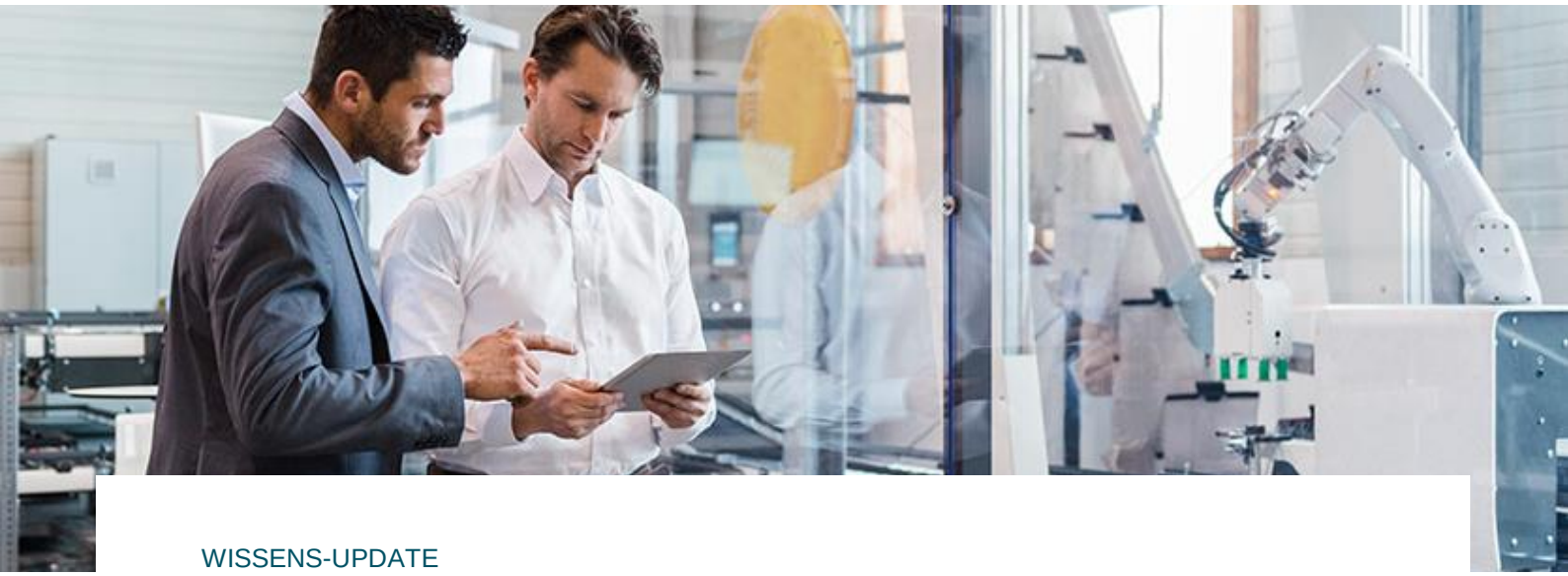
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

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



WISSENS-UPDATE

Sichere IoT-Geräte: «Security by Design» heisst die Devise für heutige Produktmanager

Cyber-Sicherheit sollte bei der Entwicklung von IoT-Geräten und -Lösungen für die Industrie oberste Priorität haben. Was Produktmanager beachten müssen, damit ihre Produkte und Systeme sicher sind – und somit langfristig am Markt bestehen können, erfahren Sie in diesem Wissens-Update.

Die Industriespionage tritt mit dem Internet of Things (IoT) in eine neue Ära ein. Durch die Digitalisierung und Vernetzung der Produktion stehen heute mehr Informationen denn je auf dem Spiel. Wer sich Zugang zu einer Produktionsanlage verschaffen kann, verfügt über detaillierte Daten zu Anlagensteuerungen, Maschinenparks und letztlich auch Produkten. Bleibt der Datenklau unbemerkt, können Wettbewerber 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 so lange still, bis das Lösegeld bezahlt wird. Ein Angriff hat zudem Auswirkungen auf das Kundenvertrauen, denn durch die zunehmende Vernetzung der Supply Chain stehen auch die Daten von Geschäftspartnern auf dem Spiel. Die Bedrohungsszenarien machen es deutlich: Hersteller von IoT-Geräten müssen Sicherheitsaspekten oberste Priorität einräumen.

Ihr Wettbewerbsvorteil durch IoT-Sicherheit

Für die meisten Kunden aus der Industrie ist Cyber-Sicherheit schon heute ein zentrales Verkaufsargument. Manche Industrieunternehmen haben die Cyber-Risiken, die von IoT-Geräten ausgehen, jedoch noch nicht erkannt. Das mag daran liegen, dass sich Unternehmen 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 jedoch 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, denn der Markt ist unübersichtlich: Zurzeit gibt es im IoT-Umfeld über 500 verschiedene Protokolle für die Datenübertragung 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.

«Security by Design» und Orientierung an Standards

Ein effizienter Schutz von IoT-basierten OT-Systemen beginnt bei der Produktentwicklung. «Security by Design» sollte die Devise der Hersteller lauten: Bereits bei der fachlichen Anforderungsanalyse muss der Fokus darauf liegen. 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 beispielsweise die Funktion für das sichere Signieren und Kontrollieren eines Updatepakets auf dem IoT-Gerät einerseits und anderseits die Updatefähigkeit und damit die Cyber-Resilienz im Feld garantieren.

Im Gegensatz zur IT, wo der Sicherheitsstandard ISO 27001 den Rahmen für die Produktentwicklung vorgibt, existiert für den Bereich OT bislang keine ISO-Norm. Dennoch gibt es durchaus Standards, an denen sich Produktentwickler orientieren können. Dazu gehören insbesondere die von der International Society of Automation (ISA) erarbeiteten Normen IEC 62443 (ISA-99) und IEC 62264 (ISA-95). 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.

Plug-and-Play darf nicht das Ziel sein

Entscheidend für die Sicherheit einer IoT-Landschaft sind zunächst die Übertragungstechnologien, mit denen die Geräte vernetzt werden. Wo immer möglich sollten offene Industriestandards wie Ethernet, WLAN, oder Bluetooth 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 kryptologische Methoden verschlüsselte Kommunikation. Besonderes Augenmerk gilt dabei der Geräteidentifizierung, -registrierung und -konfiguration.

Auf Consumer-Seite mag es sehr benutzerfreundlich sein, wenn ein Gerät nach dem Einschalten im Netzwerk und IoT-System automatisch erkannt und konfiguriert wird. Im industriellen Kontext ist dieses Plug-and-Play-Prinzip aber zu riskant. Für den Einsatz in der OT sollten neue Geräte erst identifiziert, authentifiziert und validiert werden, bevor sie anschliessend sicher in der IoT-Umgebung registriert werden.

Schlüsselfaktoren: Product und Security Lifecycle

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.

Die Garantie für langfristige Sicherheit darf aber nicht allein die Daten betreffen. Neben der «Security» ist für Industrieunternehmen auch der Aspekt der «Safety» zentral: Selbst in der hochautomatisierten Smart Factory der Zukunft werden Menschen arbeiten, deren Gesundheit es zu schützen gilt. Nicht zuletzt deshalb ist das Fehlen von verbindlichen Garantiefristen bei IoT-Geräten mit nicht zu unterschätzenden Gefahren verbunden.

Externes Knowhow ist unerlässlich – CyOne Security ist der kompetente IoT-Sicherheits-Experte

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.

CyOne Security unterstützt Produktmanager und Entwicklungsleiter dabei, das Prinzip «Security by Design» bei der Produktentwicklung von Beginn an zu berücksichtigen. Die 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 und schützen Sie Ihre IoT-Geräte vor Cyber-Risiken, um als Hersteller nachhaltig Erfolg zu haben.

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.