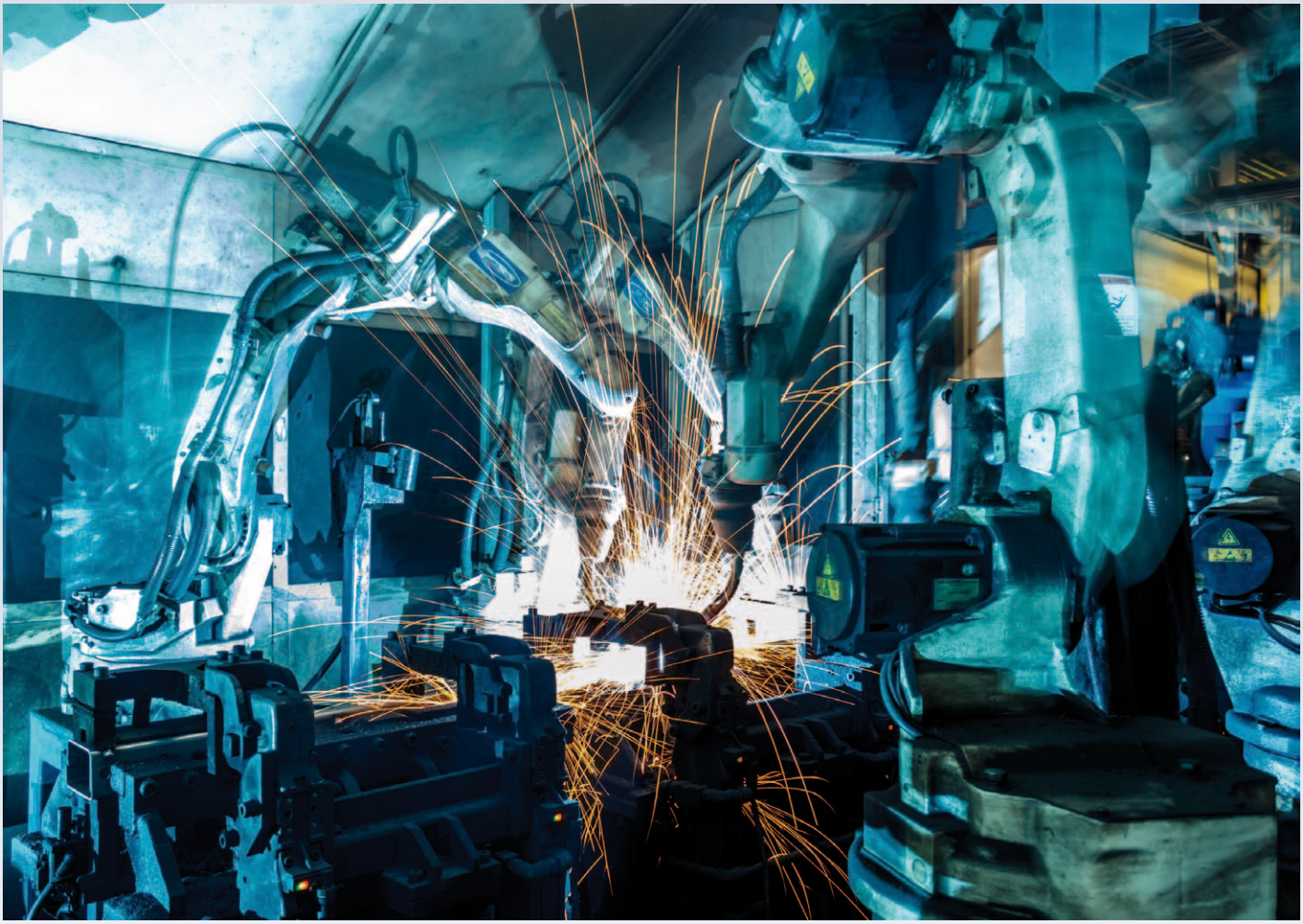
Die Fabrik von Morgen – sicher digitalisiert



Kurz gefasst

Die Fabrik von Morgen ist digital und vernetzt. Dadurch kann die Effizienz gesteigert werden, allerdings bieten Transparenz und Vernetzung auch ein breites Einfallstor für ungebetene Gäste. Wie kann die Kommunikation sicher gemacht werden und worauf kommt es an?

Die Implementierung von Industrie 4.0 erfolgt durch die digitale Vernetzung von Prozessen, Maschinen und Rechnern. Der Datenaustausch zwischen diesen Komponenten schafft durch die Zwischenschaltung eines Datensammlers Transparenz und ermöglicht Unternehmen die Optimierung von Produktionsprozessen. Allerdings öffnet er auch die Türen für Datenklau und Industriespionage – sofern nicht auf die Sicherheit geachtet wird...

Immer wieder lesen wir es in den Tageszeitungen, dass Unternehmen Opfer eines Cyberangriffs werden. Dabei berichten betroffene Unternehmen von den verheerenden Folgen, wenn Sicherheit nicht im Mittelpunkt der Implementation stand. Gut ein Drittel der Sicherheitsverantwortlichen von Unternehmen haben in einer aktuellen Umfrage angegeben, dass ihre industriellen Steuerungsanlagen von Kriminellen schon attackiert wurden. Während im Office-Bereich großen Wert auf die Sicherheit in Form von Firewalls, Honeypots oder auch Sandboxes gelegt wird, werden Vorkehrungen im Produktionsnetz sträflich vernachlässigt.

Durch völlig automatisiert ausgeführte Angriffe und Penetrationen von Firmennetzwerken bleiben Infektionen von ungeschützten IoT-Geräten jahrelang unbemerkt. Diese können über lange Zeiträume infiziert sein und dabei sensible Daten abschöpfen. Mit sicherheitsgehärteten Geräten gelingt die Kommunikation von der Maschinenwelt in die IT-Welt und in die Cloud ohne Verlust oder Korruption von Daten. Ein integrierter TPM Crypto-Chip bildet die Basis für härteste Sicherheitsmechanismen, die eine zuverlässige Implementierung neuer datenbasierter Dienstleistungen garantieren.

Worauf kommt es an?

Bei der Entscheidung für einen IoT-fähigen Datensammler ist es von höchster Relevanz darauf zu achten, dass das Gerät nach dem Security-by-Design-Konzept konzipiert wurde. Bei diesem Ansatz werden notwendige Sicherheitsmechanismen bereits bei der Entwicklung des Produkts identifiziert und reali-

Beispiel eines sicherheitsgehärteten Datensammlers der Firma Arend Prozessautomation

siert, da ganzheitliche Sicherheit als grundsätzliche Anforderung in den Entwicklungsprozess aufgenommen wird. Dabei sind z. B. Datenflussdiagramme, Bedrohungsanalysen sowie Nutzer- und Täterprofile zu erstellen und strenge Codierrichtlinien einzuhalten. Der umfassende Test des Sicherheitskonzepts und implementierter Sicherheitsfunktionalität, möglichst durch Externe, beendet die Entwicklung nach dem Security-by-Design-Ansatz.

Warum nicht einfach nachrüsten?

Würden erst im Nachhinein Maßnahmen zur Sicherheit getroffen werden, könnten lediglich noch Lücken gestopft werden. Ein durchgehender Schutz wäre nicht länger gewährleistet.

Sicherheit durch Absicherung des Betriebssystems

Der Schutz vor Schadsoftware wird zum Beispiel durch die Absicherung des Betriebssystems mit einem integrierten Hardware-Kryptoprozessor und einem Schlüsselspeicher garantiert. Auf dessen Basis wird ebenfalls die Datenkommunikation abgesichert und bietet Schutz, der weit über Software-Zertifikate hinausgeht. Auch die Integration in ein Security Information and Management System (SIEM) wird möglich. Im IoT-Cyber Security Konzept ist die Möglichkeit zum Update und Einspielen sicherheitskritischer Patches integriert.

Konnektivität

Um ein vielfältig anwendbares Gerät zu erhalten, spielt die Konnektivität des jeweiligen Geräts eine wichtige Rolle. Der offensichtliche Grund liegt darin begründet, dass unterschiedliche Maschinenparks mit unterschiedliche Anschlussmöglichkeiten und Kommunikationsprotokollen arbeiten. Um zu gewährleisten, dass eine breite Masse den jeweiligen Datensammler anbinden kann, ist eine hohe Konnektivität daher unabdingbar und macht das Gerät leicht integriebar. Jedoch wird der Konnektivität auch eine ganz andere Rolle zugesprochen: Wird ein Gerät mit limitierten Anschlussmöglichkeiten gewählt, so kann es unter Umständen zur Notwendigkeit der Zwischenschaltung eines weiteren Geräts zur Erfassung von Sensorwerten kommen. Dadurch bietet das Unternehmen Angreifern eine zusätzliche Angriffsfläche, sofern Netzwerkfähigkeit besteht. Davon abgesehen, entstehen den Unternehmen hierdurch zusätzliche Kosten. Daher sollte beim Kauf eines IoT-Devices darauf geachtet werden, dass ausreichend digitale und analoge Anschlüsse zur Verfügung stehen. Des Weiteren spielen serielle Schnittstellen, IO-Link, separierte LAN-Schnittstellen sowie die Möglichkeit der Einbindung von Datenbanken über ODBC eine wichtige Rolle.

Aufbau eines sicheren VPN-Tunnels

Besondere Relevanz für die Kaufentscheidung erhält eine separate und physikalisch trennbare Netzwerkschnittstelle, die als Fernwartungszugang für Steuerungen dient und nur nach vorheriger Authentifizierung genutzt werden kann. Diese sollte so gestaltet sein, dass sie sich automatisch nach einer gewissen Zeit bei Nicht-Abmeldung abschaltet. Durch diese zuschaltbare Netzwerk-Schnittstelle wird ein VPN-Zugang wesentlich sicherer, als mit einem herkömmlichen Schlüsselschalter, der im alltäglichen Produktionsalltag gerne vergessen wird wieder auszuschalten.

Konfiguration

Bei modernen Systemen wird heute keine separate Software zur Konfiguration des Datensammlers benötigt. Die vollständige Konfiguration kann in der Regel direkt über den integrierten Webserver vorgenommen werden. Hier können erfasste Sensordaten und Steuerungsvariablen vorab gefiltert, gespeichert und mit anderen Messwerten verknüpft werden. Aus den Sensordaten werden relevante Informationen erzeugt, die über das Web angezeigt oder über verschiedene Kommunikationsprotokolle in weitere Systeme geführt werden.

Visualisierung von Hauptwerten

Durch moderne Visualisierungskonzepte können ohne aufwändige Interaktion alle Hauptwerte von Komponenten und Aggregaten angezeigt werden. Die Hauptwerte können frei konfiguriert werden. Per Klick sind tiefere Einblicke in die Anlage, die Werteverläufe und Meldungen direkt einsehbar. Dabei können alle Sensoreingänge des Geräts je nach Einsatzzweck und Situation benannt werden. Jenseits der internen Visualisierung können bei modernen Systemen die erfassten und aufbereiteten Daten mit verschiedenen Protokollen weiterverarbeitet werden. Hierzu stehen unterschiedliche Industrie- und IT-Protokolle zur Verfügung. Zur Integration der Daten in Auswertungssysteme relevanter Lösungsanbieter (on-premise oder cloud-basiert) stehen verschiedene Konnektoren zur Verfügung.

Eine modulare Softwarearchitektur ermöglicht jederzeit eine flexible Erweiterung der Protokolle und Konnektoren, so dass die Zukunftsfähigkeit erhalten bleibt. Die Digitalisierung der Produktion bringt sehr viele Vorteile. Damit sich keine Nachteile einschleichen, muss auf die Sicherheit mithilfe zukunftsträchtiger sicherheitsgehärteter IoT-Devices geachtet werden. Bei der Kaufentscheidung sollten daher Security-by-Design und ausreichende Konnektivität die oberste Priorität haben.

Autorin:
Sara Hengel, Marketingleiterin bei Arend Prozessautomation GmbH
www.arend-automation.com