Sichere Infrastruktur in Produktionsnetzen

SASCHA LESER

Unter Internet of Things (IoT) versteht man die Vernetzung aller Komponenten eines Netzwerks. Jedes Gerät, das über eine eigene Rechenlogik verfügt, liefert Daten (Netzwerk-Switche, die Maschinensteuerung oder der WLAN-Access-Point). Weitere Knotenpunkte (Haussteuerung, handelsübliche Haushaltsgeräte) oder Maschinenteile (Antrieb) lassen sich durch nachträglich installierte Sensoren in jedes Netzwerk integrieren.

Unter Industrie 4.0 versteht man die Optimierung ganzer Wertschöpfungsketten durch die aus der Vernetzung verfügbar gewordenen Erkenntnisse aus Daten. Die Vorteile von gesammelten Daten liegen in der Möglichkeit zur korrekten Interpretation der Daten. So kann man beispielsweise erkennen, ab welcher Stückzahl das Präzisionswerkzeug einer CNC-Bearbeitungsanlage ausgetauscht werden muss, um Ausschuss zu vermeiden und unnötige Kosten zu verhindern.

Anwendungsfälle reichen von der Effizienzsteigerung bei der Produktion über Predictive Maintenance, also der Kostenreduktion durch die Vorhersehbarkeit von aufkommenden Reparaturfällen, bis zu noch nicht erschlossenen Absatzwegen durch die entsprechende Deutung der vorliegenden Erkenntnisse. Daten haben immer auch einen sehr starken Bezug zur Wertschöpfungskette. Durch Daten werden entweder Kosten vermieden oder neue Geschäftsfelder und digitale Services sorgen für zusätzliche Umsätze.

Getrieben wird diese Entwicklung nicht nur durch Entscheidungen des Managements, sondern oftmals auch durch externe Faktoren wie verändertes Verhalten des Kunden, der durch neue technische Möglichkeiten höhere Erwartungen hat als noch zu früheren Zeiten. Der Kunde erwartet unter anderem in Echtzeit den exakten Status und Standort seiner Bestellung abfragen zu können.

Um alle Daten miteinander in Einklang zu bringen, ist es unumstößlich, dass alle Daten in derselben Sprache miteinander kommunizieren. Das erweist sich in der Praxis jedoch als schwierig, da viele Hersteller auf proprietäre Protokolle setzen und sich erst langsam entsprechende Standards herauskristallisieren.

Foto: Montri/Fotolia

Mit Augmented Reality wird der Service an Maschinen unterstützt. Auf dem Bildschirm werden ergänzende Hinweise für den Monteur gezeigt.

Durch die komplette Vernetzung und Integration von Cloud-Diensten zu Analysezwecken ergeben sich zusätzliche Gefahrenquellen, da die Anzahl der Angriffsmöglichkeiten massiv zunimmt und bislang unter Sicherheitsgesichtspunkten vernachlässigte Geräte zu einem Einfallstor für Angriffe werden können. Eine nicht gepatchte Firmware der Kaffeemaschine kann zu einem Angriffspunkt für einen Hacker werden, wenn diese Kaffeemaschine mit dem Produktionsnetz verbunden ist.

Um eine sichere Produktionsumgebung realisieren zu können, muss daher eine mehrstufige Absicherung erfolgen, die bei der Schulung der Mitarbeiter beginnt und keinen relevanten Sicherheitsvektor außer Acht lässt.

Der erste Schritt ist die Abtrennung des Produktnetzwerks vom Unternehmensnetzwerk, um Übergriffe zu verhindern. Jedes Gerät, das Bestandteil des Produktionsnetzwerks ist, muss zusätzlich wenigstens durch eine Firewall abgesichert werden, um alle Angriffe auf die Maschinen zu verhindern. Die Datenkommunikation innerhalb des Netzwerks sollte verschlüsselt sein, um Schäden durch Datenlecks vorzubeugen. Gegen Trojaner, Viren und sonstige Schadsoftware hilft nur eine regelmäßige Überprüfung der Endgeräte durch einen Virenscanner mit einer aktuellen Virendatenbank. Die Verwendung von Wechselmedien sollte so gesteuert werden, dass nur verifizierte und von der IT kontrollierte Wechselmedien nutzbar sind und somit „Fremdgeräte“ gar nicht erst in der Lage sind, Schäden zu verursachen.

Drahtlose Netzwerke dürfen dabei nicht vergessen werden. So kann zum Beispiel ein WLAN Access Point mit derselben SSID wie die des Firmennetzwerks versehen und heimlich eingeschleust werden. Ohne Vorbeugen kann ein solches Fremdgerät für eine sehr lange Zeit im Netzwerk verbleiben und heimlich Schäden verursachen, ohne dass der Betroffene davon Kenntnis erlangt. Cloud-Anbindungen sollten ebenfalls ständig geprüft werden, da von intern nach extern kommuniziert und dadurch Ports geöffnet werden.

Foto: ADS-TEC

Bedienung und Wartung der Maschinen werden durch mobile Geräte erleichtert.

INFORMATIONEN

Über ADS-TEC

ADS-TEC ist Hersteller von Industrie-IT-Lösungen sowie von intelligenten Lithium-Ionen-Batteriespeichersystemen. Die Security-Lösung besteht aus einer sicherheitszertifizierten Firewall, einer Fernwartungslösung sowie einem zentralen Managementportal mit Unterstützung von Standardprotokollen und Schnittstellen.

www.ads-tec.de

Die jeweiligen Sicherheitsvektoren bieten jedoch nur ausreichenden Schutz, wenn die betriebene Firmware-Version jederzeit auf einem aktuellen Stand ist. Dies kann bei entsprechenden Stückzahlen nur über ein zentrales Managementportal gehandhabt werden, um die Übersicht zu behalten. Denn schließlich sollte die Firewall nicht durch mangelnde Beachtung vom wichtigsten Sicherheitsvektor zum Einfalltor werden.

Gerade für den exportorientierten Maschinenbau ist die Möglichkeit der Fernwartung immens wichtig, speziell auch für Abnehmer aus China, wo der Internet-Zugang stark reglementiert ist.

Neben der Absicherung aller Angriffsvektoren wird ein zentrales Portal benötigt, durch das die verschiedenen Sicherheitslösungen verwaltet werden können, das Alarm-Funktionen bietet und Monitoring-Funktionen bereitstellen kann. Dieses IoT-Portal muss zugleich die Schnittstelle in der Datenkommunikation darstellen. Durch die Unterstützung standardisierter Protokolle und Schnittstellen wird die Sicherheitslösung nahtlos in die vorhandene Infrastruktur integriert und bietet daher zugleich die Grundlage für Analytics.

Sascha Leser
Produktmanager Internet of Things
ads-tec GmbH