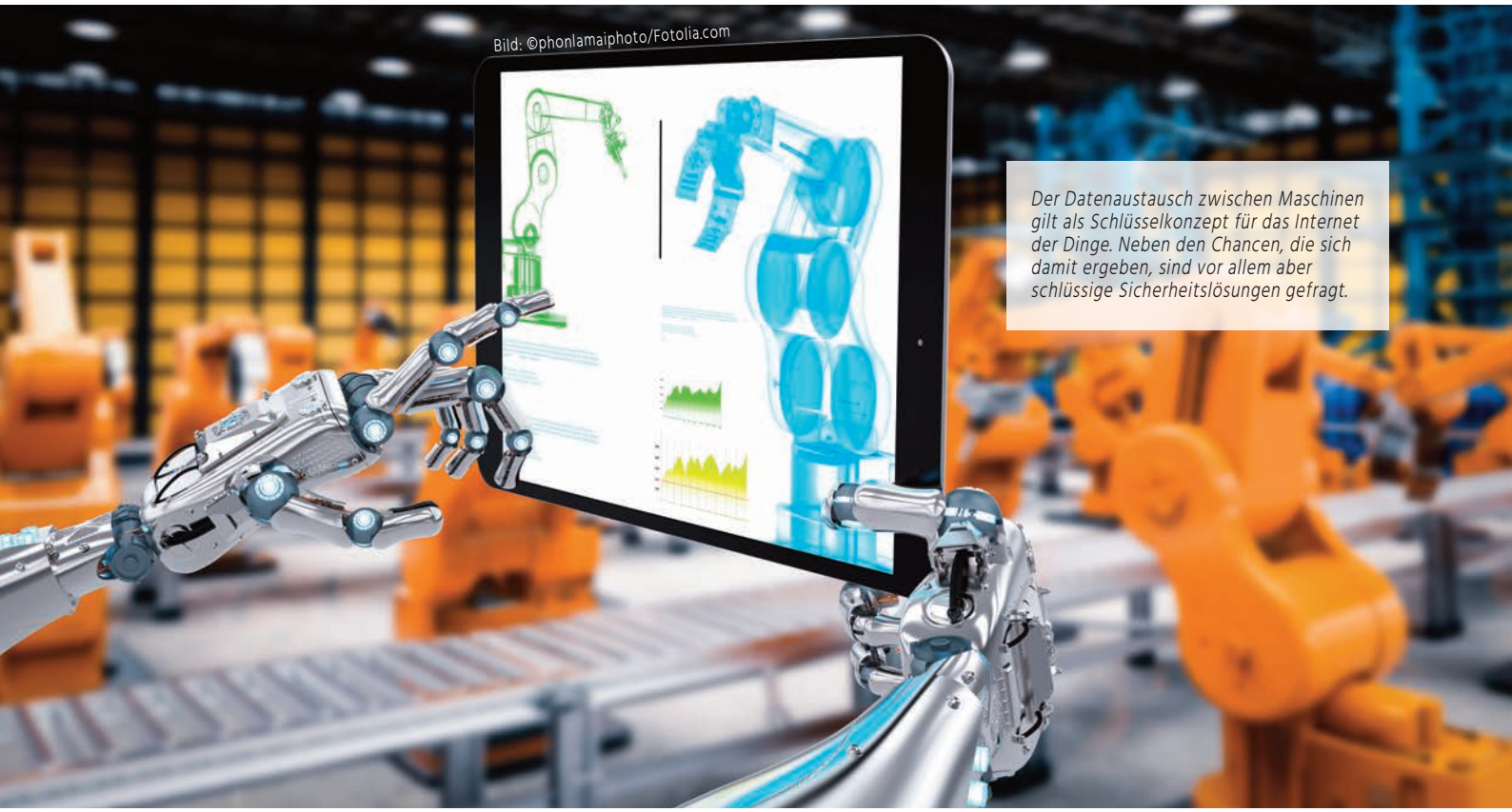

Der Datenaustausch zwischen Maschinen gilt als Schlüsselkonzept für das Internet der Dinge. Neben den Chancen, die sich damit ergeben, sind vor allem aber schlüssige Sicherheitslösungen gefragt.

Gefahren, Lösungen, Visionen

Die Identität für ein sicheres IoT

Der Datenaustausch zwischen Maschinen (M2M) ist ein Schlüsselkonzept für das Industrielle Internet der Dinge. Wesentlich für die erfolgreiche und vor allem sichere Vernetzung weltweit verteilter Systeme sind die Etablierung und Nutzung von geeigneten Standards sowie der Aufbau eines gemeinsam nutzbaren Vertrauensankers.

Sobald ein Unternehmen die Sprünge von der Mechanisierung, Elektrifizierung und Digitalisierung geschafft hat, steht mit dem nächsten Schritt der industriellen Revolution die Internetanbindung und Hochkonnektivität der cyber-physischen Systeme an. Dabei entsteht für Unternehmen die Herausforderung, ihre vormals gekapselten Systeme hin zu einem offenen System weiterzuentwickeln und abzusichern. Hierfür ist eine grundlegende Auseinandersetzung mit dem Thema IT-Sicherheit notwendig, die Antworten auf folgende Fragen geben muss:

- Darf Maschine MA von Unternehmen A Ware bei Maschine MB im Unternehmen B auf der anderen Seite der Welt rechtskräftig bestellen?
- Wie kann sichergestellt werden, dass Maschine MA mit Maschine MB von Unternehmen B kommuniziert und nicht jemand anders?
- Wie stelle ich eindeutige Maschinenidentitäten her und wie sichert man diese ab?
- Wie stellt man Vertrauenswürdigkeit her und welches Vertrauensniveau wird benötig? (LoA – Level of Assurance)
- Wie kann ich die Integrität der Daten während der Übertragung sicherstellen?
- Wie können die unterschiedlichen Architekturen in den Unternehmen, Maschinenparks (Technologien, Software und Hardware) und unterschiedlicher Performance-Kriterien (Limitierungen) umsetzen?

Sicherheit mittels Identität

Um die Sicherheitsherausforderungen des IoT und von Industrie 4.0 zu meistern, ist der Einsatz von eindeutigen Identitäten und Kryptographie unabdingbar. Damit Maschine MA von Unterneh-

Bild: ©vectorfusionart/Fotolia.com

Ein erster Ansatz zur vertrauenswürdigen Einbindung der IoT-Geräte und -Maschinen in das Netzwerk ist es, standardisiert Identitäten an die Devices zu vergeben.

men A neue Rohware bei Maschine MB im Unternehmen B bestellen darf oder andere Aktionen anfordern kann, bedarf es zunächst der Schaffung von Rahmenbedingungen. So ist beispielsweise sicherzustellen, dass eine vertrauenswürdige Einbindung der IoT-Geräte beziehungsweise der Maschinen in das jeweilige Unternehmensnetzwerk vorhanden ist – was nur mittels einer eindeutigen Identität möglich ist. Ein praktikabler Ansatz zur Realisierung dieser Grundvoraussetzung entsteht aus der standardisierten Vergabe von Identitäten an alle IoT-Geräte und -Maschinen – ähnlich den Standardprozessen zur Zuordnung digitaler Identitäten bei der Einstellung neuer Mitarbeiter. Erst die Vergabe eindeutiger Identitäten stellt beispielsweise sicher, dass nur bekannte (Maschinen-)Identitäten aus Unternehmen A überhaupt Anfragen beim Unternehmen B stellen. B muss sich dann auf die sichere Identitätsprüfung innerhalb der Domäne von A verlassen – eine klassische Vertrauensbeziehung wie sie in der IT seit Jahren erfolgreich mit Hilfe des Protokolls SAML 2.0 (Security Assertion Markup Language) etabliert wurde. Hierfür muss der bevorzugte Identitätsanbieter – in diesem Fall das Maschinenverzeichnis bei A – eine Vertrauensbeziehung zum Service-Provider aufbauen und nutzen.

Unternehmensübergreifende Sicherheit

Für den sicheren, auch über die Grenzen unterschiedlicher, teils stark beschränkter Architekturen hinausgehenden Datenaustausch, bedarf es eines ganzheitlichen Lösungsansatzes. Zwischen den Beteiligten sollte darum eine Einigung über die zu verwendenden Schnittstellen (API – Application Programming Interfaces) erzielt werden, damit Anpassungen schnell und praktikabel umsetzbar bleiben. Die Komplexität der bisherigen Schnittstellen für den Elektronischen Datenaustausch (EDI) und deren langwierige Versionsplanung sind den Anforderungen des IoT schlicht weg nicht gewachsen. Da die Verwendung der gemeinsamen Sprache für IoT-Devices und Maschinen aus Sicherheitsaspekten zudem häufig nicht ausreicht, müssen die Geräte auch in der Lage sein, mit cryptografischen Credentials umzugehen und eine verschlüsselte Kommunikation aufzubauen. Hierfür raten Experten, etwa die Firma Accessec, zum Einsatz von Prüfsummen und Zertifikaten. Hierbei sind etablierte Standards und Protokolle für die Authentifizierung der Teilnehmer sowie die Verschlüsselung und Signatur von Daten anzuwenden, da diese bereits von Experten geprüft und validiert wurden. Der Einsatz von fortschrittlichen Algorithmen und sicherem Schlüsselmaterial in Applikationen, Apps und IoT-Geräten ist in der Praxis jedoch nicht unproblematisch, insbesondere unter dem Gesichtspunkt der limitierten Geräte (Constrained Devices), die nur bedingt CPU-Leistung, Speicher und Batterie bieten. Für den sicheren Einsatz von IoT-Geräten muss über die zuvor beschriebene Prozedur die Zugehörigkeit des Endgerätes bestimmt werden (ist das Gerät im entsprechenden Kontext zugelassen), um eine Sicherheitseinstufung für die entstehende Verbindung zu ermöglichen und die jeweils erlaubten Aktionen zu bestimmen. Die Informationen können dabei über die physikalische Schicht, über die Transportschicht mit Meldungsprotokollen MQTT oder CoAP und schließlich über die Applikationsschicht ausgeliefert werden, wo schließlich auch digitale Signaturen, Message-Authentication-Codes, Sicherheitszertifikate, et cetera anwendbar sind. Dabei weisen die Protokolle MQTT oder CoAP für die M2M-Kommunikation jeweils Vor- und Nachteile auf, die abhängig vom Einsatz der jeweiligen Geräte und Applikatonen abgewägt werden müssen.

Zuverlässige Sicherheitsinfrastruktur

Die Kommunikation zwischen Maschinen wird in Zukunft eine große Rolle spielen. Eine wirksame Absicherung einer weltweiten Kommunikation im Unternehmensnetzwerk kann nur über eine eindeutige Identität der Geräte, einer Authentifizierung und Autorisierung über den Einsatz von Algorithmen und einer gemeinsamen Sprache erfolgen. Dabei ist die Einbettung der Geräteidentitäten in das Unternehmensnetzwerk, die Vergabe entsprechender Zertifikate, so wie der einhergehende Aufbau einer entsprechenden Sicherheitsinfrastruktur notwendig, um im IoT-Umfeld Einfluss auf die (externen) IoT-Geräte zu haben und die notwendige Kontrolle auf diese ausüben zu können. ■

Autor: ***Sebastian Rohr,***
Technischer Geschäftsführer,
Accessec GmbH
www.accessec.com

Autor: ***Markus Soppa,***
Research Consultant,
Accessec GmbH
www.accessec.com

Auszug aus dem Industrial Communication Journal Ausgabe 2/2017.