Heft 7-8, Juli-August 2015 | 13. Jahrgang 9,00€

manage it

[IT-Strategien und Lösungen]

Das moderne Rechenzentrum

Software Defined Data Center

Mikko Hypponen beim AIN der AXSOS AG

KMUs: Ausspähen leicht gemacht

Agile Governan

Sonderdruck

Artikel zum Thema Industrie 4.0

bridging IT

Menschen Methoden Lösungen

Enterprise

Cloud-Security im »Next Generation Workplace«

Industrie 4.0:
Erst am Anfang der Wegstrecke

Alles zu seiner Zeit

Die Idee für die Industrie ist verlockend: Im weltweiten Internet werden die Aufträge gesammelt. Sobald für ein bestimmtes Produkt eine ausreichend große Bestellung vorliegt, wird dieses Produkt automatisch gefertigt, indem dafür per Maschine-zu-Maschine-Kommunikation (M2M) alle erforderlichen Daten, Prozesse und Maschinen ein- und angesteuert werden. Mit der Fertigstellung wird selbsttätig die Auslieferung der Produkte angestoßen. Bis es soweit ist und Automatisierungs-, Steuerungssysteme, Sensoren und andere Maschinen und Fertigungskomponenten sicher miteinander sprechen, werden aber noch Jahre vergehen.

Was bis dahin für Fertigungsbetriebe zählt, ist das (sicherheits-)technisch und somit auch organisatorisch Machbare. So sind der M2M-Kommunikation bis heute enge Grenzen gesetzt. Für durchgängige M2M-Prozesse müssten die Maschinen und andere an den Prozessen beteiligten Fertigungskomponenten eigenständig die richtigen Datenbestände ansprechen und extrahieren können, um anschließend für den gezielten Datenaustausch die richtigen Maschinen und Komponenten zu identifizieren. Damit dieser Datenaustausch angriffs- und ablaufsicher über die Bühne geht, müssten die Maschinen und Komponenten außerdem dazu in der Lage sein, sich gegenseitig zu authentisieren und für zulässige Ausführungsschritte zu autorisieren. Dies alles kann nur funktionieren, wenn Identity and Access Management (IAM) sowie Verschlüsselungsfunktionen ab Werk zu einem integrativen Bestandteil der Maschinen und Komponenten werden. Noch mehr: Alle vernetzten Maschinen und Komponenten, also auch Durchflussmesser, Stellventile und Bedien-Panels, müssten wie heute Personen für die Zuordnung von Rechten über eine eigene Identität verfügen.

Notwendige Innovationen stehen noch aus. Streng genommen müssten diese integrierten Sicherheitsmechanismen nicht nur lokal, sondern auch im Zusammenspiel mit anderen Werksniederlassungen greifen, sowohl gegenüber firmeneigenen Werksniederlassungen als auch gegenüber den Werksniederlassungen von Zulieferern. Dies alles ist bis heute Zukunftsmusik, zumal nicht nur für die Interoperabilität, sondern auch für den Schutz und die Absicherung der M2M-Prozesse echte, also herstellerübergreifende Standards, noch nicht etabliert worden sind. Soviel steht schon heute fest: Weder herstellerspezifische Strategien und Standards aus der IT-Ecke noch aus der Fertigungsecke werden für die M2M-Kommunikation die notwendige Interoperabilität und Sicherheit ab Werk abbilden können. Gefordert sind stattdessen branchenspezifische Out-of-the-Box-Lösungen, die herstellerübergreifend auf Basis allgemein gültiger Standards zusammenwirken. Was der Markt heute für die M2M-Kommunikation stattdessen bietet, sind Prototypen, die für den realen Einsatz noch nicht geeignet sind. Sie werden dazu herangezogen, um in einer ersten Stufe die Transaktionen zwischen den Maschinen und Komponenten auszutesten. Die Thematik der Hardware-integrierten Sicherheitstechniken sowie Strategien und Standards für deren Integration werden wohl erst in einigen Jahren aufgegriffen werden.

Bis dahin müssen Fertigungsunternehmen, die in die Industrie 4.0 starten wollen, mit den (Sicherheits-)Techniken auskommen, die der Markt zur Verfügung stellt. Dazu zählen an den besonders gefährdeten WAN-Schnittstellen der TCP/IP-Protokollwelt Firewalls, Virtual Private Networks (VPNs), starke Verschlüsselungsverfahren, Fragmentierung von Datenpaketen sowie Intrusion Prevention Systeme (IPS) unterschiedlicher Couleur. In Ermangelung integrierter Sicherheitstechniken auf Prozessebene sollten Fertigungsunternehmen zudem für Industrie 4.0 organisatorische Vorkehrungen vorsehen.

Geeignete Vorkehrungen treffen. Sämtliche Maschinen und Fertigungskomponenten sollten klassisch innerhalb der firmeneigenen, abgeschotteten Cloud platziert werden, ebenso die Datenbasen, um darüber die Fertigung voranzutreiben. Ebenso schutzwürdig sind Auftrags- und Kundendaten. Kritische Daten und Systeme gehören in die eigene, abgeschirmte Cloud. Im öffentlichen, hoch angriffsgefährdeten Internet haben sie nichts zu suchen.

Dort, wo die vernetzte Fabrik via TCP/IP mit anderen Werksteilen des eigenen Unternehmens oder von Zulieferern zusammenspielen soll, sollte mit Bedacht vorgegangen werden. Generell sollte gelten: Kritische Daten sollten soweit wie möglich nicht nach Außen geben werden, dann können diese Daten auch nicht an physischen Netzverbindungen abgegriffen werden. Die einzelnen Vorkehrungen, die für Industrie 4.0 im Verbund getroffen werden sollten:

- Integration in die Corporate Cloud,
- klare Trennung zwischen eigenen Fertigungs- und fremden Lieferantendaten,
- redundante Auslegung von Verkabelung, Verbindungen, Systemen, Datenbanken, Sensoren und Steuerungen,
- hinreichende Abschirmung der Sensoren, die per Funk angesprochen werden, um darüber Systeme, Maschinen und Komponenten zu steuern,
- Firewalls platziert innerhalb einer De-Militarisierten Zone (DMZ),
- Einsatz von VPNs,
- Anwendung ausschließlich starker Verschlüsselungsverfahren,
- Fragmentierung der zu übertragenen Datenpakete, um sie erst am Ziel wieder in die Ursprungsform zusammenzusetzen,
- Einsatz von IPS und Anti-Advanced Persistent Threat (APT)-Programmen.

Zu solchen Vorkehrungen gehört auch, für das Gesamtprodukt kritische Teile

» **Die Thematik der Hardware-integrierten Sicherheitstechniken** sowie Strategien und Standards für deren Integration werden wohl erst in einigen Jahren aufgegriffen werden. «

nicht in Ländern wie China zu fertigen beziehungsweise fertigen zu lassen. Die Sicherheitstechniken sollten generell in Zeiten der Industriespionage und Ausspähungen durch Geheimdienste aus vertrauenswürdigen Quellen stammen. Einzelne, vor allem große Fertigungsunternehmen, gehen angesichts der Aktivitäten der NSA dazu über, unter anderem ihre Verschlüsselungsprogramme selbst zu entwickeln oder entwickeln zu lassen. Ein Kunde von bridgingIT geht noch weiter: Er baut für die Verarbeitung der Fertigungsdaten auf ein eigens für dieses Unternehmen entwickeltes Bus-System mit Schnittstellen für Zulieferer und Logistiker auf, integrierte Werkzeuge für Analysen, Simulationen und Trendermittlungen inklusive.

Status quo und nächster Schritt. Vorerst steht in den meisten Betrieben das Sammeln und Nutzbarmachen fertigungsrelevanter Daten im Fokus. Im nächsten Schritt werden sie die Realisierung von Industrie 4.0 angehen, soweit dies technisch und organisatorisch mit den zuvor genannten Vorkehrungen möglich ist. Schon in dieser Phase werden die Unternehmen auf weitere Fragestellungen passende Antworten finden müssen.

Inwieweit verändern sich mit den neuen Internet-lastigen Geschäftsmodellen Fertigungsketten, Wertschöpfungsketten und Organisationsstrukturen? Welchen Einfluss hat dies auf die bestehende Sicherheitsstrategie und die konzeptionelle Auslegung der Sicherheitsvorkehrungen? Wie bekommt das Unternehmen das mit Industrie 4.0 einhergehende enorme Datenwachstum physisch, logisch und analytisch in den Griff? Wie geht das Unternehmen mit den sozialen Veränderungen und Spannungen, verursacht durch eine fortschreitende Fertigungsautomatisierung, um? Ist das Unternehmen dazu bereit, intern eigene Sicherheitstechniken voranzutreiben, mit allen damit verbundenen Kosten, um so diese Techniken auf Dauer unter Kontrolle zu behalten? Ist das Unternehmen reif für einen IT-Strategiewechsel – statt Homogenisierung Heterogenisierung der Systeme -, um über Schnittstellenvielfalt seinen Back-end mit der Fertigung besser zu schützen?

Bis Kunden mit ihren Bestellungen im Internet aktiv an den Geschäfts- und Wertschöpfungsprozessen des Unternehmens mitwirken werden, indem sie im Hintergrund automatisierte M2M- und Logistik-Prozesse auslösen, ist allerdings noch ein weiter Weg. Die Jahre bis zum Industrie-4.0-Automatisierungszeitalter sollten Fertigungsunternehmen dennoch voll ausschöpfen. Denn die neuen Industrie-4.0-Strukturen und -Systeme erschließen verheißungsvolle Geschäftsmodelle und bergen so für die Unternehmen, trotz aller Risiken, enorme Entwicklungs- und Geschäftspotenziale.

Martin Jansen

Martin Jansen ist Senior Consultant innerhalb der Geschäfts- und Organisationsberatung von bridgingIT.