IT-SICHERHEIT UND INDUSTRIE 4.0

Vernetzung, Big Data und Cloud

CLAUDIA ECKERT, FRAUNHOFER AISEC

In Industrie 4.0 verschwinden die Grenzen zwischen den vormals getrennten IKT-Bereichen der Produktions-IT und der Business-IT. Diese werden vernetzt, wodurch IT-Systeme mit ganz unterschiedlichen Sicherheitsanforderungen verbunden werden. Daraus ergeben sich neue Verwundbarkeiten und den Angreifern eröffnen sich neue Möglichkeiten, in Systeme einzudringen und in der physischen Welt Schäden zu verursachen. So können sich beispielsweise Computerviren, die man von Desktop-PCs kennt, auf Produktionsanlagen ausbreiten, oder Maschinen zur Fernwartung freigegeben werden, ohne diese Zugänge ausreichend abzusichern.

1. Cyberphysikalische Systeme

Maschinen und Produkte werden in Industrie 4.0 zu intelligenten, vernetzten cyberphysikalischen Systemen. Viele Komponenten dieser Systeme sind hinsichtlich ihrer Speicherkapazität oder auch ihrer Rechenfähigkeit und ihres Energieverbrauchs beschränkt. Sie müssen rund um die Uhr ihre Aufgaben erfüllen, oft unter Einhaltung strikter zeitlicher Vorgaben. Sie sind zudem häufig zertifiziert, sodass es in der Regel nicht möglich ist, im Regelbetrieb Sicherheits-Patches, die aus der Business-IT wohlbe-

Bildnachweis: Fotolia

kannt sind, aufzuspielen, oder die Komponenten neu zu starten oder neu zu konfigurieren. Klassische Sicherheitstechnologie [1], wie man sie in der heutigen Business-IT findet, beispielsweise Viren-Scanner, Firewalls, VPNs oder SSL/TLS-verschlüsselte Kommunikation zwischen Browsern und Servern in der Unternehmens-IT, oder aber auch Techniken zur Identifikation von agierenden Nutzern, wie Zugangscodes und Berechtigungsausweise, sind nicht für die ressourcenschonende, einfache Absicherung beschränkter, vernetzter Komponenten im Automatisierungs- und Produktionsumfeld geeignet. Die Komponenten müssen in der Lage sein, sich untereinander sicher zu identifizieren, Manipulationen zu erkennen und gefahrlos miteinander zu kommunizieren. Sichere und überprüfbare Identitäten von Maschinen, der Schutz vor gefälschten und nachgemachten Produkten und die risikolose Maschine-zu-Maschine Kommunikation sind neue und wichtige Herausforderungen für die IT-Sicherheit in der Industrie 4.0. Benötigt werden neue Sicherheitstechniken, wie vertrauenswürdige Betriebssystem-Kerne für die beschränkten Komponenten, oder aber auch leichtgewichtige und dennoch starke Sicherheitsmechanismen, um Manipulationen zu verhindern beziehungsweise unschädlich zu machen.

Sichere und überprüfbare Identitäten von Maschinen, der Schutz vor gefälschten und nachgemachten Produkten und die risikolose Maschine-zu-Maschine Kommunikation sind neue und wichtige Herausforderungen für die IT-Sicherheit in der Industrie 4.0.

2. Evolution statt Revolution

Der Zeithorizont des Industrie 4.0-Trends unterscheidet sich sicher von anderen Zyklen und technologischen Transformationsprozessen, denn hier geht es um industriell genutzte Maschinen und Anlagen, deren Laufzeit für zwanzig Jahre und mehr vorgesehen ist. Die Migration von der heutigen Industrie 3.0 auf die nächste, von der intensiven Vernetzung zum Internet der Dinge geprägten Generation, wird also nicht als Revolution, sondern vielmehr als Evolution stattfinden müssen. Die Nachrüstung der Netzwerkschnittstellen von industriellen Komponenten etwa mit kryptographischen Verfahren zum Schutz des Datenaustausches ist keine Standardaufgabe. Zwar gibt es ausreichend bewährte Konzepte in der klassischen IT-Welt, diese lassen sich allerdings nicht ohne Weiteres in den industriellen Kontext übertragen. Zum einen müssen die Sicherheitslösungen mit den bestehenden Standards der Systeme kompatibel sein. Zum anderen laufen die Industriesysteme unter sehr strikten Echtzeitbedingungen. Das Zeitfenster für die Ver- und Entschlüsselung der Daten oder die Authentifizierung von Nutzern und Geräten ist äußerst klein. Erforderlich ist die Entwicklung von Sicherheitskonzepten für alle Ebenen: Dazu zählt zum Beispiel auch ein durchgängiges Berechtigungsmanagement. Damit wird klar geregelt, wer welche Aktionen an dem jeweiligen System vornehmen darf und kann. Neben dem Schutz vor Angriffen über das Internet muss auch die Sicherheit bei physikalischen Angriffen gewährleistet

KURZ UND BÜNDIG

Industrie 4.0 als Transformation der Industrielandschaft stellt die intelligente Vernetzung von Produkten, Maschinen und Produktions- sowie Wartungsprozessen in den Mittelpunkt. Das Cloud Computing als zentraler Bestandteil ermöglicht die Kommunikation zwischen Produktionsanlagen und Komponenten sowie die Speicherung der Daten. Dies bringt jedoch große Herausforderungen an die Sicherheit der Systeme mit sich. Neue Sicherheitstechnologien müssen entwickelt werden, die die spezifischen Industrie 4.0-Anforderungen wie Ressourcenbeschränktheit und ununterbrochene Verfügbarkeit erfüllen.

Stichworte: Industrie 4.0, Vernetzung, Big Data, Cloud Computing, IT-Sicherheit

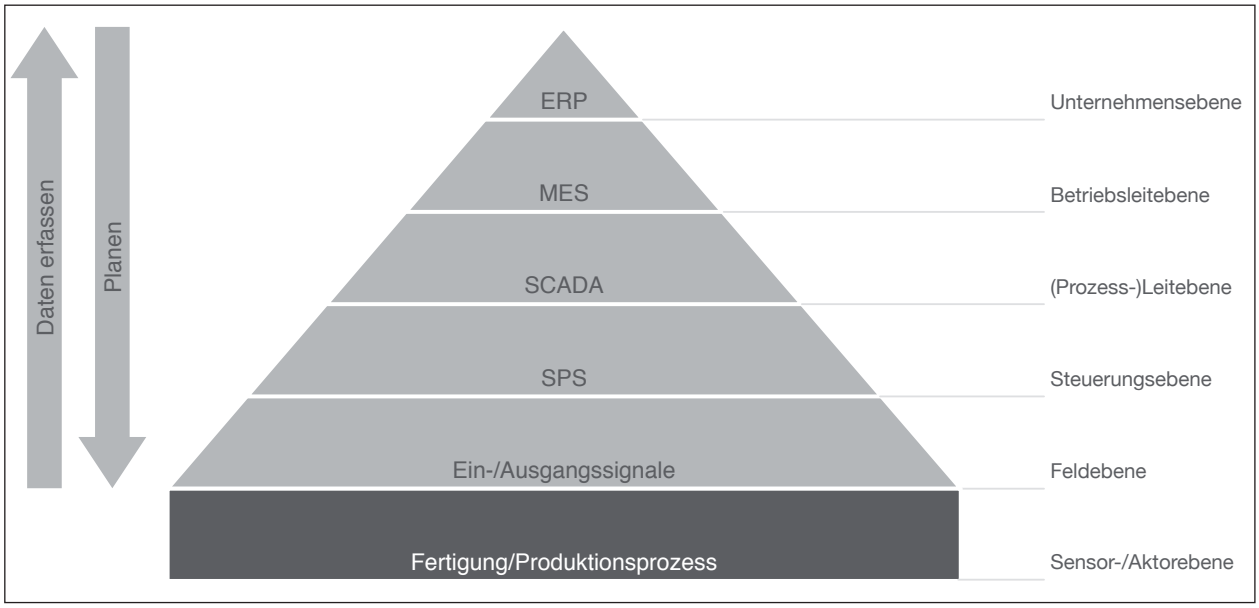

Abbildung 1: Klassische Automatisierungspyramide. Einsatz von Cloud Computing findet typischerweise auf den beiden oberen Ebenen der Pyramide statt.

sein. Dies lässt sich durch die Integration von sicheren Hardware-Bausteinen erreichen, sodass ein System sich nicht mehr booten lässt, wenn eine manipulierte oder gefälschte Komponente [2] in das System eingebracht wurde.

3. Big Data in Industrie 4.0: Segen oder Fluch?

Menschen, Maschinen, Produktionsanlagen, Geschäftsprozesse, Produkte und Dienste erzeugen ständig Daten. Zur Optimierung von Ressourcennutzungen und Geschäftsprozessen werden diese Daten in Realzeit zusammengeführt und effizient analysiert (Big Data). Die Daten dienen der Steuerung und Überwachung von Produktions- und sonstigen unternehmenskritischen Abläufen, sie steuern das Verhalten von Fahrzeugen oder auch von Anlagen und Maschinen. Eine gezielte Manipulation dieser Daten könnte somit verheerende Konsequenzen haben. Daten und Informationen können aber auch ein wertvolles Wirtschaftsgut sein, man denke beispielsweise an Produktionsdaten, die vor unberechtigten Zugriffen und Manipulationen zu schützen sind. Zudem wird eine Vielzahl von Aufenthaltsdaten, Bewegungsprofilen, Nutzungsprofilen oder auch Gewohnheiten von Nutzern der Anlagen und Maschinen erfasst. Dies stellt eine erhebliche Bedrohung der Privatsphäre dar. Die Gewährleistung einer datenschutzbewahrenden Verarbeitung von Daten ist eine zentrale sowohl gesellschaftliche als auch wirtschaftspolitische Aufgabe.

4. Herausforderungen für die IT-Sicherheit

Eine sichere Industrie 4.0 erfordert umfassende Maßnahmen, um die Korrektheit, Vollständigkeit und rechtzeitige Verfügbarkeit der Daten sowie die sichere Kommunikation und die Vertrauenswürdigkeit der eingesetzten IKT-Komponenten zu gewährleisten. Sie umfasst technologische, aber auch organisatorische Maßnahmen zur Steigerung von Vertrauen in IKT-basierte Systeme und Abläufe. Erforderlich sind neue methodische und technologische Ansätze, um die Sicherheit und Vertrauenswürdigkeit von IKT-Systemen prüfbar und kontrollierbar zu erhöhen. Das mit der Nutzung der IKT-Systeme einhergehende Risiko muss methodisch erfasst und quantifiziert werden und es müssen Prozesse und Verfahren entwickelt werden, um Risiken zu minimieren und um mit den verbleibenden Risiken verantwortungsvoll umzugehen. Langfristig tragfähige Lösungen erfordern die Entwicklung neuer Sicherheits-Technologien, die die Anforderungen hochgradig, unter Umständen spontan vernetzter und eingebetteter Systeme, zum Beispiel in Bezug auf Energie-Effizienz oder Realzeit-Anforderungen, erfüllen. Neue Sicherheitskontroll- und Schutzmaßnahmen müssen bereits frühzeitig in den

Entwurf der Systeme integrierte werden, um zukünftige IT-basierte Produkte und Systeme robuster und resistenter gegen insbesondere auch internetbasierte Angriffe zu gestalten. [3]

5. Cloud-Computing und Industrie 4.0

Cloud Computing spielt in der Vernetzung von Komponenten eine entscheidende Rolle. Durch ihre Eigenschaft, über das Internet angesprochen werden zu können und ihren serviceorientierten Charakter können Cloud-Dienste über Schnittstellen einfach genutzt werden und ihrerseits selbst auf andere Dienste zugreifen [4]. Diese Eigenschaften finden sich ebenfalls in der Entwicklung von Industrie 4.0 wieder: Auch Produktionsanlagen und deren Komponenten besitzen standardisierte Schnittstellen, die einen einfachen und homogenen Zugriff auf die Anlagenfunktionen und -informationen ermöglichen. Über diese Schnittstellen findet eine Öffnung der Systeme statt und eine Interoperabilität zwischen unterschiedlichen Komponenten und Anlagen kann durch eine Standardisierung der Schnittstellen erreicht werden. Skalierbarkeit, hohe Verfügbarkeit, schnelle Netzwerkverbindung und damit verbunden die Bereitstellung von Funktionalität durch definierte Schnittstellen nach außen machen also Cloud Computing zu einer Technologie, die grundlegend für Industrie 4.0 ist und die Umsetzung der Charakteristika wie des hohen Vernetzungsgrads der Industrieanlagen und der darauf basierenden Adaptivität und automatisierten Organisierung der Produktionsanlagen erst ermöglicht. Die Einführung von standardisierten Anlagekomponenten ermöglicht eine immer einfachere Zugänglichkeit und erlaubt den einfachen Zusammenschluss von Industrieanlagen in Cloud-Plattformen. Nicht nur aus Kostengründen ist diese einheitliche Möglichkeit des Zugriffs auf Maschinen attraktiv: Servicepersonal kann unterschiedliche Anlagen über eine einheitliche Softwareplattform erreichen und verwalten. Auch eine zentrale Sammlung von Daten wird einfacher, wenn sich die Schnittstellen der verschiedenen Maschinen gleichen. Zudem erlaubt sie eine Analyse unter Einbeziehung von Monitoring-Daten sämtlicher Systeme und Ebenen, wie in Abbildung 1 zu sehen.

6. Sichere Cloud-Systeme in der Industrie 4.0

Das risikolose Cloud-Computing ist für die sichere Industrie 4.0 eine zentrale Fragestellung. An das Sicherheitsniveau von Cloud-Services werden hohe Anforderungen gestellt: Die Übertragung von Daten und Steuerbefehlen zwischen dem Cloud-Service und der einzelnen Maschine muss über einen siche-

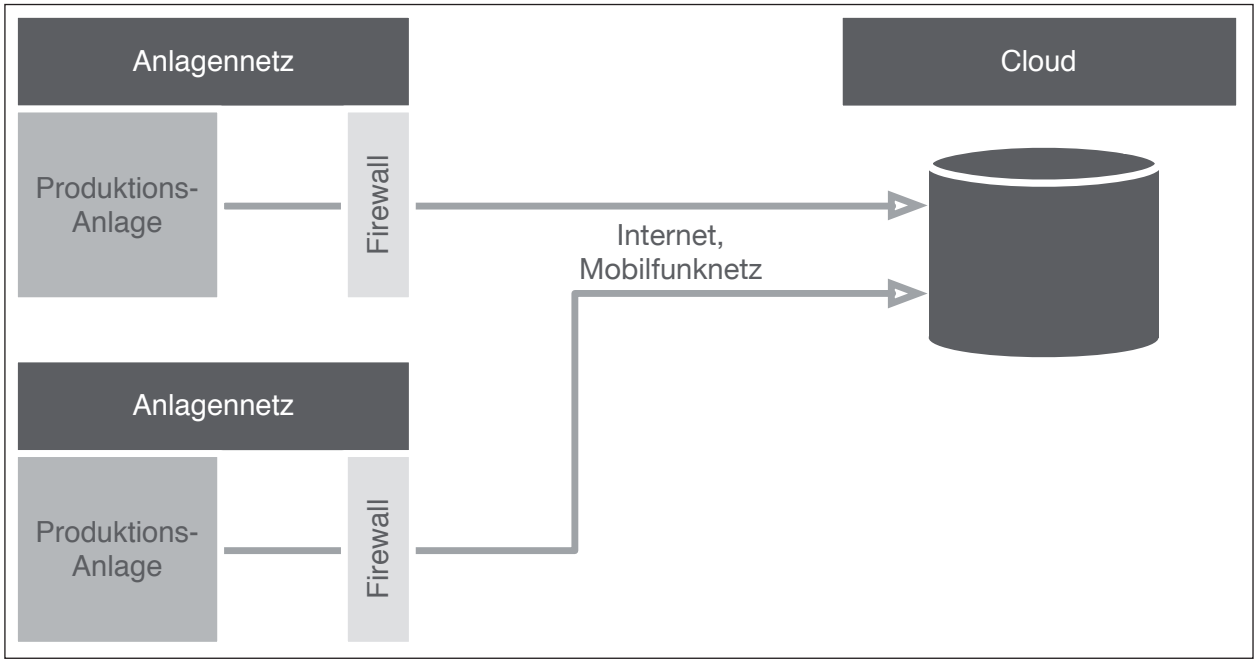

Abbildung 2: Die Cloud als zentraler Datenspeicher für Daten aus den Produktionsanlagen. Übertragung und Lagerung der Daten erfordern ein hohes Sicherheitsniveau.

ren Kanal erfolgen, die Speicherung der Daten in der Cloud muss abgesichert werden, ebenso wie die Nutzung, Verarbeitung und Weitergabe der entsprechenden Daten, wie das Schema in Abbildung 2 zeigt. Dies gilt insbesondere dann, wenn durch einen Cloud-Service die Daten mehrerer, gegebenenfalls konkurrierender Parteien verwaltet werden. Es muss somit einerseits eine sichere Mandantentrennung gewährleistet sein und ein Rollenmodell muss die Berechtigungen der einzelnen Akteure zuverlässig durchsetzen, andererseits soll eine Cloud-Infrastruktur das sichere Zusammenarbeiten der Beteiligten der Industrie 4.0-Wertschöpfungskette ermöglichen, sodass eine vollständige Isolierung der Daten und Aktivitäten der Parteien gar nicht erwünscht ist. Benötigt werden somit flexibel konfigurierbare und kontrollierbare Techniken, um die Verarbeitung und Weitergabe der Daten entsprechend der Aufgaben und Pflichten der beteiligten Parteien zu ermöglichen. Darüber hinaus muss die Verfügbarkeit gewährleistet sein, wenn der Cloud-Service wichtige Funktionen bereitstellt, ohne die eine Industrieanlage nicht weiter funktioniert. Ein wichtiges Merkmal von Cloud-Infrastrukturen ist der Zugriff auf die Cloud-Dienste über Netzwerkschnittstellen: Die Kommunikation mit der Cloud findet in der Regel über das Internet statt, Daten werden also über ein öffentlich zugängliches Netzwerk gesendet und passieren auf dem Weg vom Sender (beispielsweise einer Produktionsanlage) zum Empfänger (der Cloud) verschiedene Knotenpunkte im Netz. Diese liegen außerhalb der Kontrolle der Netzwerkadministratoren des Cloud-Providers und des Anlagenbesitzers. Zudem werden verschiedene technische Übertragungsmedien wie Kabel oder Funk- und Satellitenverbindungen genutzt. Neben den hohen Sicherheitsanforderungen an Speicherung und Verarbeitung der Daten in der Cloud stellen sich ebenso hohe Anforderungen an den Übertragungsweg zwischen Cloud und Produktionsanlage. Von besonderer Bedeutung ist dabei die korrekte, vollständige und nicht manipulierte lokale Datenerhebung in den Anlagen. Dies erfordert die Einbettung von Sicherheitsmaßnahmen direkt in die eingebetteten Komponenten der Anlage.

> Die Übertragung von Daten und Steuerbefehlen zwischen dem Cloud-Service und der einzelnen Maschine muss über einen sicheren Kanal erfolgen, die Speicherung der Daten in der Cloud muss abgesichert werden, ebenso wie die Nutzung, Verarbeitung und Weitergabe der entsprechenden Daten.

7. Zusammenfassung: Cloud gehört zur Industrie 4.0

Die Entwicklung von Industrie 4.0 und Cloud Computing gehören eng zusammen. Durch den hohen Vernetzungsgrad der Produktionsanlagen werden neue Werkzeuge benötigt, um die Maschinen zu überwachen und zu verwalten. Die Intensivierung der Zusammenarbeit verschiedener Partner, die ebenso wie die Produktionsmaschinen räumlich verteilt sind, erfordert die Nutzung sicherer Cloud-Plattformen, die eine Zusammenarbeit einfach und effektiv gestalten. Durch die steigende Komplexität von großen und verteilten Produktionsprozessen werden hohe Rechenkapazitäten benötigt, um diese Abläufe zu planen, vorab zu simulieren und in der Folge ständig zu überwachen und zu optimieren. Große Speicherkapazitäten sind erforderlich, um die Fülle der Produkt-, Produktions-, Monitoring- und Protokolldaten, die über den gesamten Lebenszyklus von Anlagen und deren Produkten anfallen, verlässlich zu speichern.

Die Funktion als zentraler Datenspeicher, in dem alle Informationen zusammenlaufen und mit ihren Schnittstellen zu Produktionsanlagen, über die Produktionsprozesse gesteuert werden können, macht die Cloud-Strukturen für Industrie 4.0 zu den kritischen Infrastrukturen. Ausschlaggebend für die Akzeptanz und die flächendeckende Nutzung von Cloud-Technologien zur Verbesserung der Geschäftsprozesse in Industrie 4.0 ist, dass die Technologie vertrauens-

würdig und sicher, aber gleichzeitig auch einfach und effizient nutzbar ist. Um dieses Ziel zu erreichen, sind noch einige Forschungs- und Entwicklungsanstrengungen erforderlich. Es gibt zwar bereits ausgereifte Ansätze für den Bereich der Business-IT, diese können aber meist nicht direkt übertragen werden, sondern müssen an die speziellen Anforderungen und Gegebenheiten der Industrie 4.0-Szenarien angepasst bzw. erweitert werden. Insbesondere die vertrauenswürdige, vertrauliche Bereitstellung von Daten in Cloud-Szenarien, in denen ein kooperatives Arbeiten von zum Teil untereinander in Konkurrenz stehenden Unternehmen unterstützt werden muss, ist derzeit noch nicht zufriedenstellend gelöst.

IT-Sicherheit im Kontext von Industrie 4.0 umfasst also sehr viele Facetten; das sichere Cloud-Computing deckt hiervon nur einen Teil ab. Zur Absicherung von eingebetteten, vernetzten Komponenten müssen neue Sicherheitstechnologien entwickelt werden, die die spezifischen Industrie 4.0-Anforderungen, wie Ressourcenbeschränktheit, Echtzeitfähigkeit und ununterbrochene Verfügbarkeit erfüllen. Neue Sicherheitskontroll- und Schutzmaßnahmen müssen bereits frühzeitig in den Entwurf der Systeme integriert werden, um zukünftige IT-basierte Produkte und Systeme robuster und resistenter gegen internetbasierte Angriffe zu gestalten. Erforderlich sind zudem neue methodische und technologische Ansätze, um die Sicherheit und Vertrauenswürdigkeit von IKT-Systemen prüfbar und kontrollierbar zu erhöhen.

LITERATUR

[1] Eckert, C.: IT - Sicherheit – Konzepte, Verfahren, Protokolle. Oldenbourg. 2013. 8. Auflage

[2] Filipovic, B., Schimmel, O.: Schutz eingebetteter Systeme vor Produktpiraterie: Technologischer Hintergrund und Vorbeugemaßnahmen. Fraunhofer AISEC Studie. 2011

[3] Tsvihun, I., Fallenbeck, N.: Journal ISIS Cloud SaaS Report, 2013.03.25. Artikel: „Cloud-Leitstand: Die Schaltzentrale für die Cloud". Volume 1. 2012

[4] Forschungsunion: Umsetzungsempfehlungen für das Industrieprojekt 4.0. April 2013

SUMMARY

IT Security for Industry 4.0
Interconnectedness, Big Data and Cloud Computing

In Industry 4.0, the boundaries between previously separate ICT sectors of production IT and business IT blur. These sectors will become cross-linked, while different IT systems with various security requirements need to be connected. This implies new vulnerabilities and opens up new possibilities for attackers to penetrate systems and cause damage in the physical world: Computer viruses, which are known from desktop PCs, spread on production plants or machines are enabled for remote maintenance, without sufficient protection of access points.

Keywords: Industry 4.0, Interconnectedness, Big Data, Cloud Computing, IT Security

SERVICE

AUTORIN

Prof. Dr. Claudia Eckert, Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC), Leiterin

Prof. Dr. Claudia Eckert ist Leiterin des Fraunhofer AISEC in München und Professorin der Technischen Universität München am Lehrstuhl für IT-Sicherheit im Informatik-Fachbereich. Als Mitglied verschiedener nationaler und internationaler industrieller Beiräte und wissenschaftlicher Gremien berät sie Unternehmen, Wirtschaftsverbände sowie die öffentliche Hand in allen Fragen der IT-Sicherheit. In Fachgremien wirkt sie an der Gestaltung der technischen und wissenschaftlichen Rahmenbedingungen in Deutschland und der EU mit.

KONTAKT

claudia.eckert@aisec.fraunhofer.de

Fraunhofer-Institut für Angewandte
und Integrierte Sicherheit (AISEC)
Parkring 4
85748 Garching
Tel.: +49 89 3229 986 292
Fax: +49 89 3229 986 299
www.aisec.fraunhofer.de