Leitfaden Industrie 4.0 Security

Handlungsempfehlungen für den Mittelstand

Auszug

in Kooperation mit

accessec
Fraunhofer AISEC
protect-ing.de
VDMA

Editorial

Wolfgang Bokämper

Verehrte Mitglieder und Leser,

die Vernetzung und Digitalisierung der Welt schreitet immer weiter voran. Dies gilt natürlich auch für alle Produktionsbereiche. Diese Herausforderung, genannt Industrie 4.0, bedarf – über die Aufgaben der eigentlich technischen Realisierung hinaus – auch der „Secure Einbettung“.

Industrie 4.0 heißt Daten und somit Informationen zu jeder Zeit an jedem Ort nutzen zu können. Aus einer solchen Verfügbarkeit werden sich viele Chancen ergeben, d. h. Informationen und deren Vernetzung werden zu einem bedeutenden Produktionsfaktor. Im Zuge eines derartigen Prozesses werden Unternehmensgrenzen fallen – fallen müssen, denn Produktentstehungsketten sind auch unternehmensübergreifend.

Macht man sich diesen Umstand bewusst, wird sehr schnell klar, dass die Aufgabe „Security“ die reine Office-Welt verlässt und neue Anforderungen stellt. Der Begriff „Verfügbarkeit“ bekommt somit eine andere Dimension. Sollte heute das E-Mail-Programm für einen halben Tag ausfallen, ist das unbequem, aber nicht lebensbedrohlich. Ein solcher Ausfall der Produktion würde aktuell ein Desaster für alle Lieferketten bedeuten. Somit ist Security eine wichtige Basis oder die „Leitplanke“ für Industrie 4.0.

Für mich ist der Trend zu mehr Shopfloor-IT schon heute klar erkennbar. Auch der Begriff „künstliche Intelligenz“ ist bis zu den Fabrikhallen vorgedrungen. Logistik, Mobilität – alles ist vernetzt und benötigt entsprechende Informationen. Eine ganzheitliche Betrachtung ist hierfür wesentlich und unabdingbar. Dabei wird natürlich klar, dass diese Aufgabe weder isoliert betrachtet noch gelöst werden kann. Alles ist Teil der Kette: angefangen bei der Komponentenherstellung über die Integration bis hin zum Betrieb der Anlagen.

Zu dieser Kette, die oft vorrangig technisch betrachtet wird, gehören aber selbstverständlich auch die Menschen. Sie heißen Entwickler, Automatisierer, Betreiber, Anwender usw. Die wichtige Aufgabe des Managements besteht darin, die Security Awareness bei den Mitarbeitern als Teil des täglichen Arbeitslebens zu integrieren.

Gehen wir also Industrie 4.0 „secure“ an und der Erfolg wird uns recht geben.

Wolfgang Bokämper

Vorsitzender des VDMA-Arbeitskreises Industrial Security,
Bereichsleiter Beschaffung, Organisation & Qualitätssicherung,
Kolbus GmbH & Co. KG, Rahden

Inhaltsverzeichnis

Management Summary

Der zuverlässige und dauerhaft sichere Betrieb von weltweit vernetzten Maschinen und Anlagen ist eine elementare Herausforderung für eine erfolgreiche Umsetzung von Industrie 4.0. Der dafür geläufige deutsche Begriff „Sicherheit“ ist irreführend, da er im Maschinen- und Anlagenbau vornehmlich im Sinne der „Safety“, also der Funktionalen Sicherheit, etabliert ist. Demgegenüber steht in diesem Leitfaden der aus dem Englischen stammende Begriff der “Security“ im Fokus. Die Security beschreibt grundsätzlich die Absicherung von IT-Systemen. Um eine klare Abgrenzung zur Absicherung der Büroinformationstechnik („IT-Security“) zu erhalten, sprechen wir bei der Absicherung von Informationstechnik in industriellen Anlagen, Maschinen und Systemen von „Industrial Security“. Werden diese Systeme nun durch die Integration von Industrie 4.0 vernetzt, so müssen sich sowohl Hersteller als auch Betreiber Gedanken darüber machen, wie sie diese unternehmensübergreifende Vernetzung dauerhaft sicher (im Sinne von „secure“) gewährleisten können. Das ist der Kern von „Industrie 4.0 Security“. Nur mit der zuverlässigen Absicherung moderner Produktions- und Prozesssysteme wird die Transformation der Industrie ermöglicht.

Ziel der „Industrie 4.0 Security“ ist es, die Security von zukünftigen Maschinen und Anlagen über den gesamten Lebenszyklus gewährleisten zu können, statt wie aktuell ein nachgeschaltetes Hinzufügen („Anflanschen“) einer Security-Funktionalität notwendig zu machen. Security muss zukünftig als integraler Aspekt bereits von Beginn an in den gesamten Produktentwicklungsprozess seitens der Maschinen- und Anlagenbauer mit einfließen („Security by Design“). Die Integration der Security erfordert es, diese schlussendlich als funktionalen Bestandteil von zukünftigen Anlagen und Systemen zu betrachten, und somit die „Security as a Function“ zu etablieren.

Dieser Leitfaden dient Maschinen- und Anlagenbauern als Einstieg und Orientierungshilfe, welche Themenbereiche, Technologien und Prozesse für eine Erhöhung der Security komplexer Anlagen berücksichtigt werden sollten. Der Fokus liegt auf der Sicht der Hersteller und Integratoren, zusätzlich werden Anforderungen an notwendige Eigenschaften oder Funktionen gestellt, die zukünftig durch Lieferanten bereitgestellt werden müssen. Die branchenspezifische Fokussierung auf den Blickwinkel des Maschinen- und Anlagenbaus ermöglicht eine angemessene Abdeckung des Anforderungsspektrums und bietet den notwendigen Tiefgang, um konkrete Handlungsoptionen aufzeigen zu können.

Um die Ziele für die Bereitstellung nachhaltig und dauerhaft sicherer Anlagen für Industrie 4.0 zu erreichen, beschreibt der Leitfaden die Berücksichtigung der Security als gleichrangiges Ziel bereits im Entwicklungs- und Konstruktionsprozess. Weiterführend umfassen die Anforderungen an „Industrie 4.0 Security“ eine Betrachtung von Gefährdungen und Risiken vor Inbetriebnahme, ein Management von Cyberrisiken während des Betriebs und eine Aufrechterhaltung der Securityfunktion im gesamten Produktlebenszyklus von vernetzten Maschinen und Anlagen. Die Risikobetrachtung bereitet Hersteller und Integratoren auf aktuelle und zukünftig zu erwartende Bedrohungslagen vor. Mit der Inbetriebnahme kann dem Betreiber gegenüber zudem ein Mindestmaß an Security gewährleistet werden. Während des Produktlebenszyklus ist die Etablierung eines Prozesses zur Annahme, Beurteilung und Reaktion auf relevante Securitybedrohungen notwendig.

Erste Hilfe zur Unterstützung bietet der Leitfaden mit dem Industrie 4.0 Werkzeugkasten des VDMA, unterstützt durch eine Online-Selbsteinschätzung.

Bestellung

Print-Ausgabe

VDMA-Mitglieder können die deutsche Printausgabe der Publikation „Leitfaden Industrie 4.0 Security – Handlungsempfehlungen für den Mittelstand“ kostenlos bei Biljana Gabric, **biljana.gabric@vdma.org**, unter Angabe ihrer Kontaktdaten bestellen.

Nicht-Mitglieder zahlen eine Schutzgebühr von 120,- Euro inkl. MwSt. zzgl. Versandkosten.Bitte bestellen Sie Ihre Printausgabe direkt beim **VDMA Verlag** http://leitfaden-i40-security.vdma-verlag.de/

VDMA
Produkt- und Know-how-Schutz
Lyoner Str. 18
60528 Frankfurt am Main
Telefon +49 69 6603-1978
Fax +49 69 6603-2978
E-Mail protect-ing@vdma.org
Internet pks.vdma.org

Fraunhofer Institut für Angewandte und Integrierte Sicherheit (AISEC)
Parkring 4
85748 Garching bei München
Internet: www.aisec.fraunhofer.de

accessec GmbH
Marktstr. 47–49
64401 Groß-Bieberau

pks.vdma.org
www.i40-security.de

VDMA Verlag
ISBN 978-3-8163-0689-4