KurzPosition
für Politik und Wirtschaft

VDMA

06/2015

Hauptstadtbüro

Industrial Security: Sichere Maschinen und Anlagen

Steht die Produktion, geht bares Geld verloren. Fallen kritische IT-Infrastrukturen wie in Krankhäusern oder bei Energieversorgern aus, stehen Menschenleben auf dem Spiel. Informationstechnik in Produktionssystemen sowie Maschinen und Anlagen vor Sabotage, Spionage oder Manipulation zu schützen, ist Aufgabe der „Industrial Security“. Das Thema bekommt zu Recht immer mehr Aufmerksamkeit, denn mit Industrie 4.0 erhält Industrial Security noch größere Brisanz für den Industriestandort Deutschland.

Kleine Lücke mit fataler Auswirkung

Maschinen werden zunehmend vernetzt, Anlagen aus der Ferne überwacht. Die Herausforderungen für den Schutz kritischer Infrastrukturen steigen, die Angriffe auf die Systeme nehmen zu. Die Angreifer agieren je nach Angriffsziel und Absicht als Wettbewerber, Mitarbeiter, fremde Staaten, organisierte Kriminalität oder Aktivisten. Sie haben den Vorteil, mit nur einer Lücke das komplette Schutzsystem auszuhebeln. In der Fabrik der Zukunft mit Industrie 4.0 bieten immer mehr Schnittstellen viel Angriffsfläche. Der Bedarf an Sicherheitsvorkehrungen steigt also weiter.

Standards brauchen Abstimmung

Bedrohungssituationen und abgeleitete Mindestanforderungen für Security-Maßnahmen sind in der Praxis nur nach spezifischen, branchenabhängigen Kriterien bestimmbar. Das IT-Sicherheitsgesetz ermöglicht genau diese branchenspezifische Erarbeitung von Security-Standards. Elementar ist, sowohl Betreiber als auch Integratoren und Komponentenhersteller zusammen zu bringen, um einen praxistauglichen Anforderungskatalog zu entwickeln. Dafür bedarf es frühzeitig einer intensiven Abstimmung zwischen der politischen Ebene, den Behörden, Unternehmen und Verbänden.

Betreiber verantworten Security

Anlagen sind oft mehr als zehn Jahre im Dauerbetrieb. In dieser Zeit können Betriebssysteme, technische Komponenten und komplette Technologien veralten. Ein einzelner Hersteller ist im Anlagenverbund jedoch nicht in der Lage, von Außen die Sicherheit stellvertretend für den Anlagenbetreiber zu gewährleisten. Die Hersteller zentraler Anlagenteile stellen die notwendigen Sicherheitsmaßnahmen und -mittel zur Verfügung. Diese Maßnahmen müssen im Rahmen eines Gesamtkonzeptes vom Betreiber auf die Gesamtanlage abgebildet werden.

KurzZahl

Wussten Sie, dass im Jahr 2013 bereits 29 Prozent der vom VDMA befragten Maschinen- und Anlagenbauer Produktionsstörungen durch Security-Vorkommnisse hatten?

Weltweite Harmonisierung anstreben

Ein nationaler Alleingang bei Industrial Security greift zu kurz. Versorgungsstrukturen liegen wie ein Netz über ganz Europa. Maschinen und Anlagen werden weltweit verkauft. Weder der Aktionsradius von global agierenden Unternehmen noch die Cyber-Angriffe machen an den Landesgrenzen halt. Daher muss die Bundesregierung sich mindestens auf europäischer Ebene für abgestimmte Sicherheitsmechanismen einsetzen. Gerade kleine und mittelständische Unternehmen haben sonst Schwierigkeiten, Standards zu erfüllen und Handel zu betreiben. Nur ein harmonisiertes Vorgehen auf internationaler Ebene kann tatsächlich zu mehr Sicherheit führen. Ein weltweit koordiniertes Vorgehen wie durch den Abschluss völkerrechtlicher Verträge und das Setzen von internationalen Mindeststandards sind zielführend.

Industrie 4.0 nur mit Security

Ohne den Schutz von Daten und Know-how unternehmensübergreifender Produktionsprozesse ist Industrie 4.0 undenkbar. Daher gilt: Der automatisierte Datenaustausch vernetzter Produktionssysteme muss sicher und zuverlässig gestaltet sein, die eindeutige Identifizierung der Prozessakteure kontrolliert und das Know-how von Produkten, Verfahren, Maschinen und Anlagen geschützt werden. Dazu müssen internationale Handelshemmnisse wie für Kryptographieprodukte abgebaut und sichere Mikrosystemarchitekturen von „Security Made in Germany“ aufgebaut werden.

Fazit

Die Daseinsvorsorge und die Industrieproduktion sind Grundsteine für Fortschritt und Wohlstand in Deutschland und Europa. Der deutsche Maschinen- und Anlagenbau ist zentraler Ausrüster aller Versorgungssysteme. Er begrüßt daher ausdrücklich das Vorhaben zu einem IT-Sicherheitsgesetz. Der Gesetzentwurf muss aber unter Beteiligung der Hersteller und Betreiber dieser Versorgungselemente konstruktiv gestaltet und mit europäischen Initiativen harmonisiert werden.

Kontakt

Steffen Zimmermann, VDMA Informatik
Telefon +49 69 6603-1978, E-Mail steffen.zimmermann@vdma.org

Andreas Rade, Geschäftsführer VDMA Hauptstadtbüro
Telefon +49 30 306946-16, E-Mail andreas.rade@vdma.org

www.vdma.org

Mehr KurzPositionen

vdma.org/kurzpositionen

Verantwortlich: Andreas Rade • Geschäftsführer VDMA Hauptstadtbüro
Redaktion: Stefanie Seele • VDMA Hauptstadtbüro
Friedrichstraße 95 • 10117 Berlin • Telefon +49 30 306946-0 • Fax +49 30 306946-20 • E-Mail berlin@vdma.org