Artikel aus dem Frankfurter Allgemeine Zeitung Verlagsspezial *IT-Sicherheit* vom 6. Oktober 2015

# Sicherheit 4.0

Die digitale Transformation soll mit Industrie 4.0 und der Automatisierung von Fertigungsabläufen richtig in Fahrt kommen. Doch noch bleibt „das Internet der Dinge" im Back-End vieler Unternehmen stecken – weil es an den Sicherheitsarchitekturen fehlt. *Von Michael Dörfler*

Das Ziel haben viele Unternehmen vor Augen: durchgehende, automatisierte Fertigungsketten, die angriffssicher betrieben werden können. Martin Jansen, Senior Consultant bei der Geschäfts- und Organisationsberatung Bridging IT, skizziert, was dafür alles umgesetzt werden müsste: „Das Unternehmen als Organisation müsste einschließlich seiner Geschäftspartner zunächst alle potentiellen Bedrohungen konzeptionell durchdringen. Danach heißt es, alle beteiligten Komponenten vor diesen Bedrohungen zu schützen, die dazu notwendigen Sicherheitsfunktionen ab Werk als Automatismen innerhalb dieser Komponenten zu implementieren und immer intelligentere Angriffsformen aus dem Cyberspace abzuwehren." Für das nahtlose Zusammenspiel von IT-, Fertigungs-, Steuerungs- und Sicherheitssystemen müssten außerdem verbindliche Standards entwickelt und anschließend sowohl von den IT- als auch den Herstellern aus dem Maschinenbau befolgt werden. „Bis dahin", räumt der Senior-Berater ein, „wird es noch viele Jahre dauern." Frühzeitig beschäftigen sollten sich die Fertigungsbetriebe nach Jansen dennoch mit Industrie 4.0, „schon um ihre digitalen Geschäfte sukzessiv ausbauen zu können".

### Teilbereiche der Fertigung besser schützen

„Was beim jetzigen Stand der Technik für die Betriebe zählt, ist die Umsetzung des technisch Machbaren und organisatorisch Vertretbaren", bestätigt Mathias Hein, freier IT-Berater in Neuburg an der Donau. Im Handlungsfokus stünden vorerst Teilbereiche der Fertigung, die weitgehend vom Internet abgeschottet sind und deshalb mit den verfügbaren Sicherheitsmitteln geschützt werden könnten. Solche Teilnetze mit Blick auf die digitalen Geschäfte über das Internetprotokoll (IP) zu öffnen, bezeichnet Hein aktuell für Fertigungsbetriebe als „viel zu gefährlich". Auch die diversen Gremien für Industrie 4.0, die es inzwischen in Deutschland gebe, konzentrierten sich vorerst auf Teilnetze, um über verbindliche Standards die Daten, Systeme und Komponenten darin künftig noch besser abzuschirmen, beobachtet er. Schon dafür müssten innerhalb dieser Gremien die IT-Wirtschaft und der Maschinenbau eng zusammenarbeiten, was schwierig genug sei.

Carsten Rossbach, Partner im Competence Center Engineered Products & High Tech bei Roland Berger, sieht Gremien, Verbände, Initiativen und etablierte Anbieter dennoch auf einem guten Weg. „Sie forcieren ihre Aktivitäten im Rahmen des Standardisierungswettlaufs." So konzipiere die deutsche Plattform Industrie 4.0 eine Referenzarchitektur. Parallel arbeite die Arbeitsgruppe „Sicherheit in vernetzten Systemen" innerhalb dieser Plattform daran, dass Aktionen wie Verbinden, Prozessieren und Speichern innerhalb von Clouds künftig besser geschützt werden können. Auch das Industrial Internet Consortium habe im Mai dieses Jahres erste Eckpunkte für eine sicherere Referenzarchitektur vorgestellt. Für Rossbach steht deshalb fest: „Offene Standards werden sich in der Produktions-IT letztlich durchsetzen."

Ob herkömmliche, herstellergetriebene Standardisierungsbemühungen ausreichen werden, um die notwendige Sicherheit herzustellen, ist jedoch fraglich. Denn dazu wäre ein Paradigmenwechsel bei der Produktentwicklung notwendig. Norbert Pohlmann, Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit an der Westfälischen Hochschule in Gelsenkirchen, außerdem Vorstandsvorsitzender des Bundesverbands für IT-Sicherheit – Tele Trust, formuliert das so: „Wir hätten im Bereich Industrie 4.0 die einmalige Chance, von Anfang an die Aspekte IT-Security und Datenschutz richtig zu berücksichtigen und robuste IT-Systeme zu entwickeln – und dadurch eine volle digitale Souveränität zu erreichen." Bis jetzt hätten die Hersteller aber immer im Nachhinein versucht, diese Aspekte einigermaßen zu berücksichtigen. Dadurch sei unterm Strich die hohe Angreifbarkeit der heutigen IT-Systeme und somit auch von Fertigungsabläufen entstanden.

**Die Top 10 Sicherheitsbedrohungen für Industrie 4.0 nach dem Bundesamt für Sicherheit in der Informationstechnik**

- Infektion mit Schadsoftware über Internet und Intranet
- Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
- Social Engineering
- menschliches Fehlverhalten und Sabotage
- Einbruch über Fernwartungssysteme
- Internetverbundene Steuerungskomponenten
- technisches Fehlverhalten und höhere Gewalt
- Kompromittierung von Smartphones im Produktionsumfeld
- Kompromittierung von Extranet und Cloud-Komponenten
- (Distributed) Denial-of-Service-Angriffe

STAND 2014

### Frühwarnsystem kann helfen

Jörg Fritsch, Research Director bei Gartner, hat klare Vorstellungen, wie IT-Sicherheit im Industrie-4.0-Umfeld künftig beschaffen sein sollte: „Was wir brauchen, ist eine adaptive Sicherheit, die auf Basis von Mikro-Perimetern funktioniert, damit die Sicherheitsfunktionen immer wieder neuen Bedrohungsszenarien angepasst werden können." Diese Sicherheitsfunktionen müssten auf allen Sensoren, vernetzten Systemen, Produktionsmitteln und zentralen Steuerungselementen zur Verfügung stehen. Oder anders ausgedrückt: „IT Security muss ab Werk zu einem Bestandteil jeder einzelnen Komponente entlang der Fertigungs- und Lieferkette werden." Das, so der Gartner-Analyst weiter, ziehe grundlegende Veränderungen sowohl hinsichtlich der Sicherheitsüberlegungen als auch der Sicherheitsarchitektur nach sich.

Bis es so weit ist, behelfen sich Fertigungsunternehmen in Teilnetzen mit den Sicherheitsmitteln, die ihnen der Markt zur Verfügung stellt. Auch die haben sich weiterentwickelt. Harald Reisinger, Geschäftsführer des Security Management-Dienstleisters Radar Services, setzt auf verhaltensbasierende Analysen und erweiterte Korrelationsalgorithmen, um abnorme und sicherheitskritische Vorfälle innerhalb von Produktionssystemen frühzeitig zu erkennen. „Aufgedeckt werden solche Vorfälle durch Analyse von Netzwerkdaten, Protokollbefehlen und Log-Auswertungen", erklärt Reisinger. Dadurch könnten Fertigungsunternehmen die Abläufe in ihren Teilnetzen vor vielfältigen Angriffsformen aus dem Cyberspace, aber auch von innen schützen. Radar Services offeriert, wie andere Anbieter auch, dieses Frühwarnsystem als Managed Security Services. Fertigungsbetriebe müssen dadurch nicht selbst diese Sicherheitssysteme vorhalten und betreiben.