Computerpartner

03.01.2016

Im Web lauern die Feinde

Die Industrie geht zunehmend mit ihren Geschäfte ins Internet. Dazu werden Fertigungsprozesse in Teilen ins Internet verlagert, um auf diese Weise kostengünstiger und näher am Kunden zu produzieren. Diese Öffnung über das Modell Industrie 4.0 hat für die Unternehmen, neben der Hoffnung auf künftig noch bessere Geschäfte, auch eine Kehrseite: Die Unternehmen gefährden über die Maschine-zu-Maschine (M2M)-Kommunikation in hohem Maße ihre Fertigungsprozesse, damit ihre geschäftliche Existenz; von Hadi Stiel *)

Hadi Stiel

Unvorbereitet in die Industrie 4.0-Ära: "Was die allgemeine Kommunikation im Internet fördert, der Einsatz von Standardprotokollen, macht Fertigungsprozesse und die daran beteiligten Daten extrem angreifbar", weiß Mathias Hein, freier IT-Berater in Neuburg an der Donau. Er ist derzeit mit mehreren Sicherheitsprojekten im industriellen Umfeld betraut. "Allgemein verbindliche Web-Standards wie TCP/IP (Transmission Control Protocol/Internet Protocol), HTTP (Hyper Text Transfer Protocol) und SOAP (Simple Object Access Protocol) laden Hacker und Industriespione förmlich dazu ein, bis in die Betriebssoftware der Maschinen und beteiligten Systeme vorzudringen." Die Gefahr für Fertigungsunternehmen, die sich unvorbereitet zu weit ins Internet vorwagen, sei schon deshalb groß, weil im schlimmsten Fall durch Datensabotage Produktionsausfälle drohten. "In diesem Fall", warnt der IT-Berater, "ist schnell das Kerngeschäft, damit die Existenz des Unternehmens betroffen."

Hein wundert sich ob der Naivität vieler Fertigungsunternehmen, mit der sie sich, ungeachtet der Warnungen aus ihrer IT-Abteilung, ins Abenteuer "IP-geprägte Industrie 4.0" stürzen. Nach seiner Einschätzung gehören Automatisierungs-, Steuerungssysteme und andere Fertigungskomponenten nicht ins öffentliche Internet der Dinge. Dort formieren sie sich dennoch mit Servern, Endgeräten und Netzkomponenten zu M2M-Prozessketten. Jedes Element, sofern es Web-Standards gehorcht, und das ist der ausgemachte Trend, ist angreifbar. Bernhard Stütz, Professor für Computerkommunikationstechnik/Computernetze am Fachbereich Elektrotechnik und Informatik an der Fachhochschule Stralsund, gibt einen Vorgeschmack davon, was Fertigungsbetriebe im Internet erwartet: "Denial-of-Service-Attacken, Trojaner, Attacken über Funk mittels handelsüblicher IOT (Internet-of-Things)-Geräte, Spionageprogramme, die über Software-Patches und -Upgrades eingeschleust werden oder bereits zuvor in der ausgelieferten US-Software eingebaut wurden, bis hin zu APTs (Advanced Persistent Threats). Sie sind als ursprüngliche Entwicklung des US-Militärs per Mustererkennung nicht mehr auszumachen." APTs passieren damit problemlos etablierte Sicherheitstechniken wie Firewalls, Viren-Scanner und IDS (Intrusion Detection Systeme).

Gefahr droht auch, wenn die Verschlüsselungssysteme zur Chiffrierung der Fertigungs- und Prozessdaten aus den USA stammen. Dann könnte der Feind, die NSA, on the fly mitlesen. Steffen Zimmermann, bei der VDMA-Arbeitsgemeinschaft verantwortlich für Produkt- und Know-how-Schutz, rüttelt auf: "Schon 2013 meldeten 29 Prozent der Maschinenbauer Produktionsausfälle durch Sicherheitslücken." Die tatsächliche Prozentzahl dürfte, weil die meisten Fertigungsunternehmen in Zeiten des Internet Imageverluste mehr denn je fürchten, weit höher liegen. Der Produkt- und Know-how-Schützer macht weitere wunde Punkte von M2M-Prozessen aus: "Sobald im Rahmen der Industrie 4.0-Kommunikation getrennte Firmennetze zusammengeschaltet werden, müssten eigentlich schärfere Zugangskontrollen und Eigenschutzmechanismen installiert werden." Er fordert außerdem eine eindeutige Identifikation sämtlicher Netzbeteiligten und eine wechselseitige starke Authentisierung.

Die Gefahr, Opfer von Hackern, Industriespionen und anderen Cyber-Kriminellen zu werden, ist schon deshalb groß, weil es dem Modell für Industrie 4.0, das sich an der SOA (Service-Orientierten-Architektur) anlehnt, an geeigneten Sicherheitsmechanismen fehlt. Die OPC (Object Linking and Embedding for Process Control) Foundation hat mit ihren UA (Unified Architecture)-

Definitionen Sicherheit bisher kaum thematisiert. "Schutzvorrichtungen wie die Abtrennung der Netze durch Firewalls und Virtual Private Networks (VPNs) sowie Gebäudezutrittskontrolle seien bei weitem zu wenig", moniert Oliver Winzenried, Vorstand und Gründer von Wibu-Systems. Außerdem müssten die für Industrie 4.0 und Big Data erforderlichen Datenmodelle erst noch erforscht werden. "So müssen für Industrie 4.0 alle vernetzten Komponenten, vom Durchflussmesser über das Stellventil bis hin zum Bedien-Panel, eine eigene Identität erhalten."

Erwin Schöndlinger, Geschäftsführer von Evidian Deutschland, stellt deshalb Identity and Access Management als ein für Industrie 4.0 essenzielles Sicherheitswerkzeugset heraus. "Starke Authentisierung, Single-Sign-on (SSO)-gesteuerte Zugriffe, automatisiertes Berechtigungsmanagement, Provisionierung von Konten sowie flankierendes Auditing & Reporting für Compliance sind dafür unverzichtbar." Außerdem müsse es möglich sein, aus der Sicherheitsstrategie und den Business-Regeln direkt die Rollen mit den individuellen Zugriffsrechten abzuleiten und diese Rechte automatisch in die involvierten Konten einzutragen. "Denn nur so können sicherheitsstrategische oder organisatorische Veränderungen durch eine schnelle und gezielte Anpassung der Zugriffsrechte vollzogen werden." Allerdings räumt Schöndlinger auch ein: "Für abgesicherte M2M-Prozesse müssten die Maschinen wie die Menschen eine eindeutige Identität erhalten und die Sicherheitsmechanismen direkt innerhalb der Automatisierungs- und Fertigungssysteme angesiedelt sein." Denn nur unter diesen Voraussetzungen könnten sich die Maschinen künftig selbständig und gegenseitig authentisieren und autorisieren. In gleicher Weise, so Schöndlinger, müssten Maschinen autark Verschlüsselungs- und Entschlüsselungsmechanismen anstoßen können.

Bis dahin ist es aber noch ein weiter Weg. "Sicherheit müsste, anders als heute, zu einem integrativen Bestandteil von Maschinen und Systemen werden, also schon bei ihrem Design und Engineering, vorausbedacht, eingesetzt und ausgetestet werden", so Zimmermann von der VDMA-Arbeitsgemeinschaft. Ob die meist proprietär ausgerichteten Hersteller diesen Paradigmenwechsel innerhalb der nächsten fünf Jahre vollziehen werden, ist mehr als fraglich. Voraussichtlich wird das Internet für Industrie 4.0 noch auf viele Jahre hinaus ein höchst unsicheres Terrain sein.

***) Autor Hadi Stiel ist freier Journalist und Kommunikationsberater in Bad Camberg**