3/18

www.digital-manufacturing-magazin.de

D, A, CH: 9,50 Euro, weitere EU-Länder: 11,70 Euro

DIGITAL MANUFACTURING

AUFBAU UND OPTIMIERUNG IT-GESTÜTZTER PRODUKTIONSPROZESSE

Industrie 4.0 | Internet der Dinge

MIT SPECIAL ROBOTIK

Umfassendes Security-Konzept für industrielle Anlagen

Cyber-Sicherheit wird zum geschäftsentscheidenden Kriterium

Vertrauen ins **Digitale** schaffen

Die digitale Revolution erfasst die industrielle Fertigung und Automatisierung in voller Breite. Sie stellt gleichsam einen Paradigmenwechsel dar, der Neubewertungen erfordert. Auch in Sachen Cybersecurity. In Zeiten des „Internet of Things" (IoT), Cloud-Anwendungen, und der totalen Vernetzung werden der Schutz industrieller Anlagen und deren Daten wichtiger denn je.

VON FRANZ KÖBINGER

SCHON LÄNGST sind nicht nur übliche PCs oder Büronetzwerke das Ziel von Angriffen. Spätestens das Schadprogramm Stuxnet, das 2010 weltweit für Schlagzeilen sorgte, führte der Industrie vor Augen, dass sich die Grenzen zwischen der Bürowelt und den Infrastrukturen zur Steuerung industrieller Anlagen mit der fortschreitenden Digitalisierung auflösen. Der Verschlüsselungs-Trojaner „WannaCry" machte dies zuletzt im Mai 2017 wieder einmal deutlich. Auch hier waren viele Fertigungsstandorte direkt betroffen – und die Gefahr durch Cybersicherheits-Risiken wird in Zukunft weiter zunehmen. Produkte, Lösungen und Services enthalten immer mehr Software, die vielfach auch in kritischen Infrastrukturen verwendet wird.

Bereits heute kommunizieren mehr als 8 Milliarden Geräte miteinander. Mehr als

20

Milliarden im Jahr 2020

Das Resultat: Schon heute kommunizieren mehr als acht Milliarden Geräte wie Maschinen, Anlagen, Sensoren und Produkte miteinander – rund 30 Prozent mehr noch als 2016. Diese Anzahl wird sich bis 2020 weiter spürbar erhöhen – bis auf mehr als 20 Milliarden. Und ein Ende ist nicht in Sicht.

Die Bedrohungen und auch die Anzahl der Vorfälle haben in den letzten Jahren stetig zugenommen. Das ist darauf zurückzuführen, dass es durch die wachsenden Datenmengen und die zunehmende Vernetzung für Hacker immer lukrativer und einfacher wird, an vertrauliche Daten zu kommen, oder einfach mittels Fernzugriff in Anlagen oder Maschinen unbefugt einzudringen und sie gegebenenfalls zu sabotieren. Cyberattacken können dabei massive Schäden anrichten, insbesondere, wenn sie sich gegen industrielle Anlagen oder kritische Infrastrukturen richten.

Mit der zunehmenden Digitalisierung beschleunigt sich dieser Trend noch – es ist gleichsam die Schattenseite der digitalen Welt. Allerdings ist Fortschrittsverweigerung auch keine Lösung; zu groß sind die Vorteile, die Flexibilität und die neuen Möglichkeiten, die eine „digitale

< Damit die digitalisierte Fabrik Realität werden kann, benötigt sie ein ausgefeiltes Security-Konzept, bei dem jede Komponente mitspielen muss.
Bilder: Siemens

Wie eine Zwiebel: Mittels Defense in Depth nutzt es dem Angreifer wenig, eines der Sicherheitssysteme zu überwinden. Mehrere Schichten gleichen ihre Schwachstellen gegenseitig aus.

Fabrik" mit sich bringt. Wer konkurrenzfähig bleiben will, muss „digital" werden.

Schutzmaßnahmen umsetzen

Jedoch gilt es, das Risiko zumindest soweit zu mindern, dass es in einem akzeptablen Rahmen bleibt, sodass erfolgreiche Angriffe sehr unwahrscheinlich werden – wohl wissend, dass absolute Sicherheit nicht wirklich erreichbar ist. Ob Risiken akzeptabel sind, legt eine Bedrohungs- und Risikoanalyse in strukturierter Form offen. Zunächst werden dabei alle erkennbaren Risiken daraufhin überprüft, wie hoch deren Schadenspotenzial und Eintrittswahrscheinlichkeit sind. Letztere hängt davon ab, wie einfach es Angreifer haben, und wie hoch deren Motivation ist, genau hier anzugreifen. Ist beides hoch, müssen auf jeden Fall zusätzliche Schutzmaßnahmen zur Eingrenzung der Wahrscheinlichkeit und des Schadensumfangs ergriffen werden.

Das hört sich einfach an, ist in der Praxis jedoch oft komplex, da gleichzeitig der Herstellungsprozess nicht wesentlich gestört werden soll. Echtzeitfähigkeit, Performance und Handhabung dürfen nicht leiden. Diese Aspekte sind jedoch meist Gegenspieler der Security-Anforderungen. Ständige Passwort-Eingaben beispielsweise werden dem berechtigten Nutzer schnell lästig, machen es potenziellen Angreifern jedoch viel schwerer einzudringen. Es gilt, den richtigen Kompromiss zu finden.

Schutzmaßnahmen, die mehr schaden als nützen, sind nicht zielführend, aber ständige Sicherheitsvorfälle und Störungen durch unzureichende Maßnahmen auch nicht. Hier kann die erwähnte Risikoanalyse Klarheit schaffen, was muss sein und was ist zu viel des Guten? Solch ein Vorgehen ist schon aus Kostengründen sinnvoll.

Die Sicherheit in der Tiefe

Glücklicherweise gibt es eine Reihe von „Best Practises", die angewandt werden können. Diese können zum Beispiel im führenden internationalen Standard für industrielle Cybersecurity, der IEC 62443 nachgelesen werden. Zwar ist jede Anlage anders und hat ihre individuellen Schutzziele, jedoch sind die möglichen Maßnahmen überschaubar. Wichtig ist aber, ob die eingesetzten Geräte und Automatisierungssysteme die erforderlichen Eigenschaften und Funktionen mitbringen, um die Anforderungen umsetzen zu können.

Im Jahr 2016 verursachten Angriffe aus dem Internet weltweit Schäden von mehr als 500 Milliarden Euro. Bis zu

1,6%

des BIP in einigen EU-Ländern

Hier kommen deren Hersteller ins Spiel. Man kann natürlich auch unsichere Geräte durch externe Maßnahmen schützen, das bedeutet aber Mehraufwand. Wenn hingegen beim Design der Geräte die nötigen Security-Aspekte bereits berücksichtigt werden (Stichwort: „Security by Design"), vermindert das die Risiken von vornherein erheblich. Auch macht es Security by Design Anwendern einfacher, umfassende mehrschichtige Schutzkonzepte („Defense in Depth") zu implementieren.

Umfassendes Security-Konzept

Defense-in-Depth-Konzepte erhöhen nicht nur die Sicherheit allgemein, sie sind im Endeffekt auch der einzig wirkliche Schutz gegen Sicherheitslücken. Diese wird man erfahrungsgemäß nie ganz ausschließen können, und bis Security-Patches verfügbar und eingespielt sind, dauert es seine Zeit. Die Kombination von Netzwerk-, System-, Endgeräte- und Software-Sicherheit jedoch gleicht einzelne Schwachstellen aus und verhindert unbefugte Zugriffe auf „geschwächte" Geräte. Damit Anlagenbetreiber dieses Konzept bestmöglich umsetzen können, unterstützt Siemens mit einem umfangreichen und in sich abgestimmten Portfolio an Security-Produkten und -Services.

Prozessverbesserungen zur Erhöhung der Produktsicherheit tun ein Übriges, um die Risiken einzugrenzen und Verlässlichkeit und Vertrauen in digitale und vernetzte Anwendungen zu schaffen. Zum Schutz der Produktion wird das Siemens Industrial Holistic Security Concept (HSC) angewandt, das Entwicklungsabteilungen und Produktionsanlagen sichert. Zudem werden die eigenen Produkte gründlichen Tests unterzogen und optimiert. Somit erfolgt eine Systemhärtung bereits mit der Auslieferung der Produkte. jbi

Franz Köbinger ist Marketing Manager Industrial Security der Division Digital Factory der Siemens AG.

The Charter of Trust

Digitalisierung und Cybersecurity bedingen einander und müssen sich zusammen weiterentwickeln. Gemeinsam mit weiteren IoT-Marktführern hat Siemens deshalb im Rahmen der Münchner Sicherheitskonferenz im Februar 2018 die globale Initiative „Charter of Trust" ins Leben gerufen. Sie fordert verbindliche Regeln und Standards auf dem Gebiet der Cybersicherheit. Zukunftsprodukte aller Partnerunternehmen sollen nach ambitionierten Cybersecurity-Prinzipien designt und umgesetzt werden. In diesem Dokument skizzieren die Unterzeichner die Schlüsselprinzipien, die erforderlich sind, neues Vertrauen zwischen Gesellschaft, Politik, Geschäftspartnern und Kunden aufzubauen und die digitale Welt insgesamt sicherer zu machen – der Kreis der Unterzeichner wächst.