Zeitschrift: Bulletin Electrosuisse
Herausgeber: Electrosuisse, Verband für Elektro-, Energie- und Informationstechnik
Band: 105 (2014)
Heft: 7

Artikel: Digitale Einbrecher
Autor: Strehlitz, Markus
DOI: https://doi.org/10.5169/seals-856262

TECHNOLOGIE **INDUSTRIE 4.0**

Digitale Einbrecher

Online-Angriffe auf vernetzte Produktionsstätten

Die Vernetzung von Produktionsanlagen bringt nicht nur Chancen mit sich, sondern auch ein erhöhtes Sicherheitsrisiko. Um die vernetzte Produktionsinfrastruktur gegen unerwünschten Zugriff zu schützen, werden Methoden der IT-Welt eingesetzt. Die eingesetzten Verfahren können aber ihrerseits im Produktionskontext zahlreiche Herausforderungen schaffen.

Markus Strehlitz

Flexiblere Fertigung, schnellere Prozesse, individuelle Produkte zu gleich bleibenden Preisen – die Zukunftsvision Industrie 4.0 bietet in der Vorstellung vieler Wissenschaftler und IT-Experten eine Fülle an Vorteilen für die Wirtschaft. Diese neuen Möglichkeiten ergeben sich unter anderem daraus, dass Maschinen untereinander und mit den IT-Systemen im Unternehmen kommunizieren. Doch mit den neuen Chancen entstehen auch neue Risiken.

Die Vernetzung bietet nicht nur Wege zum Datenaustausch, sondern grundsätzlich auch Zugang für Unbefugte mit unlauteren Absichten. In der klassischen IT-Welt gehören Online-Attacken auf Computer schon lange zum Alltag. Firmen und Privatnutzer schützen sich mithilfe eines ganzen Arsenals an verschiedenen Sicherheitstechniken.

Auch im industriellen Umfeld wird die Gefahr steigen, wenn künftig ein durchgängiger Datenfluss vom Internet bis in den Roboterfinger möglich ist. Schad-Programme wie etwa Stuxnet oder Duqu haben das Bedrohungspotenzial bereits verdeutlicht. Ziel waren in beiden Fällen Produktionsanlagen. Und die Attacken waren erst der Anfang, wie Sicherheitsexperten glauben. Sie zeigten, womit Unternehmen in Zukunft rechnen müssen.

Im Vergleich zur klassischen IT sind die Produktionssysteme bisher nur schwach geschützt. Schliesslich mussten sich Unternehmen mit diesem Thema kaum auseinander setzen. Vor allem am unteren Ende des künftigen Industrie-4.0-Netzwerks – im Bereich der Sensorik – seien Sicherheitsmassnahmen bisher vernachlässigt worden, meint Friedrich Vollmar. Er ist bei IBM Experte für Integrationstechnologien und im Arbeitskreis Industrie 4.0 aktiv. In diesem Projekt haben Vertreter der Industrie und der Deutschen Akademie der Technikwissenschaften (Acatech) Umsetzungsempfehlungen für Industrie 4.0 erarbeitet.

Sicherheit ist zentral

Das Konzept Industrie 4.0 steht und fällt mit der Sicherheit der vernetzten Technologien – der sogenannten cyberphysischen Systeme (CPS). Wer befürchten muss, dass seine Maschinen in der Werkshalle den Gefahren des Internets hilflos ausgesetzt sind, wird die vierte industrielle Revolution auf unbestimmte Zeit verschieben. CPS würden nur dann realisiert und akzeptiert werden, «wenn adäquate, zuverlässige und wirtschaftliche Lösungen zum Schutz des digitalen Prozess-Know-hows und zur Absicherung gegen Manipulation und Sabotagen entwickelt und etabliert werden». So steht es im Abschlussbericht des Arbeitskreises Industrie 4.0.

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI), das in dem Bericht zitiert wird, erkennt eine ganze Reihe von Gefahren, denen die CPS ausgesetzt sind (Kasten). Grundsätzlich sind die Produktionsnetze ein besonders sensibler Bereich, weil zum einen die Fertigungsprozesse durch Manipulationen gestört werden können. Zum anderen können sich Eindringlinge Zugang zu Produktgeheimnissen verschaffen. Unternehmen müssen sich also sowohl vor Sabotage als auch vor Industriespionage schützen.

Doch dafür muss das Rad nicht vollkommen neu erfunden werden, ist sich IBM-Mann Vollmar sicher. Die Sicherheitstechnologien, die aus dem klassischen IT-Betrieb bekannt sind, könnten auch als Grundlage dienen, um die Produktionsumgebungen vor Malware zu bewahren. Dazu zählen zum Beispiel Software-Systeme, welche die digitalen Wege – also das Netz – überwachen. Die IT-Branche hat dafür sogenannte Intrusion-Detection-Systeme entwickelt. Diese Programme identifizieren Attacken und leiten automatisch die passenden Gegenmassnahmen ein.

TECHNOLOGIE **INDUSTRIE 4.0**

Bei der Umsetzung von Industrie-4.0-Konzepten müssten ausserdem standardisierte Sicherheitsmethoden von Beginn an in die entsprechende Architektur integriert werden, sagt Olaf Sauer, der beim Fraunhofer Institut für Optronik, Systemtechnik und Bildauswertung (IOSB) für den Geschäftsbereich Automatisierung verantwortlich ist. Er denkt dabei an Authentifizierungsmechanismen und Technologien zum Verschlüsseln und Signieren von Daten.

IT-Anbieter arbeiten bereits an Sicherheitssystemen, die an die besonderen Gegebenheiten im Produktionsumfeld angepasst sind – oder haben solche sogar schon auf den Markt gebracht. So gibt es zum Beispiel Lösungen, die speziell Scada-Umgebungen vor Attacken schützen.

Hohe Verfügbarkeit als Hürde

Zu den grossen Herausforderungen im Produktionsumfeld zählt der Umstand, dass die Anlagen ständig verfügbar sein müssen. Wenn eine Maschine für mehrere Stunden ihrer Arbeit nicht nachgehen kann, weil ein Virenscanner die eingebettete Software nach Schadprogrammen absucht, verursacht das einen signifikanten wirtschaftlichen Schaden.

Zudem verfügen die Steuerungssysteme der Maschinen nur über eine begrenzte Leistungsfähigkeit. Diese ist lediglich darauf ausgerichtet, dass die Anlage ihre Aufgaben erledigen kann. Die Ressourcen reichen nicht aus, um zusätzlich noch Sicherheitssoftware auf dem System zu installieren.

Cloud-Lösungen

Wissenschaftler des Instituts für Steuerungstechnik der Werkzeugmaschinen und Fertigungseinrichtungen (ISW) an der Uni Stuttgart sehen im Cloud-Computing die Lösung für dieses Problem. In dem Modell, an dem die Spezialisten arbeiten, ist das Steuerungsprogramm nicht mehr vor Ort installiert. Es läuft stattdessen auf einem zentralen Server in der Cloud, der über Internettechnologie erreichbar ist. Eine Maschinenbox ersetzt das Steuerungssystem in der Fabrikhalle und gibt die entsprechenden Kommandos an die Anlage weiter.

Potenzielle Angriffsziele sind dann nur noch die Verbindung zwischen Server und Maschinenbox sowie die Box selbst. Da letztere keine prozessrelevanten Berechnungen durchführen muss, können ihre Ressourcen für Sicherheitsfunktionen genutzt werden. Bleibt noch die Strecke zwischen Wolke und Maschinenbox. Um Lösungen für deren Schutz zu entwickeln, arbeitet das ISW derzeit mit Spezialisten für Cloud-Computing und Netzwerktechnik zusammen. Im klassischen IT-Betrieb spielt Cloud-Computing aber bereits eine zunehmend grössere Rolle. Erfahrungen in Sachen Sicherheit aus diesem Bereich könnten daher auch für die Produktionsnetze genutzt werden.

Produktions- und Automatisierungsspezialisten arbeiten allerdings auch an ihren eigenen geschützten Cloud-Lösungen. Schliesslich wird Cloud-Computing in der Industrie-4.0-Welt ebenfalls eine zentrale Bedeutung haben. In der Forschungsinitiative Virtual Fort Knox wollen Experten aus Forschung und Industrie unter der Leitung des Fraunhofer Instituts für Produktionstechnik und Automatisierung (IPA) eine Cloud-Plattform für produzierende Unternehmen entwickeln. Firmen soll damit eine ganze Reihe an Möglichkeiten eröffnet werden: Sie können die Infrastruktur zum Beispiel nutzen, um Programme zwischen verschiedenen Standorten auszutauschen, zentralen Zugriff auf Daten zu haben oder Informationen aus unterschiedlichen Bereichen miteinander zu verknüpfen. Daneben könnten gerade kleinen und mittleren Unternehmen auf der Cloud-Plattform IT-Werkzeuge zur Verfügung gestellt werden, zu denen sie sonst keinen Zugang haben.

Der Name lässt bereits erkennen, dass Sicherheit einer der Projektschwerpunkte darstellt. Das virtuelle Fort Knox soll im übertragenen Sinne genauso sicher sein wie der Militärstützpunkt, in dem die US-Goldreserven gelagert werden. Ein grosser Teil des Projekts ist daher der Entwicklung von Technologien gewidmet, um die sensiblen Firmendaten und Anwendungen zu schützen, die in der Cloud gehalten werden.

«Virtual Fort Knox ist ein Ansatz, aber bei Weitem noch keine fertige Lösung», schränkt allerdings Professor Alexander Verl vom Fraunhofer IPA ein. Über die Sicherheitstechnik hinaus müssten in dem Projekt noch Fragen geklärt werden wie «Wer ist Besitzer der Daten?», «Wem dürfen sie weitergegeben werden?» oder «Wer haftet dafür?».

Damit wird deutlich, dass Sicherheit in der Industrie 4.0 nicht nur eine Technologie-Frage sein wird. Unternehmen müssen sich grundlegend mit dem Thema beschäftigen. IT-seitig geschützte Produktionsumgebungen müssen Teil der Gesamtsicherheitsstrategie sein. Das schliesst auch den Faktor Mensch mit ein, der immer eine potenzielle Schwachstelle darstellt. Mitarbeiter müssen im Umgang mit Sicherheitsmassnahmen geschult werden, um den Schutz der Produktionsnetze zu gewährleisten.

Hintergrund

Bedrohungen für die Industrie

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat eine Top-Ten-Liste der aktuellen Bedrohungen zusammengestellt, denen sogenannte Industrial Control Systems (ICS) ausgesetzt sind. Der Arbeitskreis Industrie 4.0 hat diese Liste in seinen Abschlussbericht aufgenommen.

1. Unberechtigte Nutzung von Fernwartungszugängen.
2. Online-Angriffe über Office-/Enterprise-Netze.
3. Angriffe auf eingesetzte Standardkomponenten im ICS-Netz.
4. (Distributed) Denial-of-Service-Angriffe.
5. Menschliches Fehlverhalten und Sabotage.
6. Einschleusen eines Schadcodes über Wechseldatenträger und externe Hardware.
7. Lesen und Schreiben von Nachrichten im ICS-Netz.
8. Unberechtigter Zugriff auf Ressourcen.
9. Angriffe auf Netzwerkkomponenten.
10. Technisches Fehlverhalten und höhere Gewalt.

Autor

Markus Strehlitz schreibt als freier Journalist über Informationstechnologie und Technikthemen.

Textbüro, DE-68219 Mannheim, ms@textbuero-strehlitz.de

Dieser Beitrag erschien im VDE-Dialog 02/2013.

Résumé

Des intrus numériques

Attaques en ligne de sites de production interconnectés

L'interconnexion de sites de production n'a pas que des avantages. Elle accroît aussi les risques en termes de sécurité. Des solutions issues du domaine des technologies de l'information sont donc mises en œuvre afin d'éviter des intrusions indésirables au sein de l'infrastructure de production interconnectée. Les procédés employés peuvent cependant être eux-mêmes à l'origine de nombreux challenges dans ce contexte de production. No