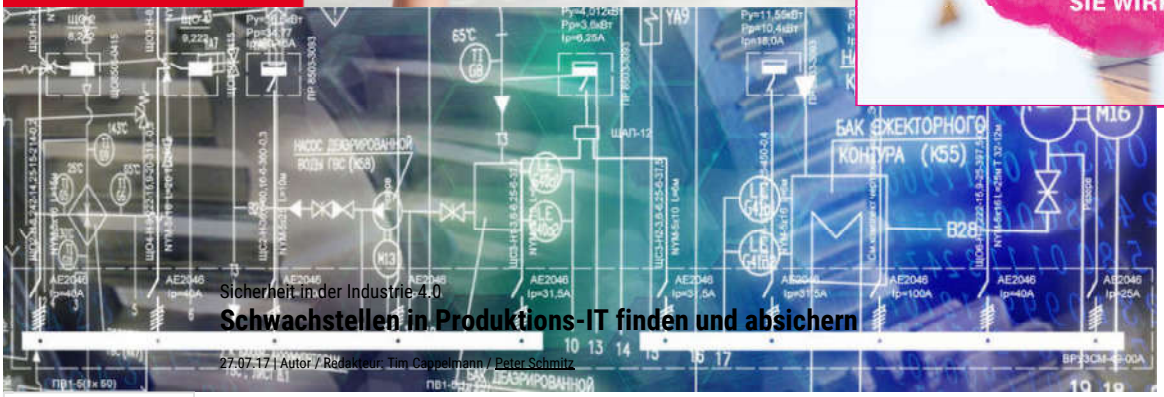
Cookies erleichtern die Bereitstellung unserer Dienste. Mit der Nutzung unserer Dienste erklären Sie sich damit einverstanden, dass wir Cookies verwenden. Weitere Informationen OK



Sicherheit in der Industrie 4.0

Schwachstellen in Produktions-IT finden und absichern

27.07.17 | Autor / Redakteur: Tim Cappelmann / Peter Schmitz

In vielen Unternehmen treffen in produktionsnaher IT unterschiedliche Softwaresysteme und Prioritäten aufeinander; das sorgt für neue Risiken. (© red150770 - stock.adobe.com)

Fabriken sind immer wieder Ziel von Cyber-Angriffen – mit teils verheerenden Folgen: Ein Produktionsstillstand oder defekte Maschinen ziehen hohe Kosten nach sich. In Zeiten von Industrie 4.0 gewinnt das Thema IT-Sicherheit immer mehr an Bedeutung. Aber wie können Betriebe produktionsnahe IT absichern?

Ein Produktionsausfall ist für jedes Unternehmen eine wirtschaftliche Herausforderung. Besonders kritisch ist die Lage, wenn es sich um Betriebe handelt, die die Bevölkerung mit Strom, Wasser oder Wärme versorgen. Die Schwachpunkte sind meistens die Schnittstellen zwischen produktionsnaher IT – also den Maschinen, die inzwischen annähernd alle via Internet kommunizieren können – und der restlichen IT des Unternehmens.

Die Fertigungskomponenten, wie etwa Walzen oder Fräsen, melden selbstständig, ob sie Öl benötigen, eine Schraube verschlissen ist oder eine Wartung ansteht. Über ein Product Lifecycle Management liefern die Maschinen darüber hinaus hilfreiche Informationen für die Weiterentwicklung der Produkte. Die Voraussetzung dafür ist jedoch die Verknüpfung der Komponenten mit der Unternehmens-IT. Diese Schnittstellen stellen ein Sicherheitsrisiko dar.

Risiken heterogener Systeme

In der Regel treffen hier unterschiedliche Softwaresysteme aufeinander, die zunächst nicht kompatibel sind. Die Entwicklung neuer Fertigungssysteme ist häufig Aufgabe von Automatisierungstechnikern. Grundsätzlich lehnen diese ihre IT-Protokoll-Landschaften zwar an IETF- oder IEEE- Standards an, doch ein belastbarer Industriestandard innerhalb der Fertigungsanlagen hat sich längst noch nicht etabliert. Das erschwert das Zusammenwirken der Systeme – Security Devices können den Datenfluss nicht erfassen.

share me
share me
tweet me
share me
PDF
Weiterempfehlen
Drucken

Anzeige

Es entstehen Sicherheitslücken, durch die Cyber-Kriminelle ohne großen Aufwand Schadcode einschleusen können. Ein einfacher USB-Stick, den beispielsweise ein externer Wartungstechniker an einer Fertigungskomponente anschließt, reicht aus, um die Malware in Umlauf zu bringen. Systemkopplungen zu IT-Dienstleistern oder Vorlieferanten im Sinne des Supply-Chain-Managements weichen Verantwortlichkeiten auf. Vertragsinhalte und Haftungsfragen müssen deshalb im Industrie 4.0-Ansatz neu gedacht werden. Es stellt sich beispielsweise die Frage, wer haftet, wenn die Produktion aufgrund einer Störung im Datenfluss zum Erliegen kommt.

Schwieriges Patch-Management

In den meisten Betrieben sind Maschinen von unterschiedlichen Herstellern im Einsatz. So kommt es, dass jede Komponente eine eigene, proprietäre Software besitzt. Auch hier stellt sich wieder die Frage nach der Kompatibilität der Software mit derjenigen der Office-IT. Ein Einkäufer legt bei der Wahl der Geräte sein Augenmerk nicht auf die Software, sondern auf Wirtschaftlichkeit und Durchsatzzahlen. Die IT-Verantwortlichen haben demnach wenig Einfluss, wenn es um die Wahl möglichst homogener Software-Systeme geht.

Ein weiteres Sicherheitsrisiko entsteht, wenn ältere Komponenten auf neue Systeme treffen, die nicht interoperabel sind. Diese veralteten Technologien zu patchen, um einen gewissen Sicherheitsstandard zu erreichen, ist eine Herausforderung. Denn für ein Software-Update muss die Produktion ruhen. Die meisten Anlagen sind jedoch dafür ausgelegt, an 365 Tagen im Jahr 24 Stunden zu produzieren.

Anzeige


Um unproduktive Phasen zu minimieren, planen die Verantwortlichen teils nur alle sechs Monate ein Update. Ein langer Zeitraum, in dem sich Schadcode ausbreiten kann. Dazu kommen weitere Herausforderungen für die IT-Verantwortlichen: Erfolgt die Implementierung der Fertigungsanlagen nicht so, wie es die IT-Protokolle vorsehen, hakt es auch bei den Verfahren zur Datenübertragung und den Interfaces. Das erschwert die Arbeit von Security Monitoring Systemen erheblich.

Awareness schaffen

Die Folge: Anomalie- oder signaturbasierte Intrusion Detection Systeme (IDS) melden im Produktionsumfeld viel zu häufig False Positives, da sie den Datenfluss als solchen nicht erkennen. Die Maschinen in die etablierten IT-Sicherheitsstrukturen des Betriebes einzubinden, ist für die IT-Verantwortlichen demnach keine leichte Aufgabe. Gerade deshalb sollten sie auf höchster Ebene Awareness für Sicherheitsthemen schaffen. Meist reicht es bereits aus, auf gesetzliche Vorgaben zu verweisen, die zur Sicherheit produktionsnaher IT bestehen. Der Geschäftsführung muss bewusst sein, dass diese unter schwierigen Voraussetzungen nicht zu erfüllen sind.

In Hinblick auf die Technologie steht die Entwicklung eines Sicherheitskonzeptes an erster Stelle. Ausgangspunkt bildet eine umfangreiche Analyse des Ist-Zustands. Auch hier steht die Verknüpfung zwischen Office-IT und Fertigungskomponenten im Fokus, die meist über das ERP-System geschieht. Um einen Produktionsstillstand zu vermeiden, bietet sich das Bilden von Zonen und die Festlegung von Schutzbedarfen an. Restriktive Firewall-Regelwerke begrenzen diese Bereiche. Auch der Übergang aus einer in die andere Zone wird streng reglementiert.

Als letzter Schritt bleibt der Einsatz einer eigenen Sicherheits-Hardware für jede zu schützende Fertigungskomponente. Schließlich bietet aber auch diese Vorgehensweise keinen vollumfänglichen Schutz. Deshalb sollte es oberste Priorität sein, die Schnittstellen zwischen den einzelnen Komponenten auf ein Minimum zu reduzieren.

Fazit

IT-Sicherheit ist immer auch ein Awareness-Thema. Um Cyber-Kriminellen keine Angriffsfläche zu bieten, sollten Unternehmen in die Schulung ihrer Mitarbeiter investieren. Im Idealfall steht der Geschäftsführung eine Doppelspitze aus Risikomanager und IT-Spezialisten zur Seite, die das Thema Sicherheit an höchster Stelle platziert. Das fachliche Know-how dieser Doppelspitze versetzt Betriebe in die Lage, auf Bedrohungen für die IT in ihrer Produktion angemessen zu reagieren.

Über den Autor: Tim Cappelmann ist Leiter Managed Services bei AirITSystems.

KOMMENTAR ZU DIESEM ARTIKEL

ANONYM MITDISKUTIEREN ODER EINLOGGEN ANMELDEN

Name eingeben...

Zeichen: 0/1500

Kommentieren

MEHR ZUM THEMA

Schutzschild für Steuerungssysteme

Produktions-IT gegen Cyber-Attacken absichern

mehr...

Datensicherheit bei der M2M-Kommunikation

Sicherheitsstrategien für die industrielle Fertigung

mehr...

Kommentar von Dr. Sebastian Schmerl, Computacenter

Industrial Security – Cyber Defence für die Produktion

mehr...

Nachgefragt: 8 Experten zum Thema Industrie 4.0 und Security

Industrial Security - so stark wie ihr schwächstes Glied

mehr...

Industrial IT Security

Spezielle Risiken, spezielle Sicherheitslösungen

mehr...

Kommentar von Dror-John Röcher, Computacenter

Industrie 4.0 – das volle Potenzial sicher nutzen

mehr...

PASSENDE FIRMEN ZUM THEMA

Alle Firmen

IT-Sec Report by bloodsugarmagic

78050 Villingen-Schwenningen | Deutschland

mehr...

PASSENDE WHITEPAPER & WEBCASTS

Alle Whitepaper Alle Webcasts

Cybersicherheit und Schutz vor Datendiebstahl

Management von Risiken innerhalb der eigenen Organisation

mehr...

Cyberkriminalität ist auch in der Industrie angekommen

IT-Sicherheit für die Industrie 4.0

mehr...

Data Theft Prevention

Der Schlüssel zu Sicherheit, Wachstum und Innovation

mehr...

Dieser Beitrag ist urheberrechtlich geschützt. Sie wollen ihn für Ihre Zwecke verwenden? Infos finden Sie unter www.mycontentfactory.de (ID: 44806708 / Internet of Things)

Oder kontaktieren Sie uns direkt

Security-Insider ist eine Marke von Vogel Business Media. Unser gesamtes Angebot finden Sie hier

AGB | FWG | Hilfe | Kundencenter | Media | Datenschutz | Impressum
Copyright © 2017 Vogel Business Media

© ALEXMAZ - Fotolia.com; Vogel IT; red150770 - stock.adobe.com; © Taiga - Fotolia; © Rainer Plendl - Fotolia; Computacenter; Bild: Rockwell Automation; Bild: Innominate Security Technologies; Bild: Computacenter; IT-Sec Report by bloodsugarmagic; DriveLock;