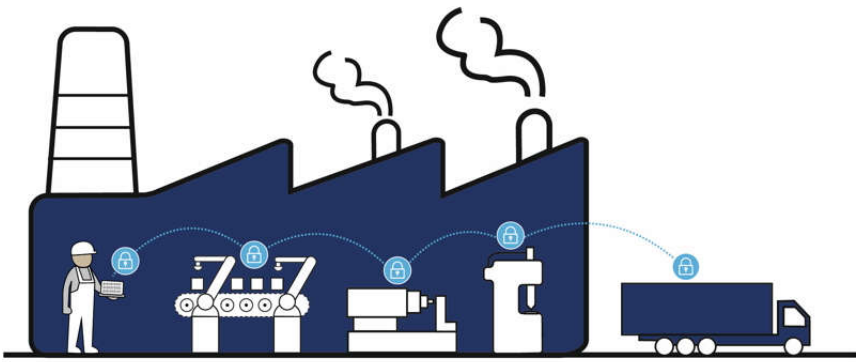
LANLINE-NEWSLETTER

Lesen Sie regelmäßig die aktuellsten Nachrichten aus der LANline-Welt in unserem **LANline-Newsletter**

Fallstricke bei der Industrie 4.0

Sicherheitslücke an der Schnittstelle

12. Mai 2017 | Von Tim Cappelmann. *[ts]*
Schlagwörter: Airitsystems, IIoT, Industrial IT



Die stete Weiterentwicklung der IT hat industrielle Prozesse flexibler gemacht und

deutlich verbessert. Industriebetriebe sind heute in Zeiten von Industrie 4.0 miteinander vernetzt, schon seit Langem sind viele Fertigungskomponenten digitalisiert. Das birgt einige Herausforderungen. Besonders hinsichtlich der Sicherheit müssen Unternehmen ihre Hausaufgaben machen.

Office-IT-Systeme und die Systeme der produktionsnahen IT driften häufig auseinander. Denn in der Regel entwickeln und implementieren Automatisierungstechniker neue Fertigungssysteme und -anlagen. Dabei orientieren sie sich bezüglich der Software in den meisten Fällen nicht an Industriestandards, da ihre Kernkompetenzen in anderen Bereichen liegen. Dementsprechend schwierig ist es, die Fertigungskomponenten einer Fabrik wie beispielsweise eine Schweißmaschine an die Office-IT anzubinden, was aber im Rahmen eines Product-Lifecycle-Managements immer häufiger nötig ist. Diese Schnittstellen vor dem Eindringen von Malware zu schützen, ist eine Herausforderung für die IT-Verantwortlichen. Einen effektiven Schutz vor Sabotageakten oder Industriespionage gibt es unter diesen Voraussetzungen kaum bis gar nicht.

Wenn gängige IT-Systeme und die proprietäre Software der Fertigungskomponenten aufeinandertreffen, gibt es einige

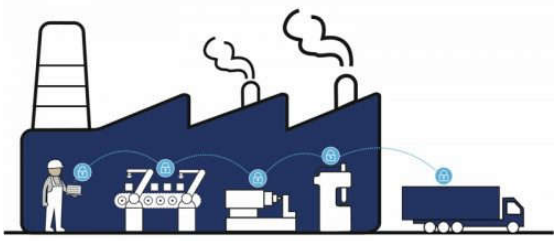
Fallstricke. Grundsätzlich versucht die Industrie ihre IT-Protokolllandschaften an IETF- oder IEEE-Standards zu orientieren. Das hat den Vorteil, dass heterogene Systeme zusammenarbeiten können. Die Interoperabilität dieser Systeme ermöglicht den Security Devices, den Datenfluss zu erfassen. In der Praxis gelingt dies in der Fertigung aber nur selten. Gerade im Zusammenhang mit älteren Anlagen stehen die IT-Verantwortlichen deshalb immer wieder vor den gleichen Problemen: Nicht IT-protokollkonforme Interfaces und Verfahren zur Datenübertragung, veraltete Technologien, die sich nicht patchen lassen, oder die nicht IT-protokollkonforme Implementation der Anlagen. Die Folge: Anomalie- oder signaturbasierte Intrusion-Detection-Systeme (IDS) agieren im reinen Produktionsumfeld häufig mit einer besorgniserregenden False-Positive-Rate, da sie im Datenfluss den Kontext nicht erkennen. Schon simple Stateful Firewalls haben auf Layer 4 Probleme mit ungewöhnlichen TCP-Sequenzen.

Wenn es um die Implementierung von neuen IT-Security-Maßnahmen geht, bleiben die Wünsche der IT oft zugunsten der Produktion auf der Strecke. Denn oberste Priorität hat der reibungslose Betrieb der Fertigungsanlagen.

Schwieriges Patch-Management

Folglich gestaltet sich das Patch-Management im Bereich der

produktionsnahen IT sehr schwierig. Die Fertigungsanlagen sind für Produktionszeiten rund um die Uhr ausgelegt. Unproduktive Zeiten sind auf ein Minimum beschränkt. Intervalle für Software-Updates von bis zu sechs Monaten sind daher keine Seltenheit, in Anbetracht der aktuellen Schadcodezyklen aber viel zu groß. Wie können IT-Verantwortlichen trotz dieser Umstände ein gewisses Maß an Sicherheit gewährleisten? Zunächst ist es ratsam, auf höchster Ebene die ungünstigen Voraussetzungen für ein Sicherheitskonzept anzusprechen und dort ein Bewusstsein dafür bei den Entscheidern zu schaffen. Auch in Bezug auf die Sicherheit produktionsnaher IT gibt es gesetzliche Vorgaben, die es einzuhalten gilt.



Das Bilden von Zonen gleichen Schutzbedarfs ist eine gute Möglichkeit, um den Schutz der Produktion zu erhöhen. Dabei begrenzen restriktive Firewall-Regelwerke jede dieser Zonen. Bild: Airitsystems

Die Grundlage eines Sicherheitskonzeptes bildet die genaue Analyse des Ist-Zustandes. Wie sind die Fertigungsstraßen mit der Office-IT verknüpft und an welchen Schnittstellen bestehen Sicherheitslücken?

Häufig erfolgt die Verknüpfung über das ERP-System. Ist eine Sicherheitslücke gefunden, ist es für die IT nicht immer einfach, diese auch zu schließen. In der Regel ist das Ruhenlassen der Produktion zugunsten einer Sicherheitsmaßnahme keine Option. So bleiben manche Maßnahmen aufgrund der Umstände auf der Strecke. Das Bilden von Zonen gleichen Schutzbedarfs ist in solchen Fällen eine gute Möglichkeit, um den Schutz zu erhöhen. Restriktive Firewall-Regelwerke begrenzen jede dieser Zonen. Die Übergänge zwischen Zonen unterschiedlichen Schutzbedarfs sind reglementiert. Diese Bedarfe können IT-Verantwortliche notfalls durchsetzen, indem sie in jede Komponente der Fabrik eine eigene Hardware mit einer Firewall integrieren. Auch diese Vorgehensweise schließt nicht alle Sicherheitslücken, doch bleibt den IT-Verantwortlichen oft nur zu akzeptieren, dass ein gewisser Bereich der produktionsnahen IT nicht optimal geschützt ist. Nicht zuletzt deshalb ist es sinnvoll, die Kommunikationsmatrix gering zu halten, also nur wenige Schnittstellen zwischen den Komponenten zu bilden.

Gefahrenpotenziale erkennen

Ein weiteres Problem stellt die Heterogenität der Anlagen dar. Innerhalb einer Fabrik kommen meist Fertigungskomponenten von mehreren Herstellern zum Einsatz. Jeder Hersteller

entwickelt seine eigene proprietäre Software. Die Einkäufer legen ihr Augenmerk aber selten auf den IT-Unterbau der Maschinen. Für sie stehen vor allem die Durchsatzzahlen im Vordergrund. Die IT hat dementsprechend kaum Mitspracherecht bei der Auswahl der Fertigungskomponenten.

Um Schutzmaßnahmen zu definieren, ergibt es Sinn, mögliche Bedrohungsszenarien durchzuspielen. Der häufigste Weg, auf dem Schadcode in Unternehmen gelangt, ist über fremde Hardware. Ein Beispiel: Ein Techniker des Anlagenherstellers schließt zur Wartung seinen Laptop an der Produktionskomponente an und schleust so ungewollt einen Virus ein. Im schlimmsten Fall droht ein Produktionsstillstand – ein Szenario, das vermutlich die meisten produzierenden Unternehmen aus leidvoller Erfahrung kennen. Schutz bietet hier die Absicherung der Schnittstellen durch Einwahlrouter, die keine direkte Verbindung zwischen externer Hardware und Fertigungsanlage ermöglichen.

Besonders gefährdet sind Kritis-relevante Unternehmen, also Einrichtungen, deren Ausfall zu Versorgungsengpässen führen kann. Solche Ausfälle beispielsweise von Kraftwerken zur Stromversorgung haben eine große mediale Wirkung, was für manchen Hacker ein zusätzlicher Ansporn ist. Weniger betroffen sind

Fertigungsanlagen von Angriffen mit dem Ziel der Industriespionage. In diesem Zusammenhang ist vorrangig die IT im Bereich Forschung und Entwicklung gefährdet.

Den Herausforderungen in puncto Sicherheit begegnen Unternehmen im besten Fall mit einem umfassenden Risiko-Management. Um Bedrohungen im Bereich der IT zu identifizieren und weiterzugeben, ist fachliches Know-how gefragt. Deshalb ist es sinnvoll, eine Doppelspitze aus Risiko-Manager und IT-Beauftragtem zu bilden. Diese sollte direkt der Geschäftsführung unterstehen, um auf höchster Ebene ein Bewusstsein für das Thema IT-Sicherheit zu schaffen.

Tim Cappelmann ist Leiter Managed Services bei Airitsystems (www.airitsystems.de).

Mehr zum Thema

- Firewall für die Industrie 4.0
- Studie: Relevanz interner IT sinkt
- IT und Satelliten sollen Landwirtschaft verbessern
- All-Flash-Innovationen für die hybride IT
- Geschäftsführung weiß zu wenig über Angriffe auf die IT

SHARE: