Digitalisierung auf dem Shopfloor

Gefahr im Verzug

Hacker haben inzwischen erhebliche kriminelle Energie aufgebaut, sind besser organisiert und gehen entschlossener denn je vor. Auch das Produktionsumfeld ist inzwischen massiv betroffen. Dabei leistet die Vernetzung von OT und IT massiv Vorschub bei den Angriffspunkten. Handlungsempfehlung in diesem Spannungsfeld gibt ANDREAS DEML.

Ob Internet der Dinge, Industry 4.0 oder IIoT – alle diese Begriffe fassen einen Megatrend zusammen, der seit mehreren Jahren in Produktionshallen und Fertigungslinien, aber auch in der Logistik um sich greift. Gemeint ist die Vernetzung industrieller Geräte wie Sensoren, Steuergeräte oder auch Transportsysteme und die Dynamisierung in der Datenaggregation. Diese Entwicklung ist für die Automatisierung, zentraler Bestandteil jeder Produktionsumgebung, prägend geworden.

Die üblicherweise nachträglich durchgeführte Aufrüstung ursprünglich isoliert arbeitender Produktionsgeräte und die Einbindung in Netzwerke wird auch als „Brownfield"-Szenario beschrieben: Auf Altsysteme – häufig langlebig und kostenintensiv –, die aus vielschichtigen Gründen nicht mehr aktualisiert werden können, werden neue Technologien aufgesetzt, die die bereits vorhandene Komplexität weiter steigern, um den Ansprüchen der Digitalisierung im Unternehmen gerecht zu werden.

Das Problem hierbei ist, dass viele solcher Produktionssysteme nicht entwickelt wurden, um an das Internet angebunden zu werden. Durch die aktuelle Entwicklung – Angriffe auf Produktionssysteme werden immer häufiger; Angreifer investieren mehr Geld, Zeit und Aufwand – steigt das Risiko signifikant, selbst einem Sicherheitsvorfall ausgeliefert zu sein. Der Lagebericht 2020 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zeigt, dass die Anzahl neuer Schadprogrammvarianten im Vergleich zu 2019 um über drei Millionen angestiegen ist und eine Fortsetzung des Trends beobachtet werden kann, dass Angreifer vermehrt cyberkriminelle Angriffe auf Unternehmen und Institutionen durchführen (1).

Mit der Anbindung dieser Produktionssysteme in IT-Netze gehen auch neue Geschäftsprozesse und Strukturen einher. Verantwortlichkeitsbereiche beginnen zu verschwimmen, da Produktionssysteme und die IT nicht mehr klar voneinander abgegrenzt werden können. Zu Recht wird deshalb die Sicherheit dieser Produktionssysteme immer mehr zur Priorität. Dieser Bereich der Sicherheit wird auch als „OT Security" (Operational Technology Security) bezeichnet.

Produktionssysteme sind schon immer ein zentraler Bestandteil der Wertschöpfung von produzierenden Unternehmen gewesen und hatten entsprechende Priorität im Rahmen von Sicherheitskonzeptionen – durch den Einsatz von IIoT-Geräten und die Anbindung von Produktionssystemen an größere Netzwerke oder das Internet wird die komplexe Thematik OT-Security um weitere Dimensionen erweitert.

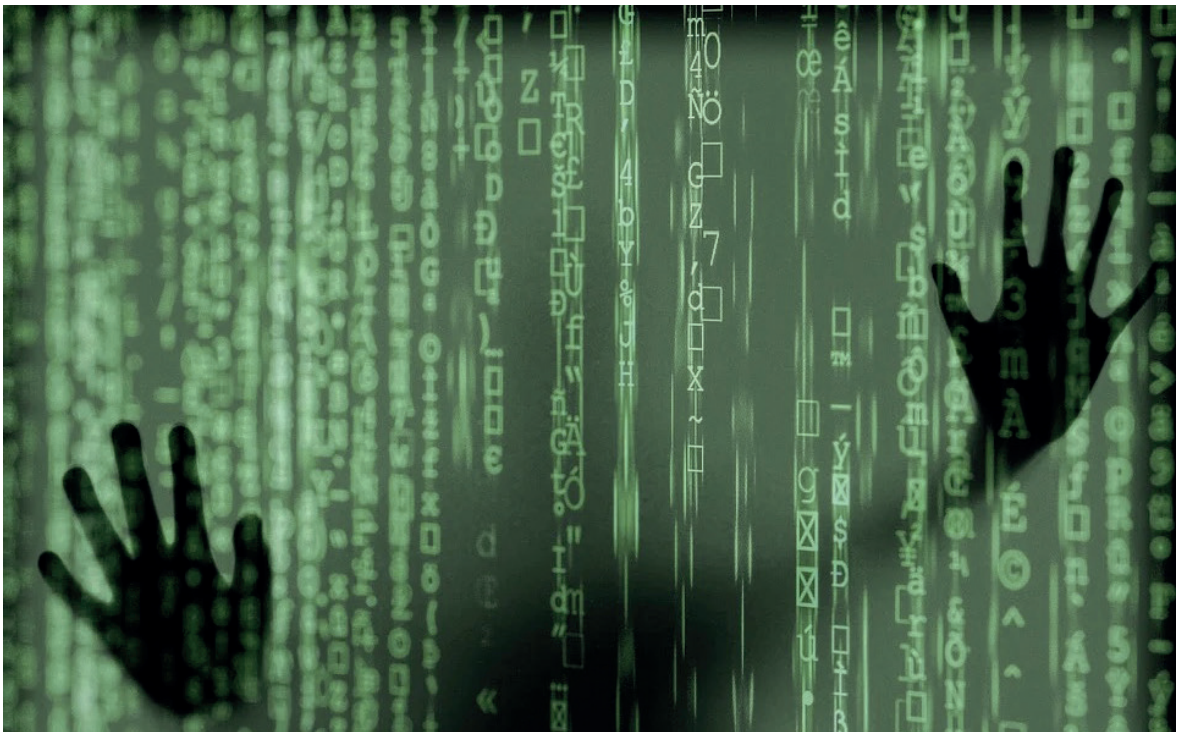
Um den reibungslosen Verlauf der Produktion in einem Betrieb zu gewährleisten, ist es daher wichtiger denn je, entsprechende präventive Maßnahmen zu treffen, um einen den neuesten Entwicklungen entsprechenden Reifegrad in der OT-Security zu gewährleisten.

Sichere IT-Architekturen

Produktionsstart der neuen S-Klasse. Vermehrt sind Fertigungslinien Hackerangriffen ausgesetzt

Bild: Mercedes-Benz

Eine große Rolle in der effektiven Sicherheit von vernetzten IT-Systemen spielt die Architektur der Netze innerhalb der Firma. Eine konventionelle, seit Jahren eingesetzte, aber bis heute als Best Practice betrachtete Methode dafür ist die Netzwerksegmentierung und -segregation. Diese Methodik sieht vor, das geplante Netzwerk in logische Unternetzwerke aufzuteilen (zu partitionieren) und die Netzübergänge durch technische Maßnahmen wir Firewalls zu kontrollieren, um die Ausbreitung von Angreifern innerhalb des Gesamtnetzes zu verlangsamen.



Beispielsweise könnten in einer OT-Umgebung die IIoT-Geräte der einzelnen Fertigungshallen in unterschiedlichen Netzwerken untergebracht sein. Doch nicht nur eine geografische Trennung (Segregation) ist wichtig und sinnvoll, sondern auch eine logische, beispielsweise die Trennung des Produktionsnetzwerks von der Personalabteilung. Bei der Trennung von Netzen sollte immer das Need-to-know-Prinzip angewandt werden – mit anderen Worten: die Systeme oder Mitarbeiter haben nur Zugriff auf diejenigen Systeme und Daten, die sie für ihre Aufgaben tatsächlich benötigen.

Häufig eingesetzt wird hier die IEC-Norm 62 443, die sich explizit mit der IT-Sicherheit von Produktionssystemen auseinandersetzt und ein entsprechendes Sicherheitskonzept aufbaut. Aufgeschlüsselt in vier Abschnitte werden die Themen Richtlinien & Prozesse, Systeme, Komponenten/Produkte sowie grundsätzliche Strategien beschrieben. Über einen sogenannten Defense-in-Depth-Ansatz soll sichergestellt werden, dass durch das Aushebeln einzelner Sicherheitsmaßnahmen die Gesamtsicherheit der Umgebung weitestgehend gewährleistet ist (2). Im Kontext der OT-Sicherheit wird hier ein „Zwiebelprinzip“, also eine Etablierung mehrerer Schutzschichten, eingesetzt (siehe Grafik).

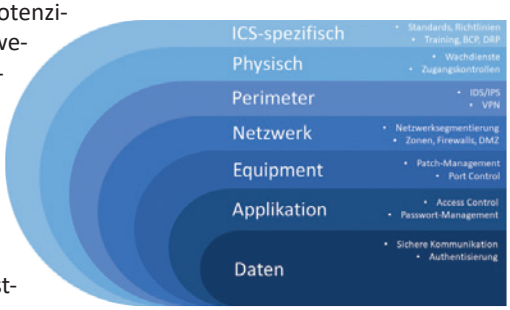
Zu weiteren „architektonischen“ Maßnahmen gehört unter anderem die Einführung von DMZs (demilitarisierten Zonen) zwischen Produktionsnetz und dem Internet oder anderen Netzwerken. In einer DMZ können Webserver oder Datenbanken für Sensorwerte installiert sein, die für externe Dienstleister bereitgestellt werden. Im Falle eines erfolgreichen Angriffs auf diese Server würde weiterhin das Produktionssystem mithilfe einer zweiten Firewall geschützt sein. Außerdem ist auch der Einsatz von VLAN (Virtual LAN) im Produktionsnetzwerk denkbar, um dynamisch zeitlich und logisch abgeschlossene Bereiche zu schaffen, in dem zum Beispiel Dienstleister Wartungen durchführen können.

Fernwartung – die versteckte Backdoor

Viele Geräte in Produktionsstätten sind nur für den Einsatz in internen Netzwerken konzipiert worden. Dort kommunizieren sie mit Steuergeräten, RTUs, SCADA-Systemen oder anderen verbundenen Netzwerkgeräten. Eine Anbindung an das Internet ist dabei nicht vorhergesehen; diese ist in der Praxis jedoch verbreitet, um beispielsweise die Fernwartung der Geräte durch externe Dienstleister und Partner zu vereinfachen. Außerdem müssen Mitarbeiter wie Ingenieure oder Netzwerkadministratoren von anderen Standorten aus oder aus dem Homeoffice auf Geräte oder Monitoringsysteme zugreifen können, um eine schnelle Konfigurierung vornehmen zu können und die Antwortzeiten zu minimieren.

Häufig ist eine der einfachsten Methoden, die OT-Geräte direkt über das Internet zugänglich zu machen (über eine statische Portweiterleitung, VPN). Selten wird jedoch berücksichtigt, dass eine Fehlplanung oder eine falsche Konfiguration dazu führen kann, dass Dienstleister und potenzielle Angreifer auf das Netzwerk zugreifen und sich dort lateral bewegen können, oder dass aufgrund eines falschen Berechtigungsmanagements ein Zugang zu sensiblen Systemen möglich ist.

Unabhängig von der weiteren Sicherheit der Netze ist es also prioritär, auch ein Zugriff externer Dienstleister auf OT-Geräte im internen Netz zu segregieren und zu monitoren, um die Angriffsfläche zu begrenzen und die Sicherheit innerhalb des Firmennetzwerkes zu gewährleisten, sodass Abhängigkeiten und zwangsläufige Beeinträchtigungen der OT-Landschaft durch Dienstleister minimiert werden.



Zwiebelprinzip bei Defense-in-Depth
Quelle: Autor

Was tun?

Infolge des signifikanten Anstiegs der Angriffe in den letzten Jahren rücken auch mittelständische Firmen immer mehr ins Fadenkreuz der Angreifer. 2020 verdoppelte sich der Schaden durch Cyberangriffe im Vergleich zu den Vorjahren auf 223 Milliarden Euro, wie der Branchenverband Bitkom mitteilen ließ. Im Hinblick auf eine sorgenfreie Zukunft ist es also für Unternehmen in Deutschland wichtiger denn je, Vorsorge zu betreiben.

Ein Ransomware-Angriff, der sich ungehindert im Firmennetzwerk verteilt, kann die Produktion wochen- bis monatelang lahmlegen. Der Hiscox Cyber Readiness Report 2020 zeigt unter anderem auf, dass sich der Medianschaden durch Cyberangriffe von 10 000 US-Dollar im Jahre 2019 auf 57 000 US-Dollar erhöht hat (3). Mit 44 Prozent hat nahezu die Hälfte aller Firmen im Produktionsbereich mindestens einen Securityvorfall gemeldet. Da nach einem solchen Angriff die Kosten für Wiederaufbau und Verlust durch angehaltene Produktion signifikant ausfallen können, ist es nur ratsam, eine intensive Auseinandersetzung mit dem Thema OT Security im eigenen Betrieb zu forcieren.

In Risikokalkulationen häufig nur unzureichend berücksichtigt sind unter anderem Reputationsschäden, die unabhängig von einer akuten Situation langfristige Effekte haben und sich nachhaltig auf das Vertrauen von Kunden auswirken können. Präventiv ist es mit präzise gewählten, auf das Unternehmen abgestimmten geringen Investitionen möglich, einen signifikanten Mehrwert zum Reifegrad der Sicherheit in der Produktionsumgebung beizutragen.

Die OT-Security stellt einerseits eine Herausforderung dar, die mit neuen Ansätzen anzugehen ist; andererseits bietet sie aber auch die Chance, den Einsatz von IT-Systemen in der industriellen Prozess- und Fertigungstechnik zu vereinfachen, zu modernisieren und sicherer zu gestalten.

Alle an einen Tisch

Operational Technology zieht sich durch viele verschiedene Verantwortlichkeitsbereiche im Unternehmen, daher ist es wichtig, diese Herausforderungen ganzheitlich anzugehen, um eindeutig definierte Prozesse und hohe Synergien zu gewährleisten und einen angemessenen Reifegrad in der OT-Security zu erreichen.

Der Autor ist Head of Global OT Security Center of Excellence bei der BDO Cyber Security GmbH

(1) www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html
(2) Zum Beispiel: en.wikipedia.org/wiki/Defence_in_depth
(3) www.hiscox.de/cyber-readiness-report-2020/

www.bdosecurity.de