MEINUNGEN

CYBERSICHERHEIT IN DER OT: SIND DIE INDUSTRIEUNTER-NEHMEN BEREIT

Khobeib Ben Boubaker
Head of Industrial Security Business Line, Stormshield

„Die Industrie mag keine Fremdkörper“, sagt Thierry Hernandez, Industriekundenbetreuer bei Stormshield. Dennoch ist die Sicherung der Produktionsinfrastruktur eine grundlegende Herausforderung und die Cyber-Lösungen sind ausgereift. Ist die Industrie bereit?

OT – für Operation Technology oder Betriebstechnologie – ist überall. Und vor allem in den Fabriken, wo die Produktion immer stärker automatisiert wird. *„Die Verbindung zwischen IT und OT besteht bereits seit Jahrzehnten“*, betont **Thierry Hernandez**, Account Manager für die Industrie bei Stormshield. *Nur mit Industrie 4.0 gibt es viel mehr Datenflüsse“*. Datenflüsse und die damit verbundenen Cyberrisiken. Aber von welchen Risiken ist die Rede? Mit welchem Schutz? Welche Strategien sollten kurz-, mittel- und langfristig umgesetzt werden? Antwortelemente

VIELFÄLTIGE CYBERRISIKEN FÜR DIE INDUSTRIE

Trotz der grundlegenden Bedeutung des Datenflusses in OT-Netzwerken haben einige Industrieunternehmen Schwierigkeiten, die damit verbundenen Probleme anzugehen. Fernab von böswilligen Angriffen liegen ihre täglichen Prioritäten darin, die Sicherheit ihrer Außendienstmitarbeiter, die mit schweren und potenziell gefährlichen Maschinen zusammenleben, und die Kontinuität der Produktionslinien zu gewährleisten.

„Man muss sich vor Augen halten, dass Risiken auch durch Nachlässigkeit entstehen können, und sich nicht nur auf direkte böswillige Angriffe konzentrieren. Da es in einer Fabrik viele Beteiligte gibt, stellt jeder Durchgang oder Eingriff ein zusätzliches potenzielles Einfallstor dar."

Thierry Hernandez, Industrial Account Manager bei Stormshield

Was die Cyberbedrohungen im OT betrifft, *„muss man sich vor Augen halten, dass Risiken auch durch Nachlässigkeit entstehen können, und sich nicht nur auf direkte böswillige Angriffe konzentrieren"*, meint Thierry Hernandez. *Da es in einer Fabrik viele Beteiligte gibt, stellt jeder Durchgang oder Eingriff ein zusätzliches potenzielles Einfallstor dar."* Industrielle Routinevorgänge wie Fernwartung und Updatekampagnen werden dann zu potenziellen Schwachstellen. Um sicherzustellen, dass die Fernwartung nicht zu einem Bedrohungsvektor wird, muss z. B. sichergestellt werden, dass die Bediener nur Zugriff auf die benötigten Geräte haben. Die Authentifizierung der Benutzer und die damit verbundenen Privilegien werden zu einem wesentlichen Punkt, den es zu beherrschen gilt.

Ein weiterer Vektor für große Cyberrisiken? USB-Sticks, wie eine von Honeywell durchgeführte Studie feststellt: 2021, 37 % der Bedrohungen speziell für die Verwendung von Wechseldatenträgern konzipiert worden sein. Dennoch ist es ein wahres Paradoxon in der Industrie so schwer ist es, ohne sie auszukommen: Die Beteiligten sind oft externe Dienstleister, die keinen Zugang zum Netzwerk haben, und so werden USB-Medien für die Integratoren unentbehrlich. *„Man geht lieber das Risiko ein, USB-Sticks zu verwenden, als das Risiko, die Produktion zu unterbrechen"*, sagt Thierry Hernandez, Global Account Manager bei Stormshield. Um den Einsatz dieser Tools so sicher wie möglich zu gestalten, müssen sie im Vorfeld kontrolliert werden, was in der Regel mithilfe von weißen Stationen geschieht.

Schließlich sind wissentlich bösartige Angriffe (APT im Fachjargon für Advanced Persistent Threat), seltener. Sie sind jedoch vorhanden und werden von der Industrie nur schwer in Betracht gezogen. **Vincent Nicaise**, Leiter der Abteilung für Industriepartnerschaften und Ökosystem, erklärt dies damit, dass man sich der Verwundbarkeit dieser Netzwerke erst später bewusst wurde. *„Cybersicherheit in der IT gibt es seit dem Aufkommen des Internets. Bei den OT-Netzwerken ist es gerade einmal ein Jahrzehnt her, dass man sich darüber Sorgen gemacht hat"*, fasst er zusammen. *Seit 2010 gab es einige große Angriffe,*

die Industrieanlagen, aber auch kritische Infrastrukturen, Urananreicherungsanlagen oder auch Elektrizitätswerke betrafen. Manchmal sogar, ohne dass diese mit dem Internet verbunden sind. Das Bewusstsein für die Gefahr für industrielle Systeme entstand erst im Nachhinein. Und die Reife der Akteure und Entscheidungsträger in diesem Bereich hat sich seither deutlich weiterentwickelt".

Ob durch Nachlässigkeit oder böswillige Angriffe, derselbe Bericht von Honeywell betont, dass **79 % der Bedrohungen wahrscheinlich kritische Auswirkungen auf die Systeme der Betriebstechnologie haben werden**. Daher ist es dringend notwendig, diese kritischen Systeme zu schützen.

DER BESONDERE ANSATZ DER CYBER-SICHERHEIT FÜR DIE INDUSTRIE

Und um diese OT-Netzwerke zu schützen, ist es unmöglich, die gleichen Lösungen und Techniken wie in der IT zu kopieren und einzufügen. Denn im Bereich der Cybersicherheit unterscheiden sich die Ansätze von IT und OT.

„In einigen Produktionslinien, die vor 20 Jahren installiert wurden, gab es natürlich keine Cybersicherheit."

Vincent Nicaise, Manager für Industriepartnerschaften und Ökosystem Stormshield

Erstens: Während IT-seitige Informatik flexibel und reaktionsschnell ist, geht **die industrielle Informatik von viel längeren Zeiträumen aus**. So wird ein IT-Park etwa alle fünf Jahre ausgetauscht, sagt Vincent Nicaise, während die Betriebstechnologie bis zu 40 Jahre lang halten kann. *„Bei einigen Produktionslinien, die vor 20 Jahren installiert wurden, gab es natürlich keine Cybersicherheit." Und in den Lastenheften für Bauwerke fand man keine Zeile zu diesem Thema, das mehrere Millionen Euro kostet*", betont er. Ein **zeitlicher Unterschied**, der sowohl für die Hardware als auch für die Software gilt. So wird das Informationssystem regelmäßig aktualisiert, um das neueste verfügbare Betriebssystem zu verwenden. Auf der anderen Seite wird es nicht immer ratsam sein, die Software der Betriebstechnologie auf den neuesten Stand zu bringen, da die Hardware nicht unbedingt an neue Softwareversionen angepasst wird. Während die Sicherheitswartung (Safety Maintenance, SM) und die Betriebswartung (Operational Maintenance, OM) in der IT miteinander vereinbar sind, ist dies bei der OT nicht der Fall: *„SM kann OM schaden*", fasst Thierry Hernandez zusammen.

Auch die Umwelt ist ein großer Unterschied in den Ansätzen, da die Umwelt der EO weniger beherrscht wird. Zunächst am Standort: IT-Assets befinden sich in der Regel an Orten wie Geschäftsräumen oder Serverräumen, wo die Zugangskontrolle einfach ist. OT-Assets wiederum können sich in weniger kontrollierbaren Umgebungen befinden, z. B. in einem Straßenschrank oder im Herzen eines Wasserturms in der Wildnis. Andererseits sind diese Technologien oft unangenehmen Bedingungen ausgesetzt: Staub, Feuchtigkeit, extreme Temperaturen, Vibrationen etc. *„Eine klassische Firewall kann nicht bei -40 Grad funktionieren, da braucht es gehärtete Geräte*", erklärt Vincent Nicaise. Die Installation von Cybersicherheitstechnologien ist daher eine erste Schwierigkeit, während die Zugangskontrolle für physische Wartungsarbeiten eine andere ist ...

Schließlich **unterscheiden sich auch die Prioritäten bei der Cybersicherheit**. Vincent Nicaise schematisiert dies mit zwei Pyramiden. Die erste, die der IT, präsentiert an der Spitze die Vertraulichkeit – über diese Netzwerke werden viele sensible Daten transportiert, die es zu schützen gilt. Zweitens die Integrität: Sicherstellen, dass die empfangene Information dieselbe ist wie die gesendete Information. Schließlich die Verfügbarkeit: Sicherstellung der Kontinuität des Dienstes. Für die OT sind die Prioritäten umgekehrt, demonstriert er. **Die Verfügbarkeit ist der Kardinalwert: Es gibt Fälle, in denen es unmöglich ist, eine Produktionslinie anzuhalten**. „*Um zum Beispiel in unseren Häusern über Strom verfügen zu können, muss der Energietransport rund um die Uhr gewährleistet sein*", veranschaulicht der Experte. *Ebenso muss eine Trinkwasseraufbereitungsanlage in der Lage sein, die Bevölkerung mit Wasser zu versorgen, ohne dass die Versorgung unterbrochen wird*". Die Integrität steht an zweiter Stelle der Prioritätenliste, da es sich lohnt, darauf zu achten, dass die Werte des Befehls nicht verändert werden. „*Im Jahr 2021 wurde eine Wasseraufbereitungsanlage in Florida Opfer eines Cyberangriffs, der darauf abzielte, die Konzentration von Natriumhydroxid zu erhöhen. Der böswillige Akt wurde schnell erkannt, aber die potenziellen katastrophalen Folgen sind leicht vorstellbar*." Und bei den operativen Technologien steht der Datenschutz am Ende der Rangliste. Der Grund? „*Sehr oft sind die Daten nicht vertraulich*", sagt Vincent Nicaise.

Und wenn Sie den Ansatz einmal verinnerlicht haben, wie können Sie eine Baustelle für die Cyber-Sicherheit für die Industrie einrichten?

DIE EINFÜHRUNG DER CYBER-SICHERHEIT FÜR DIE INDUSTRIE

Zwar können die mit einem Angriff verbundenen Risiken eine gewisse Panik auslösen, aber Panikmache ist nicht angebracht, sind sich die beiden Experten einig. „*Es muss ein Bewusstsein dafür geschaffen werden, dass man seine Cybersicherheit organisieren kann. Man kann mit den wirklich kritischen Punkten beginnen und im Laufe der Zeit abwickeln*", empfiehlt Vincent Nicaise. Dazu führen Experten für Cybersicherheit eine Risikoanalyse durch. Wie im Fall der IT besteht sie darin, die Risiken, ihre Kritikalität und ihre Wahrscheinlichkeiten zu identifizieren, um zu entscheiden, wo gehandelt werden soll. „*Zum Beispiel kann man vernetzte Objekte haben, denen es an Sicherheit mangelt, die aber nicht in der Lage sind, großen Schaden anzurichten. Ist dies eine Priorität?*", fragt Vincent Nicaise.

Die Einrichtung kompatibler Firewalls zur Kontrolle der betrieblichen Abläufe wird häufig empfohlen, ebenso wie der Schutz von Arbeitsplätzen, um anormale Aktionen zu erkennen und zu blockieren. Dann können einfache Mechanismen eingesetzt werden, wie die Einrichtung einer Netzwerksegmentierung, einer DMZ (*demilitarisierten Zone*) für IT/OT-Zonen oder auch einer Abschottung. Und um noch einen Schritt weiter zu gehen, können Integratoren den Datenfluss zwischen den Geräten analysieren, um zu definieren, ob sie miteinander kommunizieren dürfen. Aber das Hinzufügen von Lösungen – Firewall, Überwachung von Automaten, Netzwerkstationen – kann zu einem vorübergehenden Verlust der Übersichtlichkeit führen, der die Industrieunternehmen zurückschrecken lässt. Thierry Hernandez sagte: „*Die Industrie muss beruhigt werden. Unsere Produkte sind für die Industrie gedacht und nicht-intrusiv*", d. h. sie sind so konzipiert, dass sie im täglichen Produktionsbetrieb kein Hindernis darstellen.

Letztlich ist es die Wahrnehmung der Cybersicherheit von Produktionsmitteln, die sich ändern muss. Einige Unternehmen sind sich der Herausforderungen des Schutzes ihrer OTs bewusst geworden, manchmal geleitet von staatlichen Richtlinien. Dies gilt insbesondere für die lebenswichtigen Betriebe in Frankreich, wie z. B. die Bereiche Transport, Energie, Wasser oder Seveso-Standorte, die mit einem Risiko schwerer Unfälle behaftet sind. In der verarbeitenden Industrie ist das Thema jedoch noch marginal. *„Aus der Sicht des Industriellen ist der unmittelbare Gewinn nicht klar*", sagt Thierry Hernandez. *Er wird Tools bevorzugen, die die Produktion verbessern. Wenn er sich aber bewusst wird, dass seine Produktion bei einem Angriff ausfallen kann, dann wird er von einer Rendite überzeugt sein*." Im Bereich der Cyber-Sicherheit für die Industrie wie auch anderswo gilt: Vorbeugen ist immer besser als heilen.

STORMSHIELD

Stormshield, eine hundertprozentige Tochtergesellschaft von Airbus CyberSecurity, bietet innovative End-to-End-Sicherheitslösungen zum Schutz von Netzwerken (Stormshield Network Security), Desktops (Stormshield Endpoint Security) und Daten (Stormshield Data Security). **www.stormshield.com**

Version 1.1 - Copyright Stormshield 2022