STORMSHIELD

MEINUNGEN

WELCHE ART VON CYBERSICHERHEIT BENÖTIGEN INDUSTRIELLE SYSTEME IM ZEITALTER DER INDUSTRIE 4.0?

Khobeib Ben Boubaker
Head of Industrial Security Business Line, Stormshield

Die Industrie 4.0 ist auf dem Vormarsch und mit ihr eine Reihe von Bedrohungen – aber auch einige Vorurteile. Wie kann man die allgemeine Sicherheit in einem Gebiet gewährleisten, das zunehmend industrielle Systeme, Internet der Dinge, Cloud und Big Data kombiniert? Spoiler: Es ist keine Frage von Sensoren.

Sie kennen sicherlich die Geschichte der vernetzten Kaffeemaschine, die ein industrielles Petrochemie-Unternehmen mit einer Ransomware infizierte. Diese Geschichte fasst die Herausforderungen beim Schutz einer zunehmend vernetzten Industrie 4.0 zusammen – nämlich die Sicherung einer wachsenden Angriffsfläche. Das ist ein bisschen so als wollte man Zugluft in einem Gebäude stoppen, in dem immer mehr Türen und Fenster geöffnet werden. Das schrittweise Hinzufügen intelligenter Sensoren und/oder Cloud-Speichern schufen neue Schnittstellen mit der Außenwelt. So viele mögliche Schwachstellen in einem industriellen Sektor, der bereits stark im Visier von Cyberangriffen steht und der auch vor internen Missgeschicken nicht sicher ist.

TECHNOLOGISCHE VIELSCHICHTIGKEIT

Konkret gesagt setzen sich industrielle Systeme aus Ausrüstung vor Ort zusammen (Motoren, Ventile... und Sensoren), die von Kontrollsystemen - remote oder lokal - (SCADA Maschinen und Anwendungen) und von Informationssystemen (für die Datenanalyse) gesteuert werden. *„Was man heute Industrie 4.0 nennt ist vor allem ein Konzept rund um die Digitalisierung einer Industrie zur kontinuierlichen Verbesserung*", betont **Thierry Hernandez**, Account Manager Stormshield und Industrieexperte. *„Dieses Konzept beruht auf mehreren Elementen wie der Entwicklung von Tools (Robotik, AGV, Augmented Reality Software, etc.) und Technologien (Telekommunikationsprotokolle, Sensoren und vernetzte Objekte zum Senden von Daten). Und bei alledem werden die verschiedenen Teile des Werks miteinander verbunden. Das Ziel ist also, Daten an eine Cloud oder ein Edge Computing zu senden, die algorithmusbasierte Lösungen mit hoher Rechenkapazität auf dem neusten Stand hosten. Die Hauptrollen des Konzepts sind dabei operationale Exzellenz durch Energieeffizienz, Zeitersparnis und gesenkter Rohstoffverbrauch oder auch vorausschauende Wartung.*"

Produktion wird also optimiert, flexibel und flüssiger. Dank der vorausschauenden Wartung können sogar Ausfälle antizipiert werden, um so einen konstanten Workflow zu garantieren.

„Einfach ausgedrückt ist die Produktion in vier Stufen organisiert", erklärt Thierry Hernandez. *„Das erste Layer sind die Automaten, die alle Aktoren und Ventile steuern. Das zweite ist SCADA (die Überwachungs- und Erfassungssoftware, die sich auf die gesammelten Daten stützt, um sicherzustellen, dass alles gut läuft, dass also zum Beispiel die Tanks gefüllt sind). Das dritte Layer besteht aus der MES-Steuerung, die die Produktionsüberwachung und die Planung verwaltet. Das vierte und letzte Layer ist das ERP, das vor allem die Herstellungsbefehle auslöst.*" Diese Softwarepakete erlauben es, die Gesamtheit der Unternehmensprozesse zu steuern, und machen sie dadurch zu einem wesentlichen Bestandteil – der in der globalen Cyber-Schutz-Strategie nicht vergessen werden sollte.

Fügt man dem Ganzen noch eine Cloud und 5G hinzu, merkt man schnell, dass das Werk 4.0 eine technologische Vielschichtigkeit mit komplexer Architektur ist, das nach seinen ganz eigenen Regeln funktioniert.

INDUSTRIELLE CYBERSICHERHEIT GEBRAUCHT

Auch wenn die Cybersicherheit für industrielle Systeme gerade im Aufbau ist, muss man sich mit bestimmten Altlasten beschäftigen. Und darin liegt möglicherweise das Problem. *„In Frankreich besteht ein industrielles System im Schnitt etwa 15 Jahre. Das entspricht dem Durchschnittsalter des Maschinenparks bei Fertigungsgeräten. Bei Zügen und U-Bahnen haben diese Systeme eine Lebensdauer von 30 bis 40 Jahren. Sieht man sich noch komplexere Systeme an wie Nukleareinrichtung dann ist man bei einer Lebensdauer von 60 Jahren. Diese häufig sehr alten Systeme sind zwangsläufig angreifbar.*", merkt **Jean-Christophe Mathieu**, Head of Cybersecurity Orange Cyberdefense, an.

„Historisch gesehen wurden diese Infrastrukturen oft auf gut Glück errichtet. Das bedeutet, dass man sie nach und nach gemäß den Bedürfnissen konzipiert und automatisiert hat und dabei Verkabelungen wie man wollte (oder konnte) durchgeführt hat.", erklärt **Stéphane Prévost**, Product Marketing Manager Stormshield. „*Infolgedessen wurden alle diese automatisierten Systeme in einem flachen Netzwerk platziert. Um sie heute zu sichern, muss man sie segmentieren.*" Die Segmentierung des Informationssystems erweist sich somit als eine Technik, um die kritischsten Werte von den übrigen zu isolieren und sie zu schützen. Folgen: abgewehrte Cyber-Bedrohungen, aber auch optimierte Geräteleistung. Da sich mehr und mehr Sensoren, Maschinen und Abläufe in Fabriken miteinander verbinden, ist die Segmentierung ein wesentliches Abwehrsystem der Industrie 4.0.

„OT FIRST"-ANSATZ

Die Problematiken 4.0 werden nicht mehr ausschließlich durch das Werkspersonal betreut. Für eine gelungene IT/OT-Konvergenz sollte man für eine gute Mischung von Beidem sorgen. Und diese zwei Welten müssen lernen, sich zu verstehen. „*Wir stellen fest, dass in vielen Unternehmen die IT- und OT-Teams Schwierigkeiten damit haben, sich auszutauschen. Die kulturellen Unterschiede sind noch immer stark und manchmal gibt es sogar Streit über Nichtigkeiten. Allerdings können wir kein globales Sicherheitskonzept einwickeln, wenn nicht alle auch miteinander sprechen und zusammenarbeiten.*", merkt Jean-Christophe Mathieu an.

Für IT-Berufe bedeutet das, dass man an das Cyber-Thema unter Einbeziehung der OT herangehen sollte. „*Die OT will, dass es immer weiterläuft. Man muss also eine Harmonie zwischen dem Schutzsystem und der Produktions- bzw. Aktivitätskontinuität finden.*", erklärt Thierry Hernandez. Also, Ja zur Firewall, sofern sie im Werk nichts blockiert.

Anders ausgedrückt: Informationsschutz darf sich nicht negativ auf die Produktion auswirken. „*Die Sicherheit muss so gewährleistet sein, dass die Verfügbarkeit des Systems sichergestellt ist und der Betrieb weiterläuft.*", betont Stéphane Prevost. Diese Notwendigkeit führt zu einer neuen Herangehensweise und zur Entstehung der industriellen Cybersicherheit, die sich zu einer eigenen Disziplin entwickelt. Mit zunehmend spezialisierten Cyber-Akteuren, darunter Stormshield, die transparente Lösungen für das bestehende System anbieten werden. „*Diese Transparenz muss während der Integrierungsphase angewandt werden, aber auch später, um im Falle eines Geräteausfalls die Produktion nicht zu beeinträchtigen.*", erläutert Stéphane Prevost. „*Unsere industriellen Firewall-Lösungen sind alle mit mehreren Garantien für die Betriebssicherheit ausgestattet, mit Bypass- oder Safe-Mode-Funktionalität, dem Konzept der Geräte-Cluster oder redundanten Stromversorgungen.*"

CLOUD UND EDGE COMPUTING - NEUE HERAUSFORDERUNGEN EINER GLOBALEN SICHERHEIT

Die Weiterleitung von Daten ist ein wichtiger Bestandteil der Industrie 4.0. „*Die Informationen müssen mit perfekter Integrität von den Steuergeräten und Sensoren ankommen und schnell an das ERP und die Cloud übermittelt werden können.*", betont Thierry Hernandez. „*Der Schutz des untersten Layer des Betriebsnetzes ist ein erstes Ziel, das es ermöglicht, die Informationen, die oben verwertet werden, an der Quelle zu sichern.*"

Ganz zu schweigen von den Anwendungen und Informationen, die das IoT durchlaufen. „*Edge Computing, einschließlich allem, was mit der Berechnung des Energieverbrauchs zu tun hat, ist sehr nah am Betriebsnetz, das wiederum direkt mit den Cloud-Infrastrukturen verbunden ist.*", betont Stéphane Prevost. „*Dies trägt zur Interkonnektivität bei und macht das operative System anfälliger für Cyber-Bedrohungen.*"

Die Industrie 4.0 braucht also eine globale Sicherheitsstrategie. Identifikation und Mapping sensibler Assets, Segmentierung (oder sogar Mikrosegmentierung für IIoT), um Teile voneinander zu isolieren und die Ausbreitung eines Angriffs zu verhindern, Absicherung von Steuergeräten und Kontrollpunkten... Industrielle Cybersicherheit scheint allmählich ausgereift. Doch das bedeutet für Jean-Christophe Mathieu, dass man sehr gut organisiert sein muss. „*Wir müssen wissen wer was, wann, wie macht, und wir müssen es rückverfolgen können. Um zu verhindern, dass Dritte in die unmittelbare Umgebung des Systems gelangen. Oder dass, wenn es doch jemand schafft, wir in der Lage sind, genau zu wissen, was er getan hat.*"

Und die Sicherheitslösungen, die in den Fabriken eingesetzt werden, müssen mithalten können. „*Bei Stormshield gehen wir sogar so weit, dass wir die Nachrichten kontrollieren, die von den Steuerungs- und Regelungssystemen an die Maschinen übertragen werden.*", erklärt Stéphane Prévost. „*Wenn eine Engineering-Stelle eine Parameteränderung an eine SPS sendet, muss sichergestellt sein, dass es die richtige Engineering-Stelle mit der richtigen Person ist, die einen Befehl sendet, der berechtigt ist.*" Diese Nachrichtensteuerung stellt auch sicher, dass die an die SPS übertragenen Werte mit dem Geschäftsprozess konsistent sind. „*Wir sind in der Lage sicherzustellen, dass ein Wert einen bestimmten Punkt nicht überschreitet, um ein Gerät oder sogar die gesamte Produktionsanlage nicht zu gefährden.*"

DIE INDUSTRIE ALS HAUPTZIEL BETRÜGERISCHER ANGRIFFE

Wie so oft in der Cybersicherheit sind Standards ein wichtiger Leitfaden für den Einsatz von Schutzsystemen. Bei industriellen Systemen dient der Standard IEC 62443als Referenz. Jeder Sektor setzt sich dann entsprechend seiner Besonderheiten zusammen, insbesondere die als Akteure von entscheidender Bedeutung, Betreiber wesentlicher Dienste oder SEVESO klassifizierten Branchen, die ein sehr hohes Maß an Sicherheit erfordern. Clusif, eine französische Vereinigung von Anwendern von Informationssystemen, hat eine Übersicht über Normen und Standards für die Cybersicherheit von Industriesystemen erstellt. Sie haben über 50 Stück erfasst.

Trotz dieser Standards sind industrielle Systeme verwundbar. Insbesondere deshalb, weil die materiellen Geräte (SPS, Steuerungen, Regler usw.), ob vernetzt oder nicht, für sehr unterschiedliche Einsatzgebiete verwendet werden und das Herzstück vieler Systeme sind. So finden wir zum Beispiel dieselbe Art von programmierbaren Steuerungen für das Management eines Gebäudes (Heizung, Lüftung, Klimaanlage) auch an einer Produktionslinie, die beispielsweise ein Auto herstellt. Sobald eine Sicherheitslücke bei einem dieser weit verbreiteten Geräte entdeckt wird, sind daher alle diese Systeme gefährdet. *„Es gibt viele Ähnlichkeiten zwischen den Branchen.“*, merkt Thierry Hernandez an. *„Wir können einen Player in der Kosmetik mit einem in der Pharmazie vergleichen, weil Infrastrukturen und Architekturen einander ähneln können. Aber der Sicherheitsstandard wird von der jeweiligen Unternehmensführung abhängen.“* Also **von einem gewissen Wissen über Cyber-Bedrohungen**.

Und diese Bedrohungen sind real. Neben Datendiebstahl und Industriespionage haben es Hacker mittlerweile sogar auf SPS und Sicherheitssteuerungen abgesehen und bedrohen den Produktionsapparat mit Ransomware. Auf das Risiko hin, Katastrophen auszulösen, wie z.B. einen Betriebsstörfall oder einen Produktionsstillstand, die als die schädlichsten Risiken gelten. *„Unabhängig von den Folgen einer böswilligen Handlung oder eines internen Fehlers ist die größte Bedrohung ein Produktionsausfall. Das hat enorme wirtschaftliche Konsequenzen.“*, sagt Hernandez. Die Reederei AP Moller-Maersk zum Beispiel hat die Kosten für die Cyberangriffe, die sie 2017 erlitten hat, auf 300 Millionen Dollar geschätzt.

Angriffe können auf zunehmend komplexe, große und vernetzte Lieferketten abzielen. Ein von einem Cyber-Kriminellen „umparametrierter“ Sensor könnte zum Beispiel eine größere Ventilöffnung als erlaubt hinterlassen. Bei einem Wasserturm könnte dies die Überflutung eines ganzen Gebietes bedeuten. Oder eine schwere Betriebsstörung verursachen. Im November 2020 formulierte ein israelischer Forscher sogar ein Szenario, in dem es möglich wäre, aus einem Computervirus einen biologischen Virus zu erzeugen. Gänsehaut vorprogrammiert.

Wie wir sehen konnten sind IIoT-Lösungen und industrielle Systeme kaum darauf vorbereitet, in einem vernetzten Umfeld - und somit unter höherer Anfälligkeit für Cyberangriffe - zu arbeiten. Die Informationen, die diese vernetzten Geräte sammeln

und weiterleiten, dürfen nicht in direkter Interaktion mit dem Kern des Systems stehen. „*Wenn doch, müssen sie ausreichend und zielgerichtet gefiltert werden, damit sie nur nach außen, also zu den vernetzten Geräten, gehen und nicht zum Kern des Systems.*“, warnt Jean-Christophe Mathieu. *Es ist wichtig, den Kern des Systems vom Rest zu isolieren.*“ Und die Beherrschung der gesamten Architektur, von A bis Z.