STORMSHIELD

MEINUNGEN

WIE KANN DIE SICHERHEIT INDUSTRIELLER PROTOKOLLE KONTROLLIERT WERDEN?

Marco Genovese
PreSales Engineer,
Stormshield

Kommunizieren, informieren, bestellen usw. In der industriellen Welt haben Automaten ihre eigene Sprache, um die gesamte betriebliche Infrastruktur zu kommunizieren und zu betreiben. In diesem Fall spricht man von industriellen Kommunikationsprotokollen. Ein lexikalisches Feld, das seine semantischen Grundlagen auf die Begriffe Sicherheit, Effizienz, Produktivität und seit dem Cyberangriff von Stuxnet auf Cybersicherheit gelegt hat. Ein Vorfall, der die industrielle Welt dazu zwang, sich der Schwachstellen industrieller Kontrollsysteme bewusst zu werden. Und schnell noch auf den bereits fahrenden Cyberzug aufzuspringen.

STUXNET SCHLUG VOR ZEHN JAHREN ZU

Kehren wir zurück in den Iran des Jahres 2010: Dieser Computerwurm zielte direkt auf die speicherprogrammierbaren Steuerungen (SPS) ab, die die Urananreicherungszentrifugen kontrollierten. Anschließend untergrub er die nukleare Infrastruktur, indem er den Betrieb von Zentrifugen störte, und er ermöglichte es vor allem dem Industriesektor, sich der Schwachstellen von Steuerungssystemen und der Notwendigkeit bewusst zu werden, Sicherheitslösungen zu industriellen Kommunikationsprotokollen hinzuzufügen.

Der Sektor war sich der Lücke bewusst, die zwischen diesen vor Jahrzehnten entwickelten Formaten für den Datenaustausch zwischen Automaten und **der Realität einer zunehmend vernetzten Welt** bestand. Da Cybersicherheit bisher kein Problem darstellte, boten nur wenige Industrieprotokolle von Haus aus Sicherheitsmechanismen an. Und das ist immer noch der Fall.

Die Angriffe von BlackEnergy und Industroyer, die speziell darauf ausgelegt sind, das Funktionieren der Stromnetze in der Ukraine zu stören, spielen bei dieser Art von Cyber-Methode eine herausragende Rolle. Wasserverschmutzung, Bruch von Rohrleitungen, Explosionen oder sogar physische Schäden, die katastrophalen Szenarien sind vielfältig. „*Industrielle Automaten sind miteinander verbunden und kommunizieren miteinander – ebenso wie mit der Überwachungsstation – über für diese Umgebungen spezifische Industrieprotokolle*“, erklärt **Vincent Nicaise**, Industrial Partnership and Ecosystem Manager bei Stormshield. „*Diese Form der Sprache hat große Auswirkungen auf die reale Welt, da sie die Steuerung physischer Systeme ermöglicht. Zum Beispiel das Betreiben eines Tankablassventils, das Umschalten einer roten Verkehrsampel auf Grün oder sogar die Steuerung des Heizraums eines Gebäudes. Da der Grad der Kritikalität dieser Kommunikation sehr hoch ist, ist es unabdingbar, eine Ebene der Cybersicherheit hinzuzufügen, um die Legitimität des Austauschs sicherzustellen*“. Aber ist das so einfach?

INDUSTRIELLE CYBERSICHERHEIT, DIE SICH AN DER ZEITLICHKEIT DER OT-GERÄTE STÖSST

Selbst nach dem Stuxnet-Vorfall **integrieren die meisten Industrieprotokolle keine Dimension für Cybersicherheit in ihren Betrieb.** Sie stellen auch keine Authentifizierungs- oder Verschlüsselungsmechanismen bereit. Eine Situation, die umso prekärer ist, als die OT-Geräte, die dies erfordern, einen viel längeren Lebenszyklus haben als die IT-Geräte. Das Cyber-Risiko vervielfacht sich daher über den Zeitraum ... Dies gilt insbesondere für die bekanntesten Protokolle wie Modbus, Profinet, BACnet (spezifisch für Technische Gebäudeverwaltung-Zentralisierte technische Verwaltung), IEC 60870-5-104 oder sogar DNP3 (spezifisch für elektrische Verteilernetze). In den letzten Jahren wurden einige Vorschläge gemacht, um die Sicherheit einiger dieser Industrieprotokolle zu verbessern.

„In den meisten Fällen garantierte jedoch keine dieser Lösungen ein akzeptables Sicherheitsniveau“, erklärt Vincent Nicaise. *„Hauptsächlich, weil die Anbieter von Automatisierungsgeräten diese ohne Kenntnis oder Erfahrung von Cyber-Risiken entwickelt hatten. Noch heute können sichere Protokolle an den Fingern einer Hand gezählt werden.“*

Es besteht ein mangelndes Bewusstsein für die Risiken, das mit hartnäckigen Missverständnissen einhergeht. Der Hauptgrund ist, dass die Industrie sich als immun gegen böswillige Handlungen ansieht, wenn sie proprietäre Protokolle und Datenbanken verwenden. Auch wenn proprietäre Lösungen einige von ihnen beruhigen können, so waren sie doch möglicherweise auch kein Gegenstand einer Sicherheitsanalyse. Alles hier hängt in Wirklichkeit von der Aufmerksamkeit ab, die der Entwickler der Sicherheit dieser Lösung rund um Codeprüfung, Sicherheitsanalyse usw. widmet. In einem Sektor, der historisch gesehen wenig empfindlich gegenüber der Cyber-Bedrohung ist, ist der Zweifel im Gegenteil berechtigt. Darüber hinaus sollte berücksichtigt werden, dass, wenn ein Protokoll nicht anfällig ist, die gesamte zugrunde liegende Kette des Protokolls das hingegen sehr wohl sein kann. Nehmen wir zum Beispiel das OPC UA-Protokoll, das die Dimensionen des Schutzes durch Signatur und Verschlüsselung einführt. Da es selbst auf dem TCP-Transportprotokoll basiert, ist es anfällig für TCP-, IP- und Ethernet-Angriffe. Zwischen dem Schutz isolierter industrieller Netzwerke oder den mit Sicherheitsmechanismen unvereinbaren Reaktionszeitbeschränkungen existieren viele weitere Mythen in Bezug auf industrielle Systeme.

ES IST WICHTIG, DASS SIE IHREN MASCHINENBESTAND GUT KENNEN

„Die meisten Industriellen können die Protokolle sehen, die ihre Geräte verwenden, aber sie haben keine detaillierten Kenntnisse über alle Austausche, die um sie herum existieren können: Welche Automaten kommunizieren miteinander und mit welchem Aktuator, welchem Sensor usw. Es ist wichtig, dass Sie die physische und logische Zuordnung Ihres Netzwerks kennen. Schließlich müssen wir in der Lage sein, diese Informationen regelmäßig zu überwachen und zu aktualisieren, da sich die Infrastrukturen im Laufe der Zeit ändern“, erklärt **Simon Dansette,** Product Manager bei Stormshield. Die Netzwerksonde kann auf diese Anforderung reagieren: Sie überwacht das Netzwerk, analysiert die Protokolle und Kommunikationsflüsse und ermöglicht die Zuordnung dieser Flussmatrix der Installation. Ihre Wirkung ist jedoch begrenzt, da es keinen Mechanismus gibt, der die Flüsse blockieren oder als infiziert identifizierte Geräte isolieren könnte. *„Diese Lösung ist nur nützlich, um die Sichtbarkeit zusätzlich zur industriellen Firewall zu erhöhen, da sie unter keinen Umständen den Datenfluss durch Blockieren böswilliger Aktionen sichert“*, erklärt Simon Dansette.

Darüber hinaus ist es unabdingbar zu verstehen, wie industrielle Prozesse funktionieren. Die meisten OT-Schulungen für IT-Experten beschränken sich leider auf HMI-Kenntnisse (Human-Machine Interface) und SPS-Konfiguration. Es ist jedoch unabdingbar zu wissen,

welche Industrieprotokolle zum Transportieren einer Bestellung oder zum Aktivieren eines Dienstes verwendet werden und welche Art von Anomalien im Netzwerk auftreten kann. Weil die Cyber-Experten, die für die Sicherung von OT-Netzwerken verantwortlich sind, benachteiligt sind – da sie die industrielle Umgebung, ihren Betrieb oder sogar ihre betrieblichen Einschränkungen nicht kennen. Diese Mängel im Zusammenhang mit der Konvergenz von IT- und OT-Welt scheinen uns auf die Kluft zwischen VOIP (Voice over IP) und traditioneller Telefonie vor 20 Jahren zurückzubringen. Damals gab es zwei Welten: die der Netzwerkexperten und die der Telefonieexperten. Jeder ignorierte die Probleme der anderen. Gegenüber der Telefonkonvergenz vor zwanzig Jahren haben wir künftig einen Vorteil: die Virtualisierung. Im Zeitalter digitaler Zwillinge ist es jetzt möglich, virtuelle Repliken der Fabrik zu erstellen, um Angriffe und ihre Lösungen zu testen.

DURCHFÜHRBARE SICHERHEITSLÖSUNGEN

Glücklicherweise bieten einige Industrieprotokolle standardmäßig Sicherheitsmechanismen an. Dies ist beispielsweise bei DNPSec (sichere Version von DNP3), OPC UA (signiert/verschlüsselt), IEC 62351 oder auch CIP Security (eine Erweiterung des CIP-Protokolls) der Fall. Das Ändern der Ausrüstung zur Unterstützung dieser Protokolle ist für Hersteller jedoch zu langwierig oder zu kostspielig. Die kurzfristige Lösung besteht daher darin, ihren ungesicherten Protokollen eine Schicht industrieller Cybersicherheit hinzuzufügen.

Dafür verwendet der Sektor derzeit zwei Hauptansätze. Einerseits können die Detektionssonden einen illegitimen Fluss oder einen Prozessdrift erkennen. Wie oben erwähnt, können sie jedoch keine illegitimen Flüsse blockieren oder das System stören. Andererseits ist der andere Ansatz die **Verwendung von industriellen Firewalls**. In der Regel basieren sie auf der Signaturerkennungstechnologie und ermöglichen es, aus einer Datenbank bekannter Malware-Signaturen, Eindringversuche in Echtzeit zu erkennen und zu blockieren. Eine Protokollanalysemethode, die auch ihre Grenzen hat: Wenn ein neuer, unbekannter Angriff auftritt, ist er daher nicht an eine Signatur gebunden und hat keine Schwierigkeiten damit, als legitimer Kommunikationsfluss durchzugehen. „*Darüber hinaus kann die Tatsache, dass eine Protokollanalyse durch Signatur angebracht wird, die Kommunikation zwischen SPS verlangsamen und den Prozess destabilisieren*“, bekräftigt Vincent Nicaise. „*Dies ist in einem industriellen System problematisch, in dem erwartet wird, dass jede gesendete Information zu einem bestimmten Zeitpunkt verarbeitet wird.*“ Zur Erinnerung: Ein industrielles Steuerungssystem, das rund fünfzig SPS integriert, generiert fast 20.000 Anfragen pro Sekunde. Und ebenso viele Antworten: Das gesamte System generiert daher insgesamt 40.000 Pakete pro Sekunde – das entspricht 40 Paketen pro Millisekunde. Daher ist es wichtig, eine geeignete industrielle Firewall-Lösung auszuwählen, um eine bestimmte Latenzzeit zu vermeiden. Eine Alternative ist dann die Verwendung eines IPS-Plugins (*Intrusion Prevention System*),

das die analysierten Daten kontextualisiert und es ermöglicht, das Industrieprotokoll und seine Spezifitäten zu identifizieren. So kann die industrielle Firewall die verwendeten Codes oder Funktionen identifizieren und passieren lassen (abhängig von der definierten Sicherheitsrichtlinie). Auf diese Weise werden die legitimen und für die Durchführung des Prozesses unbedingt erforderlichen Flüsse erkannt – und sind dann die einzigen, die wie bei einer *weißen Liste* (oder *Allow-list*) passieren können. Und um noch weiter zu gehen, kann diese Protokollanalyse mit Firewall-Regeln kombiniert werden. Ein besonders interessanter Anwendungsfall im Zusammenhang mit der Fernwartung, wo es möglich ist, die Verwendung eines bestimmten Protokolls nur einer authentifizierten Person und/oder ausschließlich während eines Zeitfensters für die Intervention zu genehmigen.

Angesichts dieses Problems *„ist es vorzuziehen, ein Intrusion Prevention-System zu wählen, das die Kommunikation gemäß dem erkannten Protokoll kontextualisiert und auf die Protokoll-Compliance-Analyse abzielt*“, verdeutlicht Vincent Nicaise. In der Tat begrenzen diese Systeme Fehlalarme, erleichtern die Verwaltung personalisierter Funktionscodes – die häufig mit Industrieprotokollen einhergehen – und gewährleisten einen globalen kontextuellen Schutz des Austauschs zwischen SPS und Kontrollstationen.

Um noch weiter zu gehen, muss eine industrielle Firewall in der Lage sein, personalisierte Signaturen (Custom patterns) zu integrieren, indem bestimmte Funktionen personalisiert und spezifiziert werden. *„Auf diese Weise kann ich bestimmen, dass die Temperatur meines Ofens niemals 500 Grad überschreiten darf, unabhängig von den Informationen, die durchgelassen werden. Das Custom pattern analysiert über die Firewall die Frames und ermöglicht die präzise Steuerung bestimmter Variablen. Wenn also die Information 'den Ofen auf 1000 Grad zu bringen' zirkuliert, wird sie blockiert und nicht verarbeitet*“, erklärt **Khobeib Ben Boubaker**, Head of Industrial Security Business Line bei Stormshield. Diese personalisierten Regeln, die der Industrie angeboten werden, ermöglichen es dann, sich vollständig an den Geschäftskontext anzupassen und die Kommunikationsflüsse im Falle einer Überschreitung eines Schwellenwerts oder nicht zuvor festgelegter Regeln noch genauer zu steuern. Ein weiterer Schritt in Richtung Cybersicherheit industrieller Systeme.

STORMSHIELD

Weltweit müssen Unternehmen, Regierungsinstitutionen und Verteidigungsbehörden die Cybersicherheit ihrer kritischen Infrastrukturen, sensiblen Daten und Betriebsumgebungen gewährleisten. Die auf höchster europäischer Ebene zertifizierten Stormshield-Technologien sind die richtige Antwort auf IT- und OT-Risiken und erlauben den Schutz der Geschäftstätigkeit. Unsere Mission: Cybersorglosigkeit für unsere Kunden, damit diese sich auf ihre Kerntätigkeiten konzentrieren können, die für das reibungslose Funktionieren von Institutionen, Wirtschaft und Dienstleistungen für die Bevölkerung so wichtig sind. Die Entscheidung für Stormshield ist eine Entscheidung für eine vertrauenswürdige Cybersicherheit in Europa. Weitere Informationen finden Sie unter www.stormshield.com.

Version 1.1 - Copyright Stormshield 2020