Risikomanagement und Früherkennung:

Unerlaubte Zugriffe im Automatisierungsnetzwerk verhindern

Der Schutz vor Cyber-Attacken, die Auswirkungen des IT-Sicherheitsgesetzes oder die unternehmerische Verantwortung für die Verfügbarkeit von echtzeitfähigen Produktionsanlagen (Automatisierungen) sind mehr denn je die aktuellen Anforderungen an die Betriebsleitung und Geschäftsführung. Ab 2017 enthält die ISO 9001 die neue Anforderung des Risikomanagements.

Von Dipl. Ing. Dieter Barelmann, VIDEC Data Engineering GmbH

IT-Security-Fachleute sind sich darüber einig, dass IT-Systeme und insbesondere Automatisierungsanlagen in der Produktion gegen die aktuellen Angriffsmethoden nicht mit traditionellen Sicherheitslösungen zu schützen sind. Die Angriffsmethoden, von denen die so genannten Advanced Persistent Threats (APT) am weitesten entwickelt sind, werden aus intelligenten Angriffsmodulen für die Schwachstellen bestimmter Zielsysteme konfektioniert. Es ist dabei weniger entscheidend, welche Unternehmen es im Detail sind, es ist relevanter, welches Land, welche Branche und welche Hersteller der IT-Systeme genutzt werden. Da die Anzahl solcher APT-Angriffe stark zunimmt, sollten Unternehmen eine Antwort auf die folgende Frage entwickeln: Wie schützt man die Leitsysteme und Automatisierungsgeräte bis in die Feldebene?

Die Leitsysteme und Automatisierungsgeräte in der Produktion sind nicht mit der klassischen IT-Infrastruktur zu vergleichen. Kernpunkt ist der Anspruch an eine sehr hohe Verfügbarkeit. Hinzu kommt, dass die Automatisierungsgeräte (speicherprogrammierbare Steuerungen, SPS) häufig einen sehr langen Einsatz in der Produktion haben. Folglich sind viele der heute gängigen Sicherheits- und Abfragemechanismen nicht enthalten und die Betriebssysteme sind vielfältig. Man hat es also mit einer sehr sensiblen Infrastruktur zu tun.

Firewall und VPN reichen nicht mehr aus!

Vorhandene IT-Sicherheitsvorkehrungen in Produktionsanlagen werden überwiegend nach dem Prinzip der Perimeter-Sicherheit mit Firewalls und VPNs realisiert. Dies bedeutet, es werden wie mit einem Zaun oder Graben einzelne Bereiche voneinander abgetrennt, die untereinander nur zulässige Kommunikationsverbindungen erlauben. Solche Sicherheitselemente, die Datenverbindungen analysieren, sie präventiv zulassen oder gegebenenfalls blockieren, sind jedoch nicht mehr ausreichend. Denn heutige Angriffsmethoden umgehen diese vermeintliche Sicherheit gezielt – zum Beispiel durch „drive by". Dabei wird der Schadcode quasi „huckepack" in zugelassenen Verbindungen mittransportiert und kann die Grenzen ungehindert passieren.

Des Weiteren besteht eine zunehmende Gefahr durch den Einsatz mobiler Endgeräte. Außerhalb des Unternehmens genutzte Laptops der Mitarbeiter und Servicetechniker sowie Smartphones und Tablets werden oft schnell und unbemerkt während der Benutzung im Internet infiziert. Mit den infizierten mobilen Endgeräten gelangen die Werkzeuge der Angreifer dann unbemerkt von den Firewalls oder innerhalb der VPNs in ihre Produktionsanlage und können sich dort unbeobachtet ausbreiten.

Überwachung mit passiven Ansatz

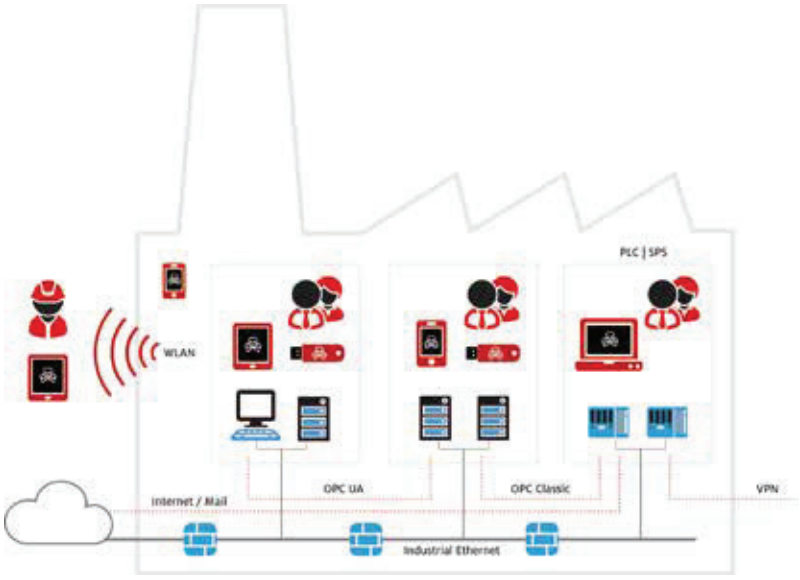
Manipulationen, Vorbereitungen oder die Durchführung von Cyberangriffen lassen sich nur durch ein kontinuierliches Monitoring der IT-Assets und Datenkommunikation in Echtzeit erkennen. Entscheidungen über die maßgeblichen Aktionen, die den Angriff stoppen und die Auswirkung entschärfen, können so verzögerungsfrei getroffen werden. Des Weiteren ist aus wirtschaftlicher Sicht zu beachten, dass für die Einrichtung keine aufwändige Konfiguration der Security-Lösung notwendig sind, sondern schon nach kurzer Zeit der automatisierten Inventarisierung der IT-Assets mit der Risikoanalyse begonnen werden kann. Eine einfache Handhabung für komplexe Thematiken ist für diese

Bereiche ein absolutes Muss, da auch der IT-Administrator einer Produktionsanlage noch kein ausgebildeter IT-Sicherheitsexperte ist. Beim Aufbau des Informationssicherheits-Managementsystems kann dann auf das Erfahrungswissen langjähriger Sicherheitsexperten mit Know-how in der Automatisierungstechnik zurückgegriffen werden.

Passives Scannen

Man kann nur schützen, was man kennt: Daher ist es notwendig, die IT-Assets und Kommunikationen aktuell zu scannen und zu dokumentieren. Jedoch: Dies muss passiv erfolgen! Profinet, ModbusTCP, EtherCAT und Co. sind spezielle Protokolle auf Basis der heute weitgehend genutzten Standardtechnologie des Industrial Ethernet für die Anforderungen der zeitkritischen Datenkommunikation in Produktionsanlagen. Jede zusätzliche Aktivität im Produktionsnetz kann diese Kommunikation stören oder Systeme zu Fehlfunktionen bis hin zum Ausfall der gesamten Produktionsanlage veranlassen. Daher ist das passive Scannen und Überwachen des Produktionsnetzes vorteilhaft. Denn die sensible Automatisierungsebene mit diversen nicht patchbaren Altsystemen verträgt keinerlei Störung durch aktive Abfragen.

Für den ordnungsgemäßen Betrieb ist die Beurteilung und das Managen von Unternehmensrisiken eine wesentliche und notwendige Aufgabe. Dies gilt insbesondere für die Automatisierung der Produktionsanlagen. Effizient auf Basis der erkannten und überwachten IT-Assets und ihrer Kommunikation, lässt sich das Risikomanagement einfach durchführen und Standard-basiert dokumentieren. Änderungen in der Automatisierung werden sofort angezeigt und das Risiko kann neu beurteilt werden. Notwendige Maßnahmen zur Risikobehandlung, zum Beispiel die Umsetzungen von Sicherheitsfunktionen oder eine Anpassung der Sicherheitssysteme, sind gezielt und wirtschaftlich durchführbar. Mit einfach zu parametrierenden Werkzeugen können die Risiken bewertet und für die ISO 9001 (2015) als haltbarer Beleg ausgewiesen werden. Die durch die Bewertung gefundenen zusätzlichen Sicherheitsmaßnahmen lassen sich somit priorisieren und ergeben für alle Beteiligten eine ergänzende Hilfe für zukünftige Investitionen. Durch die kontinuierliche Überwachung lassen sich zusätzlich Risiken durch neue oder geänderte Assets schnell und einfach in das Risikomanagement integrieren.



Etablierte Sicherheitselemente wie Antivirenschutz, Intrusion Detection oder Prevention Systeme erkennen nur bekannte traditionelle Schadsoftware wie Malware oder Trojaner.

Hinzu kommt das Erkennen von sogenannten schlafenden Verbindungen. Das sind die nicht dokumentierten Servicezugänge, die häufig über Jahre hinweg von Lieferanten genutzt wurden und teilweise noch werden. In vielen Fällen sind diese Zugänge nicht aktuell dokumentiert und haben für die Unternehmen ein nicht abschätzbares Risikopotenzial, wenn sie nicht bekannt sind und nicht überwacht werden.

Security Appliance für die Automatisierungen

Um einen wirkenden Schutz vor Cyber-Angriffen zu erhalten, sind zwei weitere Faktoren wesentlich:

Damit der Schutz schnell erreicht wird, muss die Lösung ohne aufwendige Vorab-Analysen, Konzepte und Aufwände zur Integrationen in den Betrieb einzuführen zu sein. Die „Anschaltung“ muss passiv an das vorhandene Automatisierungsnetz erfolgen, die IT-Infrastruktur muss in einem System selbstlernend identifiziert, kontinuierlich überwacht und beurteilbar sein. Auf Basis dieser Daten lässt sich die Risikoanalyse ohne Zeitverlust durch manuelle Inventarisierung unmittelbar starten.

Des Weiteren muss die Bedienung auch für Anwender ohne Vorkenntnisse möglich sein und sich in die Betriebsprozesse, zum Beispiel Leitstand und Alarmmanagement, integrieren.

Das „Industrie Risiko Management Automatisierung“ (IRMA) ist ein Industrie-Computer-System mit einer übersichtlichen Managementkonsole. Ohne jegliche Aktivitäten im Netzwerk der Produktionsanlage erfasst und analysiert IRMA die Systeme und Verbindungen. Durch die kontinuierliche Überwachung, Analyse und die intelligente Alarmierung bietet IRMA in Echtzeit Informationen zu Misskonfigurationen oder Cyberangriffen. Das integrierte Risikomanagement ermöglicht es, umgehend über die maßgeblichen Aktionen zu entscheiden, um einen Angriff zu stoppen oder die Auswirkung zu entschärfen. Ein integrierter Netzplan hilft dabei, dem Endanwender eine schnelle Übersicht seiner Anlage zu gewährleisten.