Stoppen und entschärfen

Cyber Security Wie kann man SCADA und Automatisierungsgeräte bis in die Feldebene schützen, wenn Firewalls und VPN nicht mehr ausreichen? Mit dem Industrie-Computersystem IRMA können Cyberangriffe schnell identifiziert und abgewehrt werden.

Dieter Barelmann*

Der Schutz vor Cyberattacken, die Umsetzung des IT-Sicherheitsgesetzes oder die unternehmerische Verantwortung für die Verfügbarkeit von Produktionsanlagen sind mehr denn je die aktuellen Anforderungen. IT-Security-Experten sind sich einig, dass IT-Systeme und insbesondere Automatisierungsanlagen in der Produktion gegen die aktuellen Angriffsmethoden nicht mit traditionellen Security-Lösungen zu schützen sind. Diese Angriffsmethoden, sogenannte Advanced Persistent Threats (APT), werden aus intelligenten Angriffsmodulen auf lohnenswerte Zielsysteme konfektioniert. Aber wie schützt man den Bereich SCADA und die Automatisierungsgeräte bis in die Feldebene? 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 Auswirkungen entschärfen, können so verzögerungsfrei getroffen werden. Des Weiteren ist es wirtschaftlich zu beachten, dass die Einrichtung keine beratungsintensiven Vorabanalysen der Infrastruktur sowie aufwändige Konfigurationen der Security-Lösung notwendig macht. Man kann aber nur schützen, was man kennt: Daher ist es wichtig, die IT-Assets und Kommunikationen aktuell zu scannen und zu dokumentieren. Jedoch: Dies muss passiv erfolgen. Profinet, Modbus TCP, Ethercat und Co. sind spezielle Protokolle auf Basis des Industrial Ethernets 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 veranlassen. Daher ist das passive Scannen und Überwachen des Produktionsnetzes wesentlich zu beachten. Für den ordnungsgemäßen Betrieb ist zudem die Beurteilung und das Managen von Unternehmensrisiken eine notwendige Aufgabe. Dies gilt insbesondere für die Automatisierung der Produktionsanlagen. Effizient auf Basis der erkannten und überwachten IT-Assets und deren Kommunikation, lässt sich das Risikomanagement einfach durchführen und dokumentieren. Änderungen in der Automatisierung werden sofort angezeigt und das Risiko kann neu

*Dieter Barelmann, Geschäftsführer, Videc Data Engineering

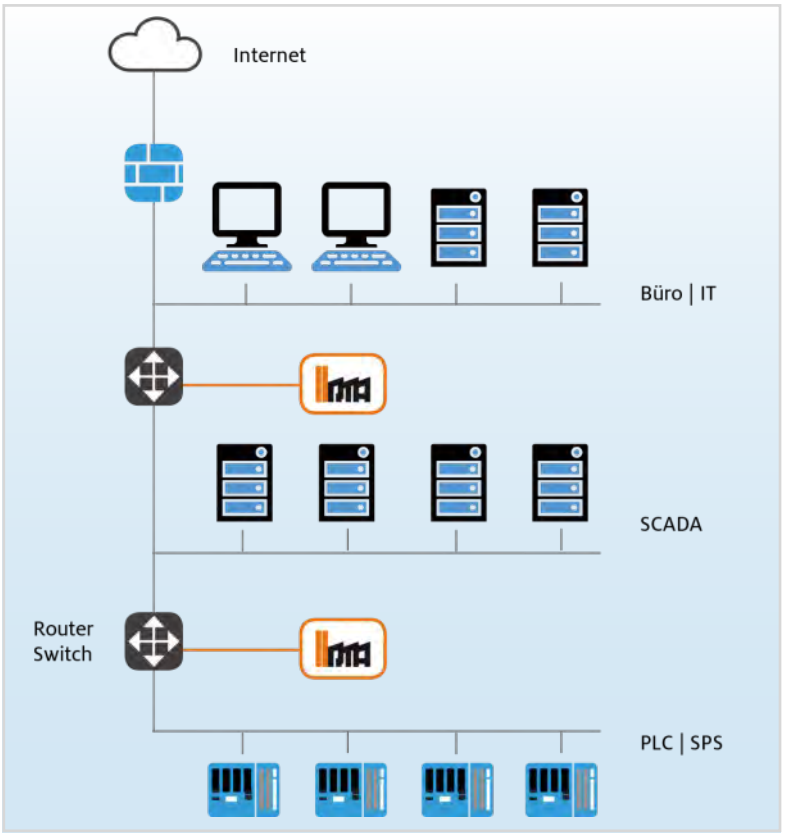

Bild: Videc

➤ **IRMA ermöglicht eine passive Anschaltung an das Automatisierungsnetz.**

beurteilt werden. Notwendige Maßnahmen, z.B. Umsetzungen von Sicherheitsfunktionen oder Anpassung der Sicherheitssysteme, sind gezielt und wirtschaftlich umsetzbar.

Security einfach und schnell integrieren

Um einen wirkenden Schutz zu bekommen, sind zwei weitere Faktoren wesentlich:

- Damit der Schutz schnell erreicht wird, muss die Lösung ohne aufwändige Vorab-Analysen, Konzepte und Aufwände in den Betrieb integrierbar sein. D.h., die Anschaltung muss passiv an das vorhandene Automatisierungsnetz erfolgen, die IT-Infrastruktur sollte selbstlernend identifizierbar, kontinuierlich überwachbar und beurteilbar sein.
- Des Weiteren sollte die Bedienung auch für Nicht-IT-Security-Fachleute möglich sein und sich in die Betriebsprozesse integrieren lassen. Also eine Übersicht zu vorhandenen, neuen und verlorenen IT-Assets und deren Kommunikationen bieten. Daraus resultieren strukturierte Informationen als Benachrichtigung oder Alarm in Folge einer Anomalie.

Firewall und VPN reichen nicht 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 – z.B. 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 mobile 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 die Produktionsanlage und können sich dort unbeobachtet ausbreiten.

Abhilfe schaffen können die IRMA-Applikationen von Videc Data Engineering. Sie überwachen momentan in Branchen wie der Wasserwirtschaft, Stadtwerken oder Offshore-Windenergie die IT-Netzwerke. Für 2018 ist von Videc eine weitere Ausweitung auf Pharma, Chemie und Logistik geplant. [kun]

Hannover Messe: Halle 7, Stand F38

IRMA

Überwachen, analysieren, alarmieren

IRMA (Industrie Risiko Management Automatisierung) ist ein Industrie-Computersystem 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.

Bild: Videc