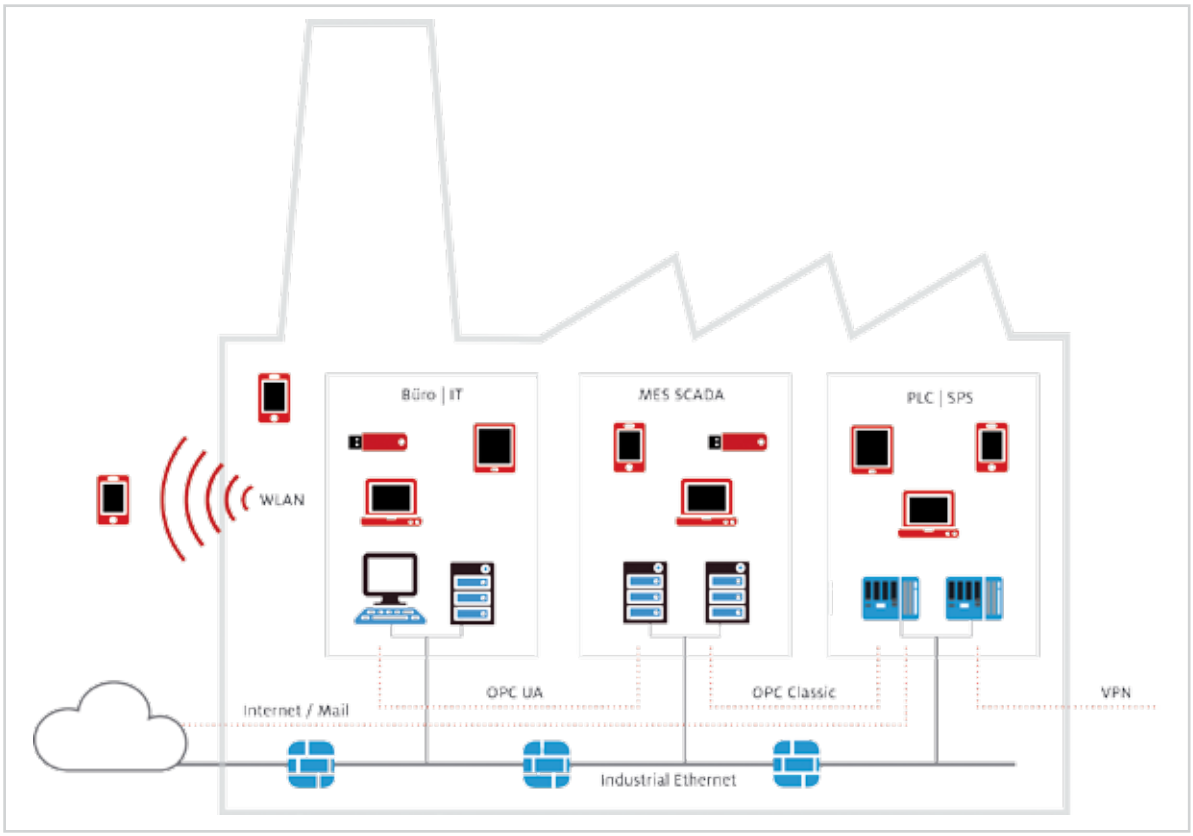
Bild: © kentoh - Fotolia

➤ Halt! Cyber-Kriminelle müssen draußen bleiben. Doch traditionelle Security-Lösungen schützen oft nicht wirkungsvoll vor neuen Angriffsmethoden.

Du kommst hier nicht rein

Security IT-Security Experten sind sich einig: IT-Systeme und Automatisierungsanlagen in der Produktion sind mit traditionellen Security-Lösungen nur noch bedingt geschützt. Denn für die neuen Vorgehensweisen heutiger Cyber-Angriffe sind diese nicht mehr ausreichend. Ein passives Monitoring soll nun Cyber-Kriminelle wirkungsvoll aussperren.
Dieter Barelmann*

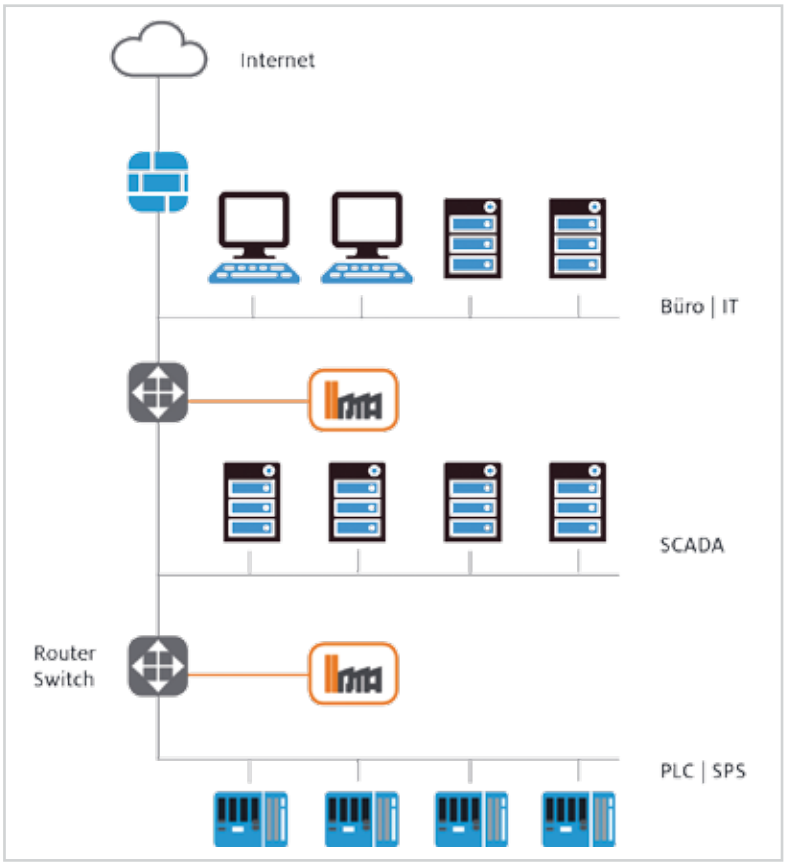
Bilder: Videc



Das Industrie-Computersystem IRMA von Videc liefert Informationen zu Cyber-Angriffen in Echtzeit – auf Basis kontinuierlicher Überwachung, Analyse und intelligenter Alarmierung.

Der Schutz vor Cyber-Attacken auf Produktionsanlagen und die Auswirkungen des IT-Sicherheitsgesetzes beschäftigen aktuell viele Betriebsleiter und Geschäftsführer. Denn nach den Einschätzungen von IT-Security Experten sind IT-Systeme und Automatisierungsanlagen vor den aktuellen Angriffsmethoden mit ihren traditionellen Security-Lösungen nicht mehr ausreichend geschützt. Etablierte Sicherheitselemente wie Antivirenschutz, Intrusion Detection oder Prevention Systeme erkennen nur bekannte, traditionelle Schadsoftware wie Malware oder Trojaner. Für die neuesten Vorgehensweisen und Technologien heutiger Cyberangriffe ist dies nicht mehr ausreichend. Dazu zählen zum Beispiel Advanced Persistent Threats (APT), also Angriffe, die mit hohem Aufwand und zielgerichtet die Standard-Schutzeinrich-

*Dieter Barelmann, Geschäftsführer, Videc Data Engineering GmbH



➤ **Das Industrie-Computersystem lernt die Produktionsnetzwerke kennen und zeigt sie übersichtlich an. Sämtliche Informationen können nahtlos im Risikomanagement genutzt werden.**

tungen umgehen und dabei meist unbekannte Schwachstellen (Zero-Day Exploits) ausnutzen. Solche Angriffe und Manipulationen können nur durch eine kontinuierliche Überwachung der Produktionsanlagen-IT entdeckt und Schäden mittels einer intelligenten Echtzeit-Analyse vermieden werden. Der Sicherheitstacho der Deutschen Telekom warnt vor zunehmenden Angriffen. So sei seit Juni 2015 ein Anstieg der Angriffe um ein 3-faches zu verzeichnen.

Passiver Schutz führt zum Ziel

Manipulationen, Vorbereitungen oder die Durchführung von Cyber-Angriffen 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 zu beachten, dass keine beratungsintensiven Vorabanalysen der Infrastruktur sowie aufwändige Konfiguration der Security-Lösung notwendig sind.

Man kann nur schützen, was man kennt: Daher ist es notwendig, die IT-Assets und Kommunikationen aktuell zu scannen und zu dokumentieren. Dies muss aber passiv erfolgen. Profinet, ModbusTCP, EtherCAT und Co sind spezielle Protokolle auf Basis des Industrial Ethernet für die Anforderungen der zeitkritischen Datenkommunikation in Produktionsanlagen. Jede zusätzliche Aktivität im Produktionsnetz kann die Kommunikation stören oder Fehlfunktionen bis hin zum Ausfall hervorrufen. Für einen störungsfreien Betrieb verträgt eine sensible Automatisierungsebene keine aktiven Abfragen, deshalb muss auf ein passives Scannen und Überwachen des Produktionsnetzes zurück gegriffen werden. Das Industrie-Computersystem IRMA (Industrie Risiko Management Automatisierung) von Videc ermöglicht eine solche störungsfreie und passive Überwachung.

Bild: Videc

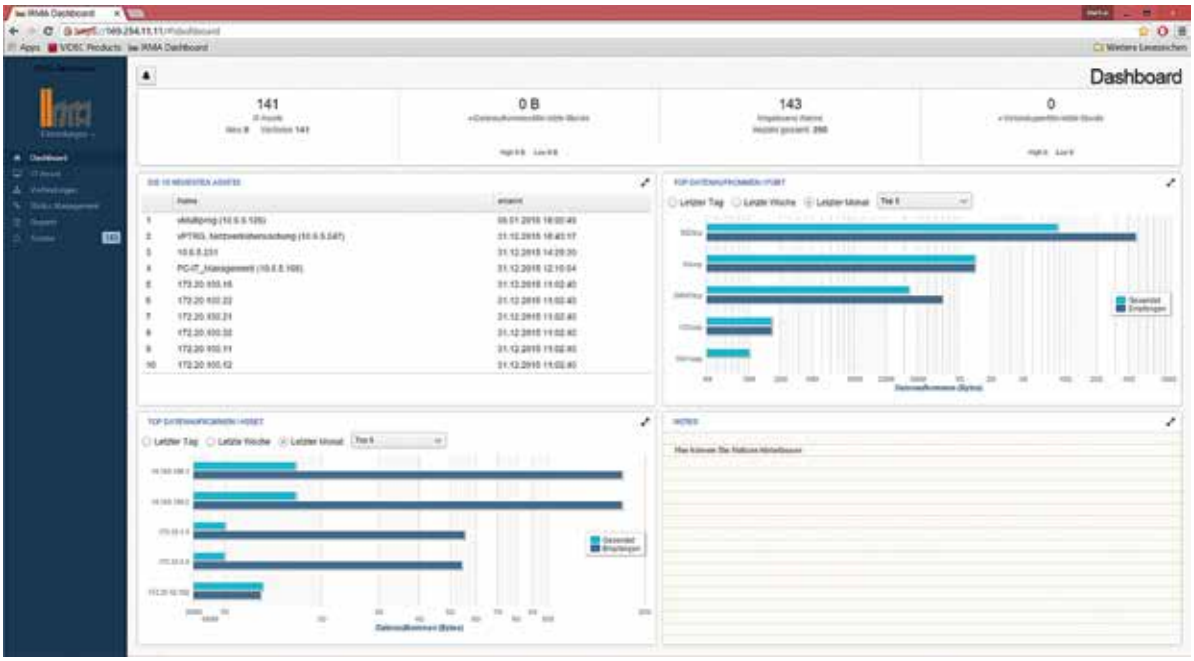
➤ **Dieter Barelmann, Geschäftsführer von Videc Data Engineering, hat sich Unterstützung und Know-how von Spezialisten ins Boot geholt.**

Man kann nur schützen, was man kennt

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. Auf Basis der erkannten und überwachten IT-Assets und deren Kommunikation lässt sich das Risikomanagement mit dem Industrie Computersystem einfach durchführen und dokumentieren. Änderungen in der Automatisierung werden sofort angezeigt und das Risiko kann neu beurteilt werden. Notwendige Maßnahmen, z. B. Umsetzungen von Sicherheitsfunktionen oder Anpassung der Sicherheitssysteme sind gezielt umsetzbar. Mit einfach zu parametrierenden Werkzeugen können die Risiken bewertet werden und für die ISO 9001 (2015) als haltbarer Beleg ausgewiesen werden. Durch die kontinuierliche Überwachung lassen sich zusätzlich neue Risiken (Assets) schnell und einfach in das Risikomanagement integrieren und geben eine zusätzliche Sicherheit, so der Anbieter. Hinzu kommt das Erkennen von sogenannten schlafenden Verbindungen. Diese sind die nicht dokumentierten Servicezugänge, die häufig über Jahre hinweg von Lieferanten genutzt werden. In vielen Fällen sind diese Zugänge nicht aktuell dokumentiert und erhöhen für die Unternehmen das Risikopotential.

Zwei Faktoren für wirkungsvolle Cyber-Security:

- Damit ein schneller Schutz erreicht wird, muss eine Security-Lösung ohne aufwändige Vorab-Analysen, Konzepte und Aufwände zur Integration auskommen. D.h. die Anschaltung muss passiv an das vorhandene Automatisierungsnetz erfolgen und die IT-Infrastruktur muss selbstlernend identifizieren, überwachen und beurteilen.
- Des Weiteren muss die Bedienung auch für Nicht-IT-Security Experten möglich und einfach sein sowie sich in die Betriebsprozesse des Unternehmens integrieren, d.h. Übersicht zu vorhandenen, neuen und verlorenen IT-Asset und deren Kommunikationen. Daraus resultieren strukturierte Informationen, die als Benachrichtigung oder Alarm in Folge einer Anomalie ausgegeben werden können.



In einem Dashboard werden übersichtlich die Analysen der Systeme und Verbindungen von IRMA ausgespielt.

„Bei der Konzeption des Produktes mussten wir neue Wege gehen. Wir haben mehrere unterschiedliche Funktionen in einem Produkt vereint und zwar so, dass sie auf Basis neuester Technologien einfach zu bedienen sind."

Dieter Barelmann, Geschäftsführer Videc Data Engineering GmbH

Schadcode passiert als Anhalt alle Grenzen

Vorhandene IT-Sicherheitsvorkehrungen in Produktionsanlagen werden überwiegend nach dem Prinzip der Perimeter-Sicherheit mit Firewalls und VPNs realisiert. Das 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.

Zudem 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 Produktionsanlagen und können sich dort unbeobachtet ausbreiten.

Cyber-Security hat Risikomanagement an Bord

IRMA ist ein Industrie-Computersystem von Videc zur Identifikation und Abwehr von Cyber-Angriffen in Produktionsnetzwerken. Das System überwacht – ohne jegliche Aktivitäten im Netzwerk – kontinuierlich Produktionsanlagen, liefert Informationen zu Cyber-Angriffen und ermöglicht die Analyse und intelligente Alarmierung mittels einer Management-Konsole. So können in Echtzeit Aktionen gestartet werden, um Cyber-Angriffe zu stoppen oder die Folgen wirkungsvoll zu entschärfen. Das integrierte Risikomanagement ermöglicht es, umgehend über die maßgeblichen Aktionen zu entscheiden. Ein integrierter Netzplan gibt dem Endanwender eine schnelle Übersicht von seiner Anlage. Basierend auf diesen Erkenntnissen lassen sich notwendige und zielgerichtete Anpassungen der Sicherheitsarchitektur im Rahmen des Sicherheitsmanagementprozesses vornehmen. Optional kann das Industrie-Computersystem IRMA Angriffsszenarien erkennen, die Alarmierung durch die Priorisierung im Risikomanagement steuern und die Anomalien der Nutzung selbstständig identifizieren. [kun]

CYBER-ATTACKEN

Sicherheitstacho der Telekom

Eine transparente Übersicht über die aktuellen Cyber-Angriffe auf DTAG-Sensoren gibt ein Gefühl für die Häufigkeit und Herkunft der Internetattacken auf ein deutsches Unternehmen. Das Portal zeigt Statistiken aus dem Frühwarnsystem der Deutschen Telekom. Die zugehörigen Sensoren werden von der Deutschen Telekom AG und Partnern betrieben. Es stehen Statistiken wie Top 15 der Ursprungsländer von Angriffen, in Angriffen genutzte Passwörter und Verteilung der Angriffsziele auf www.sicherheitstacho.eu zur Verfügung.