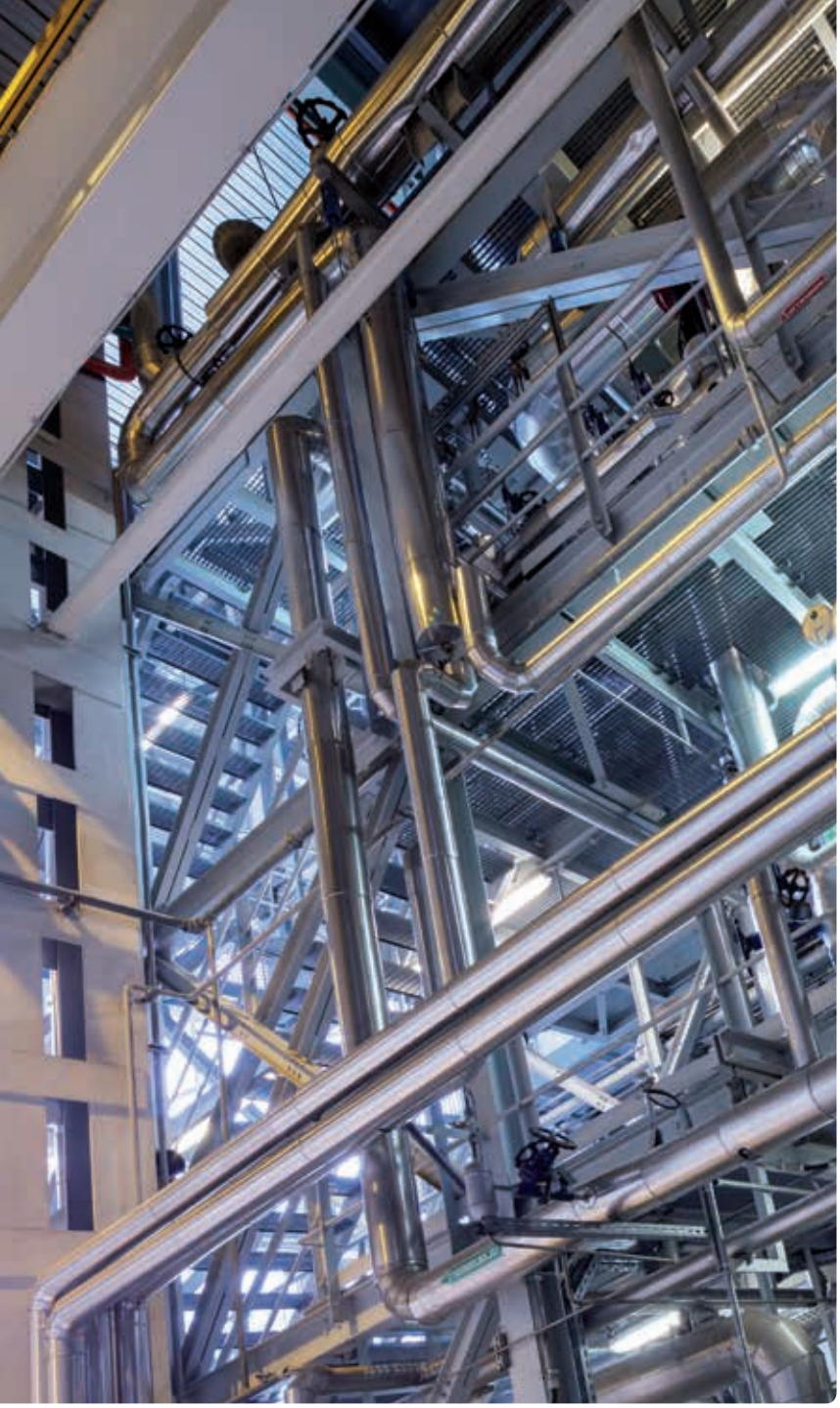


Ganzheitlicher Schutz vor Cyberangriffen in Produktionsanlagen

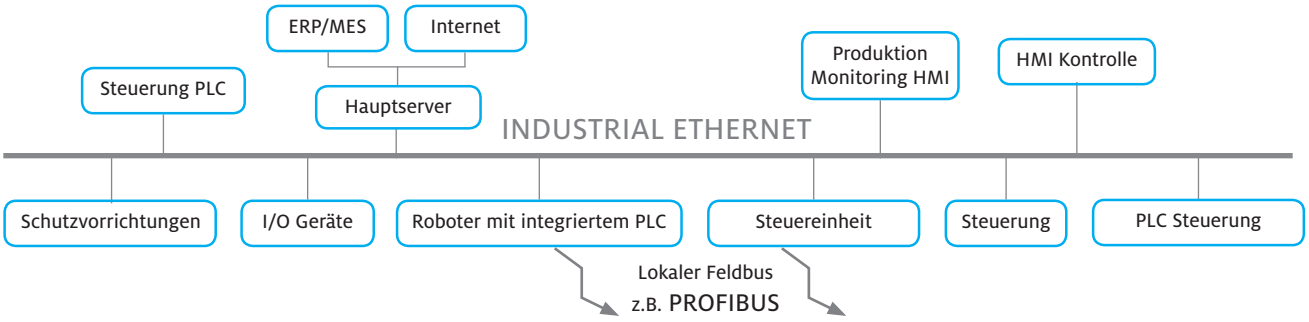
- Identifikation aller IT-Systeme in Produktionsanlagen
  - 360° Scan — passiv und ohne Aktivitäten im Industrial Ethernet
- Einfache Beurteilung im Risiko Management
  - Zentrale Analyse der Netzwerke und IT-Komponenten in MES, SCADA, SPS und PLC
- Kontinuität für den Überwachungsprozess
  - Automatisiert, integriert in das Alarmmanagement

VIDEC.

IRMA – Sicherheit und Stabilität für die Produktion durch kontinuierliche Überwachung

Industrie Risiko Management Automatisierung

IRMA ist ein Industrie-Computersystem zur Identifikation und Abwehr von Cyberangriffen in Produktionsnetzwerken. IRMA überwacht kontinuierlich Ihre Produktionsanlagen, liefert Informationen zu Cyberangriffen und ermöglicht die Analyse und intelligente Alarmierung mittels einer übersichtlichen Management-Konsole. So können verzögerungsfrei Aktionen gestartet werden, um den Angriff zu stoppen oder seine Folgen wirkungsvoll zu entschärfen.



Neue Herausforderungen im Industrial Ethernet und Industrial Internet

Mit hoher Geschwindigkeit hält die Vernetzung und übergreifende Kommunikation von IT-Systemen Einzug in die Produktionen. Mit ihr ist die einfache und direkte Integration von bestehenden Anlagen in eine effizientere Steuerung und zunehmend auch in die Managementsysteme gefordert.

Basis dafür ist das Industrial Ethernet. Dazu werden ProfiNet, Ethernet/IP oder EtherCAT bei Anpassungen und Erweiterungen der Steuerung und Automatisierung eingesetzt. Zum einen wird die Produktion dadurch durchgehend transparent, zum anderen folgt daraus aber auch, dass alle Systeme an ein Netzwerk angeschlossen sind. Strikt getrennte Netze für den verschiedenen Datenaustausch in Produktionsanlagen sind nicht mehr vorhanden. Die Annahme, dass Produktionsanlagen keine Verbindung zum Internet haben, trifft also nicht mehr zu.

Diese Vernetzung von Produktionsanlagen und ihrer Steuerungseinheiten mit der Büro-IT oder über das Internet bietet den Unternehmen nicht nur Vorteile durch eine kontinuierliche Optimierung und Flexibilisierung der Fertigung — sie birgt auch viele Gefahren. Deshalb stellt die effiziente Absicherung von Produktionsanlagen gegen Cyberangriffe, interne Manipulationen oder fehlerhafte Konfigurationen eine zunehmende Herausforderung dar.

Funktionen und Module

IRMA ist ein Industrie-Computersystem mit einer übersichtlichen Managementkonsole. Ohne jegliche Aktivitäten im Netzwerk der Produktionsanlage lernt und analysiert es alle Systeme und Verbindungen.

Nach einer Validierung oder durch die Beurteilung im integrierten Risikomanagement überwacht IRMA kontinuierlich die IT-Infrastruktur und zeigt in Echtzeit Manipulationen oder Cyberangriffe an. Entscheidungen über maßgebliche Aktionen, die den Angriff stoppen oder die Auswirkung entschärfen, können so verzögerungsfrei getroffen werden.

Basierend auf diesen Erkenntnissen lassen sich notwendige und zielgerichtete Anpassungen der Sicherheitsarchitektur im Rahmen des Sicherheitsmanagementprozesses effektiv vornehmen.

Optional kann IRMA Angriffsszenarien erkennen, die Alarmierung durch die Priorisierung im Risikomanagement effizient steuern und Anomalien der Nutzung eigenständig identifizieren.

IRMA ermöglicht:

- Vollständige Übersicht der IT-Systeme, Netzwerk- und Datenverbindungen in der Produktion zur Planung und Ergänzung der Sicherheitsinfrastruktur
- Alarmierung bei Security-Vorfällen durch die kontinuierliche Überwachung
- Absicherung von „nicht patchbaren“ Systemen z. B. Windows NT/ 2000 / XP, alte SPS, OPC Classic
- Absicherung von „zertifizierten“ Produktionsanlagen und Prozessen (z. B. Pharma, Chemie, Nahrungsmittel) ohne Re-Zertifizierung

Module im Basissystem:

- Beurteilung aller identifizierten Informationen im Risikomanagement-Prozess in Bezug auf mögliche Betriebsrisiken, z. B. Ausfall, Produktionsqualität, Datenschutz
- Überwachung bestehender und neuer Produktionsanlagen und deren Systeme:
  - Insbesondere für Systeme, für die es aktuell keine Schutzmöglichkeit gibt bzw. aufgrund der hohen
  - Betriebslaufzeit nicht mehr geben wird
    Durch Soll-Ist-Vergleich der identifizierten
  - Systeme und Datenverbindungen
    Alarmierungen
- Erstellen von Reports für Auditierungen
- Analysedaten zur Erstellung einer angepassten Sicherheitsarchitektur und Sicherheitstechnik in der Produktion

Optionale Module:

- Identifikation von Anomalien bei Systemen und Datenverbindungen
- Profile für Systeme der Automatisierung bekannter Hersteller
- Erkennen von Cyberangriffen
- Strukturierung der IT-Komponenten zum Produktionsprozess

Gefahren durch vertikale Integration

Mit OPC Classic, OPC UA oder der Windowsdatei-Freigabe (SMB) werden die Daten zwischen Systemen der Steuerungs- (SPS/PLC) und SCADA-Ebenen ausgetauscht. Durch zunehmende direkte Kopplung mit Lieferanten, Partnern und Kunden steigen die Anforderungen — und damit auch die Gefahren.

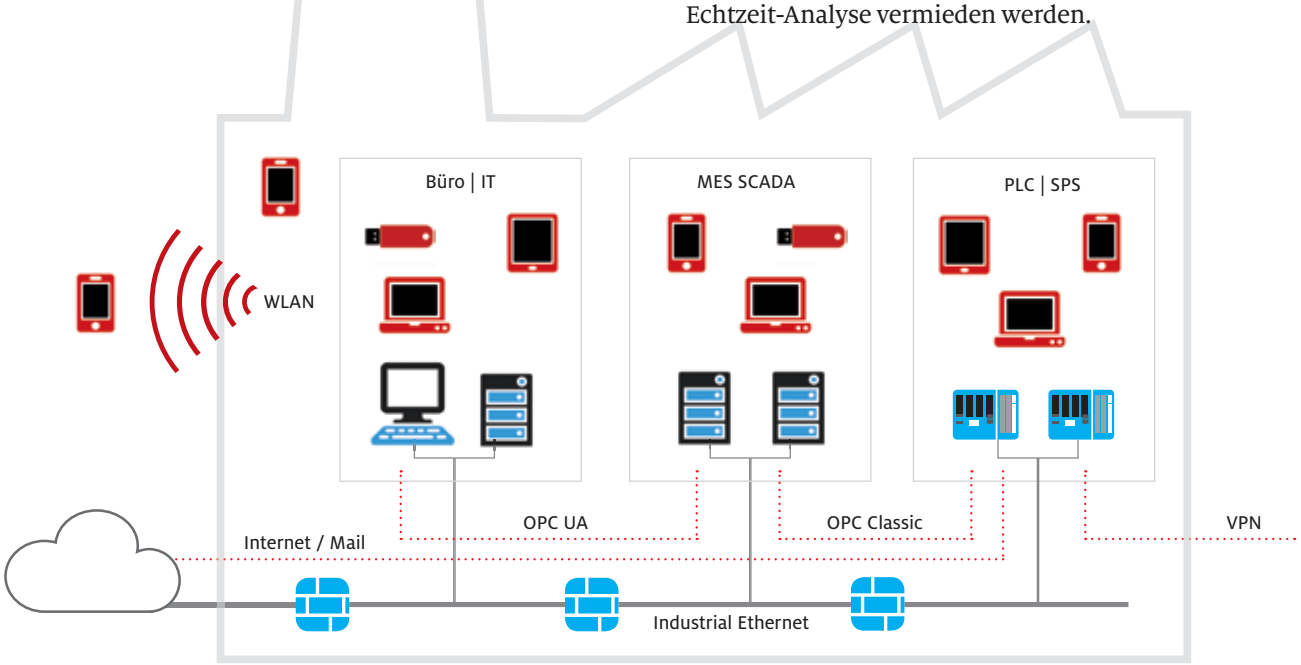
Die meisten Industrial Firewalls können die hierfür genutzten dynamischen Verbindungen mit ihren unterschiedlichen Ports oder auch den Standard Web-Port (80) nicht ausreichend kontrollieren. Es bilden sich Schwachstellen, die Cyberangriffen viele Möglichkeiten der Verbreitung und der unbemerkten Beschaffung von Informationen eröffnen.

Industrial Security muss umdenken

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-fortgeschrittene anhaltende Bedrohungen), also Angriffe, die mit hohem Aufwand und zielgerichtet die Standard-Schutzeinrichtungen 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.



Integriertes Alarmmanagement

IRMA liefert Informationen zu Cyberangriffen in Echtzeit — auf Basis kontinuierlicher Überwachung, Analyse und intelligenter Alarmierung. Die Alarmmeldungen werden in IRMA priorisiert, angezeigt und verteilt und können auch online in ein Alarmmanagement überführt werden.

Das Alarmmanagement hat eine Schlüsselfunktion an der Mensch-Maschine-Schnittstelle im Betrieb. Alarmierungen sind nur hilfreich, wenn die Häufigkeiten und die Qualität der Informationen geeignet sind, die Betriebsverantwortlichen zu unterstützen.

Mit IRMA erfolgt die Priorisierung von Alarmmeldungen wahlweise automatisch oder in effizienter Weise über das integrierte Risikomanagement. Die Alarmhäufigkeiten sind dabei auf ein handhabbares Maß beschränkt und die Aussagekraft der Alarme ist sehr hoch.

Durch die bereitgestellten Informationen werden Cyberangriffe sofort erkannt. So werden umgehende Gegenmaßnahmen ermöglicht, die einen Angriff stoppen oder seine Folgen wirkungsvoll entschärfen.

HIGHLIGHTS

Einfache Installation, umgehender Nutzen

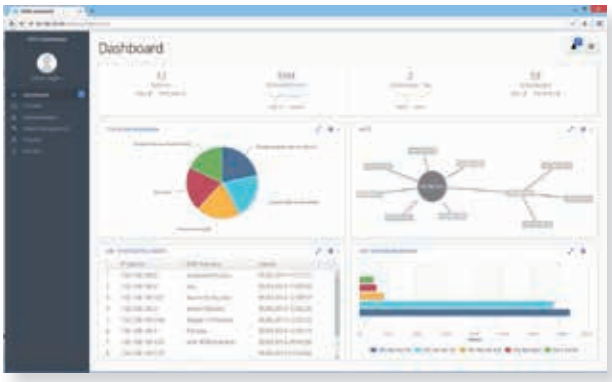
In wenigen Schritten ist IRMA bereit, ihr Produktionsnetzwerk zu überwachen. Es bietet unmittelbar Informationen zu manipulierten System- und Datenverbindungen sowie zu Cyberangriffen.

Intelligente Überwachung hilft

IRMA lernt ihr Produktionsnetzwerk kennen und zeigt es übersichtlich an. Es ermöglicht Ihnen, sämtliche Informationen nahtlos im Risikomanagement zu nutzen.

Kontinuierlich und in Echtzeit

Eine kontinuierliche Überwachung alle Systeme und Datenverbindungen in ihrer Produktionsanlage ist gewährleistet. Cyberangriffe oder Ausfälle sind sofort sichtbar und können detailliert analysiert werden.

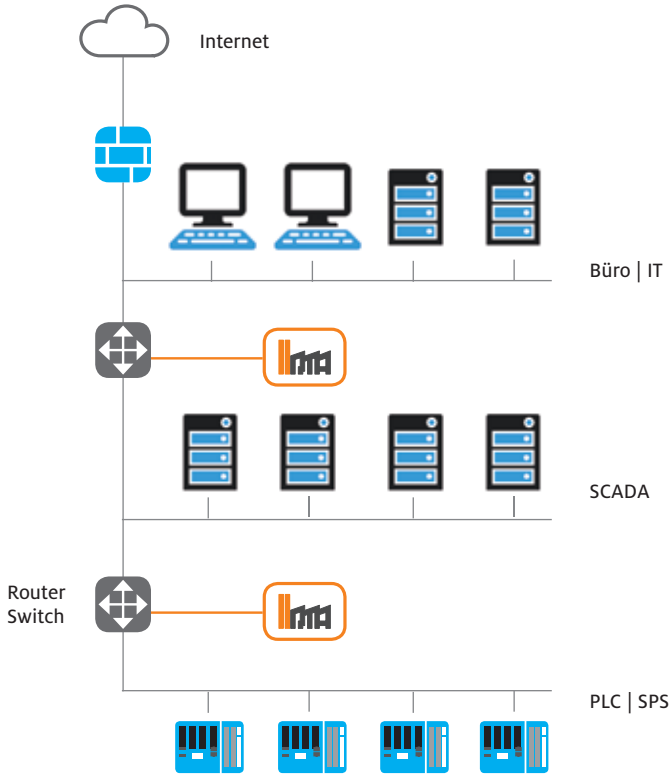


Alarmmanagement und Reporting

Mithilfe der Reporting- und der Exportfunktionen ist eine Übersicht jederzeit gewährleistet. Die direkte Koppelung mit ihrem Alarmmanagement ermöglicht eine effiziente Instandhaltung.

Mobile und Web

Neue Systeme und Verbindungen werden durch IRMA sofort identifiziert. Es ermöglicht die umgehende Beurteilung, ob diese zulässig oder — z. B. infolge eines Cyberangriffes — unzulässig sind. Diese Erkennung auch mobiler Geräte ist für Firewalls und VPNs in der klassischen Perimetersicherheit nicht möglich.



Funktioniert herstellerübergreifend

Egal, welche Hersteller in ihrer Produktionsanlage eingesetzt werden: IRMA arbeitet auf technologischen Standards und damit herstellerunabhängig.

WARUM IRMA?

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 — z. B. durch „drive by“. Dabei wird der Schadcode quasi „huckepack“ in zugelassenen Verbindungen mittransportiert und kann die Grenzen ungehindert passieren.

Kontinuierliche Überwachung

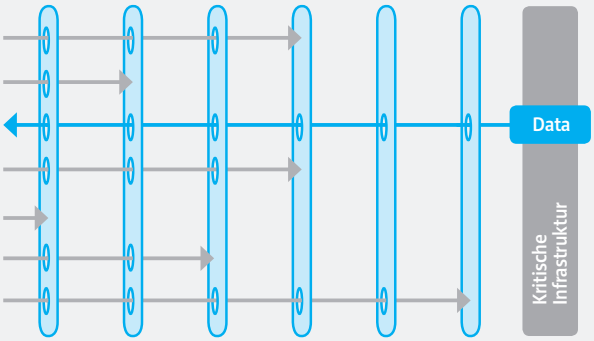
Überwachung und Reporting in Echtzeit sind die Voraussetzungen für das Erkennen von Cyberangriffen, die Ihre Produktionsanlage bereits erreicht haben. Die von den Angreifern genutzten Werkzeuge und Datenverbindungen müssen kontinuierlich beobachtet, kontrolliert und analysiert werden, um die Ausbreitung und damit auch den Cyberangriff selbst zu stoppen.

Sicherheit, die mitdenkt

IRMA ist das erste Überwachungssystem, das sich störungsfrei in den Produktionsprozess implementiert. Es lernt das kontinuierliche Überwachen und steuert die Alarmierung angepasst an die Schutzklassen in ihrem Risikomanagement-Prozess. IRMA liefert alle notwendigen Daten, um den Angriff oder die Manipulation schnellstmöglich zu beseitigen.

Info: 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 ihre Produktionsanlage und können sich dort unbeobachtet ausbreiten.



So nimmt zum Beispiel nimmt der Servicetechniker, der am Vorabend im Hotel-WLAN seine Mails abruft und im Internet surft, am nächsten Tag das gleiche, jetzt infizierte Gerät — z. B. den Laptop, einen USB-Stick oder eine vorkonfigurierte Komponente — mit in den geschützten Bereich und verbindet es zum Datenaustausch mit der Produktionsanlage.

IRMA ist sofort einsatzbereit

Für den Anschluss an das Netzwerk der Produktionsanlage erfolgt die Auslieferung im Passiv-Mode. Das System beginnt sofort mit dem Identifizieren. Bei segmentierten Netzwerken ermöglicht der Einsatz von IRMA-Tap-Clienten die ganzheitliche Überwachung.

VIDEC GmbH
Contrescarpe 1 · DE-28203 Bremen · Phone +49(0)421 - 33 950-0 · Fax +49(0)421 - 33 950-50
info@videc.de · www.videc.de
Niederlassungen und internationale Vertretungen entnehmen Sie bitte unserer Website.