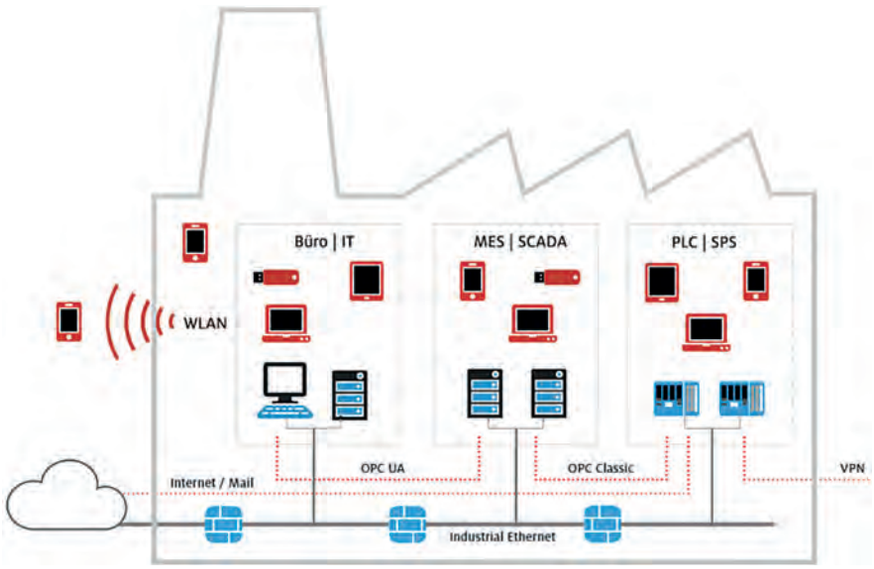



**01** Das System „Produktionsanlage" steht in ständigem Kontakt mit Zulieferern, Herstellern, Dienstleistern sowie Kunden und läuft damit Gefahr, sich zu infizieren

# Risiken und Nebenwirkungen minimieren

Die neue Welt der Automatisierung bietet ein hohes Maß an Integration, Datenaustausch und Mobilität. Dank der Nutzung von Industrial Ethernet sowie zunehmender vertikaler oder sogar globaler Integration, unter anderem durch Standards wie OPC-UA, steht den kommenden Anforderungen zu mehr Flexibilisierung und Industrie 4.0 eigentlich nichts mehr im Wege. Es stellt sich aber die Frage: Wie minimiere ich die Risiken durch Cyberangriffe – einfach, automatisiert und integriert in die Betriebsprozesse?

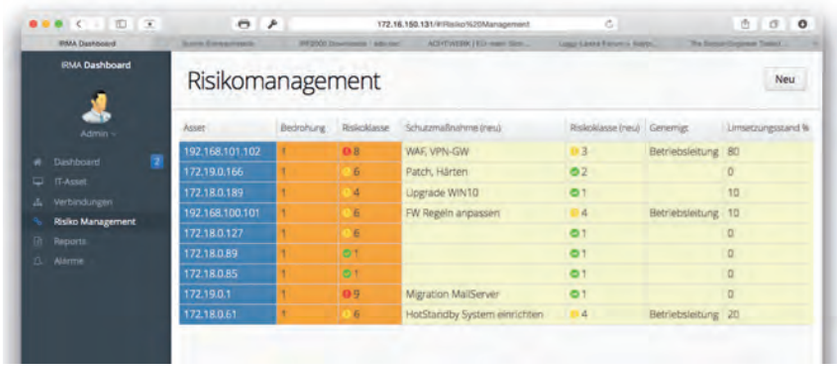
**Text**: Dieter Barelmann, Stefan Menge

Außenkontakte bringen die Gefahr mit, sich zu infizieren – das gilt für das System „Mensch" als auch für technische Anlagen. Dabei spielt der Zustand des körpereigenen Immunsystems eine entscheidende Bedeutung für die Abwehr von Krankheiten. Wie gut ist das System in der Lage, sich selbst zu schützen?

Auch das System „Produktionsanlage" steht in ständigem Kontakt mit Zuliefern, Herstellern, Dienstleistern und Kunden und läuft damit Gefahr, sich zu infizieren (**Bild 1**). Außerdem gibt es zusätzlich die Bedrohung durch direkte Cyberangriffe von Hackern und staatlichen Organisationen. Dabei ist es in Bezug auf das Resultat egal, ob die Angriffe politisch oder kriminell motiviert oder zufällig sind. Die klassischen Abwehrmechanismen, wie Firewalls und Antiviren-Software, sind nur noch bedingt tauglich. Welchen Risiken sind vernetzte Automatisierungs- und Prozessleittechnik, die häufig älter als 15 Jahre sind, aktuell ausgesetzt?

Viele Produktionssysteme werden seit Jahren mit Industrial Ethernet ausgerüstet – entweder komplett oder über Gateways zugeschaltet. Für die klassischen Scada-Infrastrukturen sind Angriffe ebenso, wenn nicht sogar stärker gefährdend, werden doch mehr und mehr Standard-IT-Komponenten eingesetzt und Sicherheitslücken nicht nachträglich geschlossen. Wie heißt es in der Automatisierung? „Never touch (change) a running System". Für die Steuerung werden web-basierte HMI oder dedizierte Apps für Tablets und Smartphone von den Automatisierungstechnikherstellern angeboten. Flexibel kann vom Arbeitsplatz der Betriebsleitung oder Geschäftsführung direkt auf die historischen Daten zugegriffen werden.

Die Risiken entstehen nun durch diese oftmals durchgängige Vernetzung und unbeschränkten Zugriffsmöglichkeiten auf die Steuerungen. Unbeschränkt daher, weil die aufwendigen Anpassungen in der Netzwerk- und Firewallkonfigu-




**02** Die Lösung Irma für das Risiko-Management

ration sowie die Pflege der Benutzer-Accounts unterbleibt. Auch eine Trennung von Büro- und Produktionsnetzwerk schafft hier keine wirkliche Abhilfe.

### Mehr Verbindungen – höheres Risiko

Mit dem zunehmenden Einsatz von Mobilgeräten erhöhen sich die Risiken nochmals. Fast jedes mobile Gerät, wie ein Tablet, Smartphone oder auch ein Laptop, lässt sich nur nutzen, wenn nahezu kontinuierlich eine Verbindung mit dem Internet besteht, zum Beispiel für Software-Updates und Zugriff auf E-Mail. Eine Folge kann sein, dass die Produktionsanlagen mehrfach ohne Schutz mit dem Internet verbunden sind. Schadsoftware kann so ungehindert eindringen. Darauf folgende Manipulationen bedrohen den reibungslosen Betrieb und die Verfügbarkeit. Auch die Service-Zugriffe von externen Dienstleistern tragen nicht wirklich zu einer höheren Sicherheit der Anlage bei. Kurz: In vielen Unternehmen kann Schadsoftware ungehindert in das Produktionsnetz und auf die Steuerungssysteme gelangen. Nun verbreitet sich der Schad-Code im Produktionsnetz Schritt für Schritt bis zu den neuralgischen Systemen und wird aktiv. Im schlimmsten Fall führt das zum Stillstand der gesamten Produktionsanlage oder zu noch weiterreichenden Schädigungen.

Wie kann mit diesen Bedrohungen umgegangen werden? Die naheliegende Schlussfolgerung ist: Zu Risiken und Nebenwirkungen fragen Sie Ihren Hersteller oder Errichter. Allerdings ist es wahrscheinlich, dass die Antwort lauten wird: Die Verantwortung für den sicheren Betrieb liegt beim Betreiber und hängt vom übergreifenden Sicherheitskonzept ab. Damit ist zwar der Nagel auf dem Kopf getroffen, aber noch keine wirkliche Antwort gefunden.

### Risiko-Management gegen Nebenwirkungen

Zur Risikoreduzierung sind eine Vielzahl von Funktionen vorhanden und Schutzsysteme am Markt verfügbar. Viele Maßnahmen sind bekannt und durchaus umsetzbar. Allerdings handelt es sich meist um Einzellösungen und sehr aufwendige Lösungen, die kontinuierlich gepflegt werden müssen. Zu den Pflegemaßnahmen gehören:

– Pflege der Benutzer-Accounts und (keine einfachen) Passworte,
– Kontrolle und Nachvollziehbarkeit der genutzten VPN-Verbindungen,
– Patchen und Aktualisierung von Betriebssystemen und Software,
– Systemhärtungen (nur was wirklich benutzt wird, ist installiert),
– White Listing (Kontrolle der installierten Software),
– aktuelle Antivirus-Software auf allen Systemen,
– Anpassungen der Netzwerk- und Firewallkonfigurationen,
– Intrusion Detection für SPS und Scada.

Das Risiko wird mit diesen Abwehrmaßnahmen reduziert. Allerdings entstehen Nebenwirkungen: Dazu zählen der hohe Aufwand, die Organisation und die Kosten. Erst ein Risiko-Management hilft, die stärksten Nebenwirkungen dieser Gegenmaßnahmen zu minimieren, und zwar den enormen Aufwand an Zeit und Kosten. Zunächst ist dafür die Kenntnis über die spezifischen relevanten Risikofaktoren von elementarer Bedeutung. Nur so lässt sich ein aussagekräftiges „Gesundheitsbild“ über die relevanten Schwachstellen des „Organismus“ entwerfen, womit dann zielgerichtet die Abwehrkräfte stabilisiert werden können.

Übertragen auf die Automatisierungs- und Prozessleittechnik ist das notwendige Wissen über die installierte Hardwarebasis und deren Schnittstellen die entscheidende Voraussetzung, um zu erkennen, welche Risiken sich aus der immer weiter steigenden Vernetzung ergeben. Auf die Frage, welche Netzelemente und -zugangspunkte im Netz existieren – auch temporäre, werden die Verantwortlichen und Administratoren meist unsicher und können nur eine vage Auskunft geben. Aus der Erfahrung lässt sich ableiten, dass die Dokumentation in der Regel unvollständig, veraltet oder im schlimmsten Fall nicht vorhanden ist. Damit bleibt auch unklar, welche konkreten Bedrohungen mit geeigneten Maßnahmen begegnet werden müssen. Aus dieser Unkenntnis des Ist-Zustands ergeben sich bis heute leider nur zwei Handlungsoptionen:

– Der Betreiber ignoriert die existierenden Bedrohungen und damit die Folgekosten eines möglichen Schadens oder
– nach dem Motto „viel hilft viel“ wird eine Vielzahl von Einzelmaßnahmen geplant und realisiert.

Auf Dauer sind beide Optionen nicht wirtschaftlich. In der ersten Option würde der über kurz oder lang eintretende Schaden bei Weitem die eingesparten Kosten für Sicherheitsinvestitionen übersteigen. Im zweiten Fall lässt sich sachlich nicht abschätzen, bis zu welchem Grad überhaupt Kosten und Aufwand für die realisierten Sicherheitsmaßnahmen sinnvoll sind. Das heißt, wie hoch dürfen die Kosten für Sicherheitsinvestitionen in Bezug auf den Wert der geschützten Infrastruktur sein.

### Assets und Schnittstellen identifizieren

Somit sind für ein ergebnisorientiertes Vorgehen die ersten Arbeitsschritte eindeutig vorgegeben: Alle im Netz vorhandenen sogenannten Assets und Schnittstellen sind valide

und am besten automatisiert zu identifizieren. Der angestrebte Nebeneffekt: Endlich hält man eine immer aktuelle Übersicht über das Netz als Planungsinstrument in den Händen.

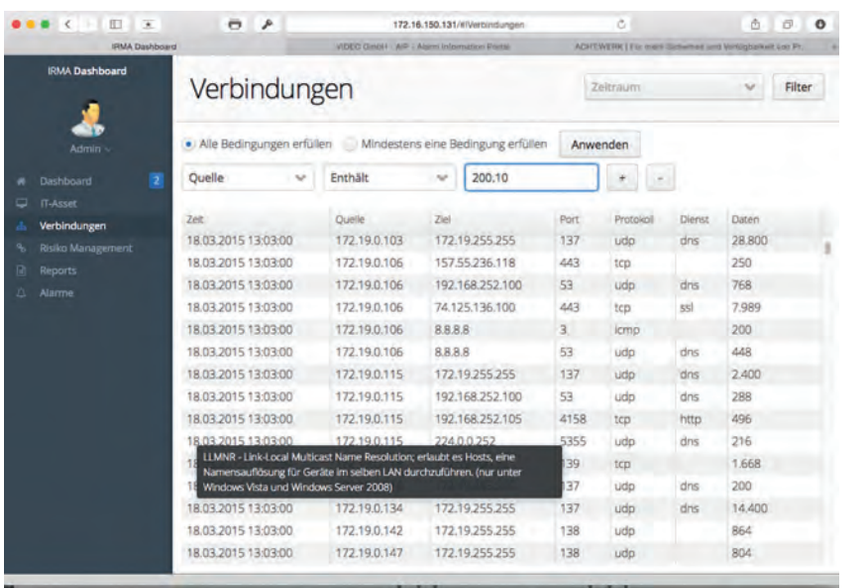
Allerdings ändern sich Netzkonfiguration, Schnittstellen und Verbindungen im täglichen Betrieb häufig. Deshalb sollte die Erfassung kontinuierlich durchgeführt und auch überwacht werden. Ein automatisiertes Verfahren mit übersichtlicher Darstellung und Auswertung ist notwendig, um den Erhebungsaufwand wirtschaftlich angemessen und langfristig umsetzbar zu halten. Das Ergebnis dieser Ist-Analyse bildet schon die Grundlage für ein qualifiziertes Risikomanagement – einfach und übersichtlich. Das gesamte Abbild kann dann regelmäßig in einem Report abgelegt und auch als Nachweis verwendet werden.

## Gegenmaßnahmen priorisieren, Nebenwirkungen minimieren

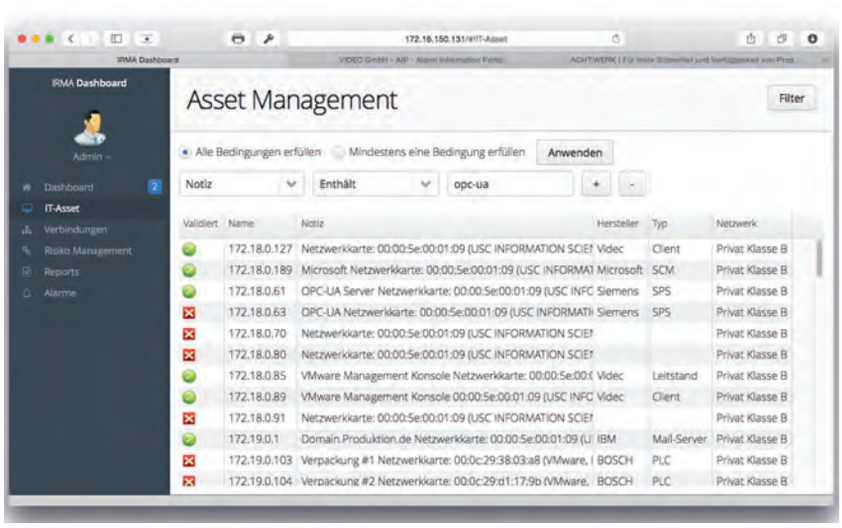
Durch diese initiale und dann kontinuierliche Aufnahme aller IT-Systeme und der Verbindungen lassen sich die vorhandenen Schwachstellen in Bezug auf die relevanten Bedrohungen in der Automatisierungs- und Prozessleittechnik bewerten. Sichere und erlaubte Verbindungen werden validiert, neue Verbindungen erkannt, aufgezeichnet und, wenn erlaubt, validiert. Alle unzulässigen Verbindungen sind identifiziert und werden notfalls sofort mittels Alarmierungssystem gemeldet. Auf Basis dieser Erkenntnisse kann nun das potenzielle Schadensausmaß abgeschätzt und ein Risikowert ermittelt werden. Mit diesem Wert kann der Betriebsverantwortliche die notwendigen und wirtschaftlich vertretbaren Gegenmaßnahmen priorisieren und die Nebenwirkungen minimieren.

Die entsprechende Lösung dafür wird unter der Bezeichnung Irma – Industrie Risiko Management Automatisierung von Videc [1] angeboten (**Bild 2**). Die Aufgaben, die diese Lösung übernimmt, sind:

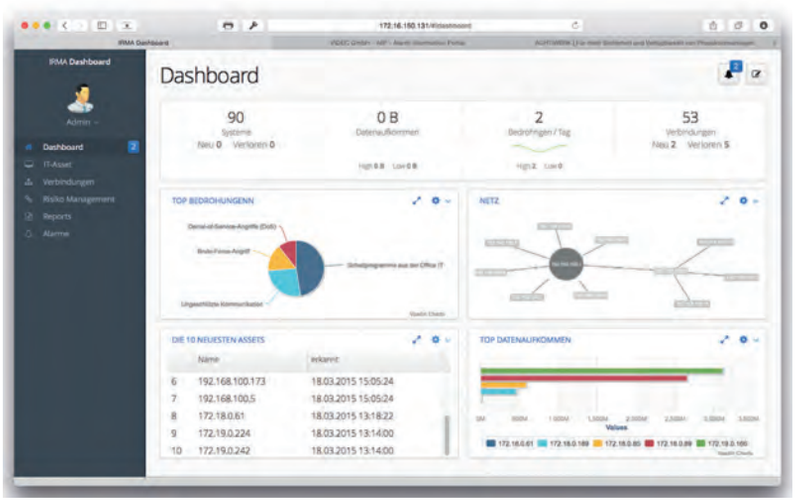
– Automatisiertes und vor allem passives Erkunden der IT-Systeme und Verbindungen der Produktionsanlage: Mit Irma werden ohne jegliche Aktivitäten im Netzwerk der Produktionsanlage die Systeme und Verbindungen identifiziert und analysiert (**Bild 3**). An einer Stelle wird sodann alles übersichtlich angezeigt und kann für die weiteren Managementschritte genutzt werden (**Bild 4**). Besonders wichtig sind die Funktionen zum einfachen Validieren und Revalidieren. Hierzu sind Filter und Suchfunktion sowie die Bearbeitung von mehreren Objekten gleichzeitig notwendig.
– Kontinuierliches Überwachen: Hierzu gehört das Erkennen von Änderungen in der Anzahl und Art von Systemen und Verbindungen in Echtzeit. Für den aufwandsarmen Betrieb muss es sodann einfach sein, Maßnahmen zu veranlassen oder den veränderten Zustand zu revalidieren. Wesentlich ist auch das Anzeigen von Veränderungen der Bedrohungslage durch neue zusätzliche Schwachstellen, die von Herstellern oder Sicherheitsorganisationen veröffentlicht werden (**Bild 5**).
– Nahtlose Integration in die Betriebsprozesse: In einfachen Worten ist es die Adaption der zusätzlichen Informationen aus der IT-Überwachung in die etablierten Systeme für den Betrieb der Produktionsanlage.




**03** Analysieren der Verbindungen




**04** Asset Management: Alles wird übersichtlich angezeigt




**05** Alle wichtigen Überwachungsergebnisse auf einen Blick


**06** Weiterleitung der Alarme und Ereignisse über das Alarmmanagement AIP

Mit dem im Alarmmanagement AIP verfügbaren wichtigen Funktionen zur Behandlung der Alarme, Ereignisse, Meldungen und Störungen sowie deren Weiterverarbeitung werden die entscheidenden Informationen an die zuständigen Fachleute oder Gruppen automatisiert weiter geleitet (**Bild 6**). Die Risiko-Managementlösung Irma bietet hierzu reichhaltige Exportfunktionen und Schnittstellen, um die Daten und Informationen aus der IT-Überwachung einfach in das Alarmmanagement oder den Instandhaltungsprozess direkt zu überführen. Ebenso ist eine Importfunktion vorhanden, um die zurückgemeldeten Ergebnisse zu übernehmen.

Bei Irma handelt es sich um ein Industrie-Computer-System mit einer übersichtlichen Managementkonsole. Ohne jegliche Aktivitäten im Netzwerk der Produktionsanlage lernt und analysiert die Lösung alle Systeme und Verbindungen und speichert diese in einer Datenbank. Die Verteilbarkeit der Irma-Client-TAPs in segmentierten Netzwerken ermöglicht die ganzheitliche Überwachung.

Basierend auf der kontinuierlichen Überwachung, Analyse und der intelligenten Alarmierung stehen in Echtzeit Informationen zu Misskonfigurationen oder Cyberangriffen zur Verfügung. Das integrierte Risiko-Management ermöglicht es, umgehend über die maßgeblichen Aktionen zu entscheiden, um einen Angriff zu stoppen oder die Auswirkung zu entschärfen. Die Verfügbarkeit der Produktionsanlage wird erhöht.

## Alles in einem System

Irma ist ein innovatives Sicherheitsprodukt basierend auf etablierten Technologien für eine optimale Sicherheit in Produktionsanlagen. Innerhalb der Produktionsanlage werden neue Angriffe in Echtzeit erkannt und Schäden vermieden. Die einfach zu installierende und zu bedienende Lösung konzentriert übersichtlich die Informationen der IT-Systeme und des Netzwerks der Produktionsanlage (SPS-Netzwerk) an einer Stelle. Automatisiert und kontinuierlich überwacht die Lösung den Zustand, erkennt neue Gefahren und Angriffe schnell in Echtzeit. Integriert in die Betriebsprozesse, wie Instandhaltung und Alarmmanagement, werden die Sicherheit und somit die Verfügbarkeit der Produktionsanlage erhöht. Die Lösung kontrolliert automatisiert und kontinuierlich den Zustand der kompletten Anlage, erkennt neue Gefahren und Angriffe schnell in Echtzeit. Irma lässt sich in Betriebsprozesse, wie Instandhaltung und Alarmmanagement integrieren, womit die Sicherheit und somit die Verfügbarkeit der Produktionsanlage erhöht wird.

Da eine Sicherheitskonzeption ein sich weiter entwickelnder Vorgang ist und sich kontinuierlich auf neue Angriffsstrategien einstellen muss, sind die Entwicklungsschritte für die Lösung Irma in ständiger Bewegung. Ein durchgängiges Update-Konzept sowie eine professionelle Beratung und Support gehören daher ebenfalls zu diesem – in Deutschland und damit ohne Nebenwirkungen entwickelten – Lösungskonzept.

## Fazit

Wer die Vorteile einer vernetzten Produktion nutzt, sollte nicht die Augen vor den Risiken, die er damit eingeht, verschließen. Deshalb: Zu Risiken und Nebenwirkungen lieber Irma fragen. Die Lösung ist einfach und ohne langen Beipackzettel mit Aufwänden, Kosten und Zeitverlust. Der Patient ist und bleibt gesund. (hz)

## Literatur

[1] Videc GmbH, Bremen: www.videc.de

## Autor

**Dipl.-Ing. Dieter Barelmann** ist Geschäftsführer der Videc GmbH in Bremen
DBarelmann@videc.de

**Stefan Menge** ist Geschäftsführer der Achtwerk GmbH & Co. KG in Bremen.
kontakt@acht-werk.de