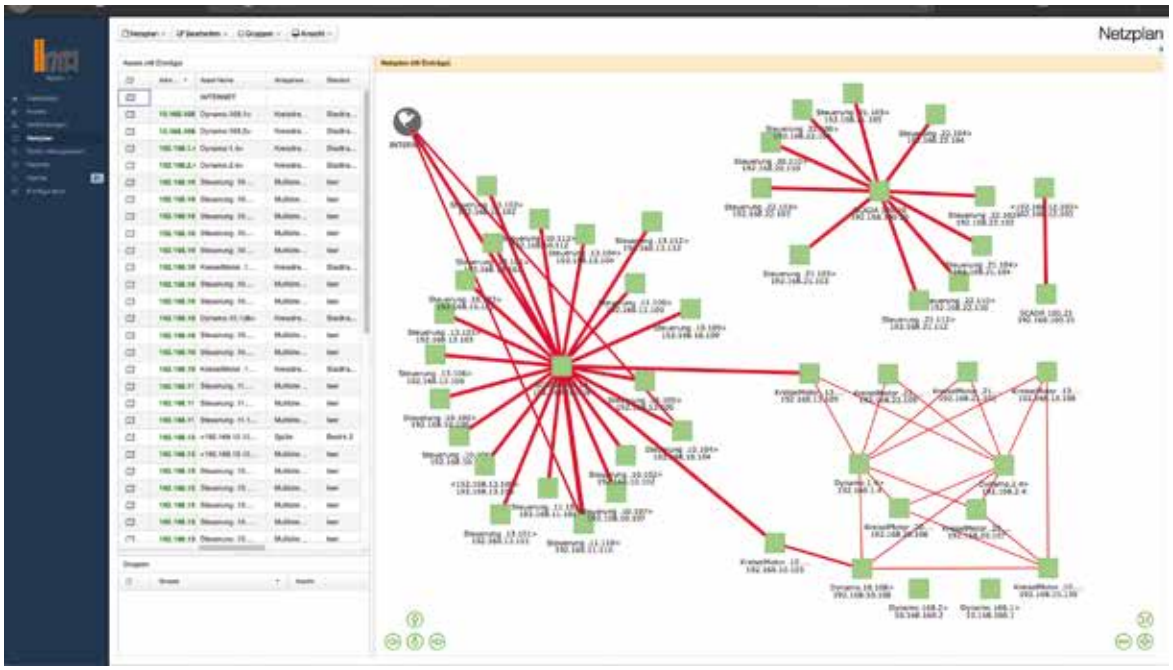


Bilder: Videc GmbH

01 Logischer Netzstrukturplan des Monitoring- und Analysetools Irma

OT-Security-Risiken messen und reduzieren

Eine Vielzahl von Hackerangriffen auf produzierende Unternehmen führte dazu, dass auch in der Geschäftsleitung eines mittelständischen Produktionsunternehmens das Risiko eines Cyberangriffs auf die Agenda rückte. Aufgrund vieler Umbauten der letzten Jahre war die Dokumentation veraltet. Zwei neue Maschinen wurden von den Herstellern gewartet und hatten somit eigene Fernwartungszugänge „mitgebracht". Auch der verstärkte direkte Datenaustausch mit den Arbeitsplätzen im Büro bereitete den Betriebsverantwortlichen bereits seit einiger Zeit Sorgen. Geschäftsführung und Betriebsleitung starteten mit Unterstützung der IT-Abteilung daher das Projekt „Industrial Security Management 2020".

Text: Dieter Barelmann, Jens Bußjäger

Nicht zuletzt die jährliche Wirtschaftsprüfung führte das Thema Cyberangriffe oben auf die Agenda. Es musste eine schnelle und gute Lösung gefunden werden. Innerhalb des Projekts „Industrial Security Management 2020" wurden an die OT-Verantwortlichen folgende Fragen formuliert:

- Wie hoch ist die Wahrscheinlichkeit eines erfolgreichen Cyberangriffs?
- Mit welchen Schäden und Produktionsausfällen muss in diesem Fall gerechnet werden?
- Sind die finanziellen Rückstellungen für den Fall eines Produktionsstillstands ausreichend?

Darüber hinaus soll die Risikobeurteilung möglichst jederzeit einfach und schnell wiederholbar sein. Weiterhin benötigt es eine Angriffserkennung, um frühzeitig die Indizien eines Cyberangriffs zu erkennen und damit mögliche Schäden zu minimieren.

Den Produktions- bzw. OT-Verantwortlichen war sofort klar, dass die vorhandene Systemmanagement- und Monitoring-Lösung für die IT-Systeme in der Büroumgebung

nicht für die Produktion geeignet waren. Es fehlten Funktionen, die die Besonderheiten der Systeme in der Produktion berücksichtigen. Im Detail wurden daher folgende weitergehenden Anforderungen formuliert, die in drei Cluster unterteilt wurden:

1. Netzübersicht und das Assetregister:
- maschinelle Erfassung der Systeme, Geräte und Datenflüsse der Produktionsanlage ausschließlich passiv und damit rückwirkungsfrei,
- jederzeit aktuelle Listen der Assets und Verbindungen sowie grafischer Netzstrukturplan,
- automatisierte Datenübertragung aus dem Monitoring für die Risikomessung.

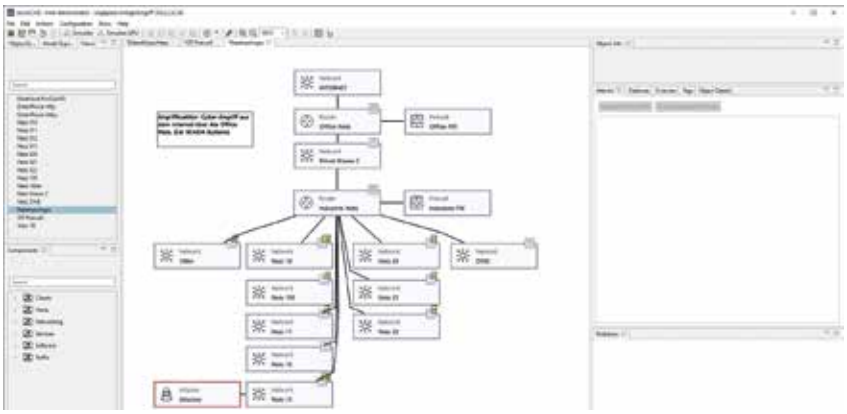
2. Verfolgung von Änderungen oder die Angriffserkennung:
- Verfügbarkeit von jederzeit aktuellen Daten,
- kontinuierliches Monitoring und Anomalieerkennung nach BSI-CS 134, um die Resilienz zur Widerstandsfähigkeit der Produktionsanlage zu erhöhen [1, 2],
- integrierte Alarmierung zur umgehenden Schadensbegrenzung.

3.Messung der Eintrittswahrscheinlichkeit oder auch erweiterte Risikoanalyse:
- Angriffssimulationen auf Basis jederzeit aktueller Daten der betrachteten Produktionsanlage mit Visualisierung der Angriffswege und der Eintrittswahrscheinlichkeiten,
- Berechnung der Erhöhung der Sicherheit durch mögliche Maßnahmen,
- Handlungsempfehlungen auf Basis valider Angriffssimulationen.

Projektumsetzung

Das Monitoring- und Analysetool Irma [1] sammelte zunächst über den Mirror-Port – ausschließlich passiv und damit rückwirkungsfrei – Informationen über Systeme und Datenflüsse im Netzwerk (**Bild 1**). Dadurch wurden die vernetzten Assets und deren Kommunikation in der Produktionsanlage identifiziert. Auf Basis der bereitgestellten, jederzeit aktuellen Informationen wurde eine Modellierung der Infrastruktur ermöglicht und als Basis für die Durchführung der Angriffssimulation zur Resilienzbestimmung mittels Securicad gesetzt. [3]

Über den Netzwerkaufbau hinaus konnte durch den Informationsexport aus Irma analysiert werden, welche Systeme miteinander kommunizieren und welche potenziellen Angriffswege daher zu berücksichtigen sind. [4] Mittels einer Visualisierung der Datenflüsse konnte eine vollständige Übersicht über das OT-Netz ermöglicht und die Dokumentation der aktuellen Infrastruktur erleichtert werden. Weiterhin wurden auch die Industrie-Kommunikationsprotokolle identifiziert und analysiert.



02 Im Securicad-Netzwerkmodell wurde die Netzwerk-Topologie visualisiert

03 Mit der Risikomatrix das Sicherheitsniveau feststellen

Die so gewonnene Kenntnis der vollständigen Datenflüsse war Voraussetzung für den nächsten Schritt der Risikoableitung: Nun konnte festgestellt werden, welche Systeme miteinander in Verbindung stehen und dadurch gegebenenfalls zu einem höheren Gesamtrisiko beitragen, falls eines der vernetzten Systeme durch einen Hackerangriff korrumpiert wird. Im Securicad-Netzwerkmodell wurde anschließend die Netzwerktopologie visualisiert und ein Simulationsmodell erstellt, in das weitere Informationen aus der Büro-Infrastruktur eingefügt und weitere Datenflüsse, beispielsweise für Fernzugriffe aus dem Internet auf die Industrieanlagen, berücksichtigt wurden (**Bild 2**).

Um schließlich die Resilienz der Anlage aus verschiedenen Perspektiven zu untersuchen, wurde abhängig vom jeweiligen Szenario der Angreifer im Internet (extern) oder im Produktionsnetzwerk (intern) positioniert.

Risikoableitung

Für das oben beschriebene Anwendungsfallbeispiel soll nun eine Risikoableitung unter der Annahme dargestellt werden, dass ein Angreifer aus dem internen Netz mit maximalem Angriffspotenzial versucht, die Scada-Systeme zu korrumpieren.

Mittels Securicad können alle potenziell möglichen Eintrittswege zu den Zielsystemen identifiziert und die Wahrscheinlichkeit für diese Wege quantifiziert werden. Anhand der Korrumpierungswahrscheinlichkeit kann zusätzlich das aktuelle Sicherheitsniveau festgestellt werden.

Die Risikomatrix stellt zwei Informationen dar: Auf der *X*-Achse wird die Relevanz der Systeme dargestellt – in diesem Fall sind alle Systeme gleich relevant. Die *Y*-Achse zeigt die Eintrittswahrscheinlichkeit für potenzielle Hackerangriffe auf die Systeme. Im vorliegenden Fall liegt das aktuelle Risiko der Scada-Systeme bei 76 % mit einem Angreifer von innen. Da alle Scada-Systeme im gleichen Netzwerk betrieben werden sowie identisch konfiguriert sind, weisen alle Systeme ein identisches Sicherheitsniveau auf (**Bild 3**). Alle diese Daten können direkt in das Risikomanagement, beispielsweise in ein Informationssicherheits-Managementsystem überführt werden.

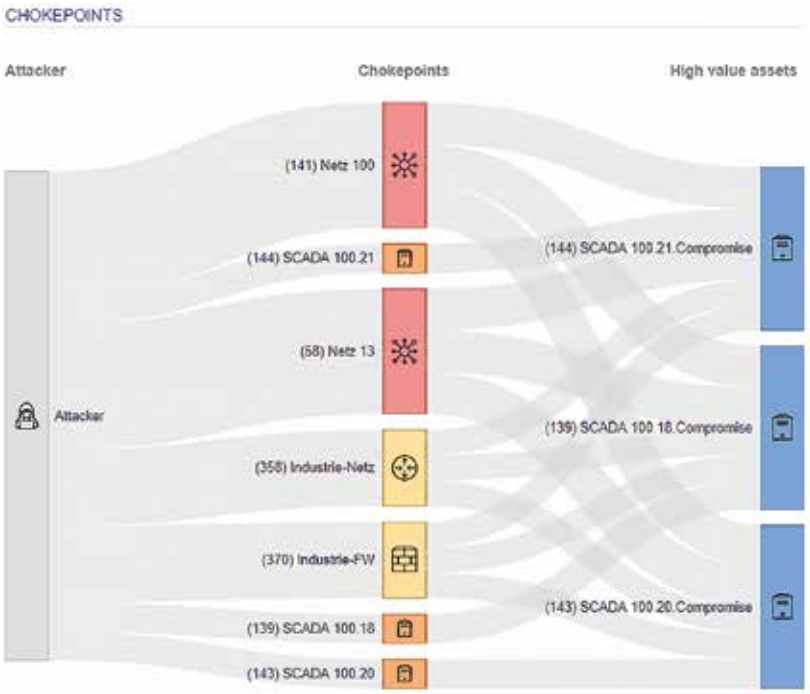
Die weitere Analyse berücksichtigt die verschiedenen Möglichkeiten, die ein Angreifer für die Übernahme der Scada-Systeme hat. Dabei wird nachfolgend dargestellt, welche Wege wie attraktiv für den Angreifer sind. Es gilt: Je breiter der Weg, desto höher die Wahrscheinlichkeit, dass dieser Weg für den Angriff genutzt wird.

Die Assets zwischen Angreifer und den Scada-Zielsystemen sind einer Risiko-Kategorie zugeordnet: Je roter die Infrastruktur-Assets dargestellt werden, desto risikobehafteter sind sie. In diesem Fall zeigen die Engstellen der Angriffswege, dass das Netz 100, in dem die Scada-Systeme betrieben werden, besonders risikobehaftet ist. Weiterhin besonders risikobehaftet ist das Netz 13, von dem aus in diesem Modell der Angreifer agiert (**Bild 4**).

Verbesserung des Sicherheitsniveaus

Die Empfehlung verschiedener Maßnahmen zur Verbesserung des Sicherheitsniveaus durch Securicad erfolgt auf Basis der wahrscheinlichsten Angriffswege. In diesem Fallbeispiel sind die beiden risikobehafteten Netze das Internet und das Netz 100. Daraus leiten sich zwei wesentliche Angriffsszenarien ab. Das erste ist die Infektion von außen bzw. dem Office-Netz. Als erstes Szenario ist ein kompromittiertes System im Büronetzwerk als „Außen"-Angreifer zu berücksichtigen. Ein möglicher Ansatzpunkt kann deshalb die Verbesserung der Sicherheit an den Übergängen von Büro- und Produktions- bzw. OT-Netzwerk sein.

Um diese Betrachtung zu untersuchen, wurde ein alternatives Modell erstellt, welches die bestehenden Netzwerkübergänge durch verbesserte Netzwerksegmentierung erweitert. Diese Segmentierung erfolgt durch Konfigurationsänderungen der Router (NAC, VLAN) oder durch den Einsatz zusätzlicher Firewalls an den Übergängen der Seg-



04 Über die Informationen der Engstellen können zusätzliche wichtige Anknüpfungspunkte für eine Verbesserung des Sicherheitsniveaus gewonnen werden

mente. Weiterhin sind auch ergänzende Funktionen möglich, wie Intrusion Detection/Intrusion Prevention System (IDS/IPS) – unter der Voraussetzung, dass die eingesetzten Systeme (FW, IDS, IPS, ...) die genutzten Protokolle verstehen.

Irma als zusätzliches Monitoringsystem mit Anomalieerkennung alarmiert bereits mit Installation für die OT-Netzwerkerkennung bei außergewöhnlichen Veränderungen im Netzwerk bzw. unterbricht diese entsprechende Verbindung (Kopplung Monitoringsystem zu Firewall/Routern). Durch diese automatisierte Alarmierung können umgehend entsprechende Gegenmaßnahmen etabliert werden. Dadurch verändert sich das gemessene Risiko, also die Eintrittswahrscheinlichkeit für einen Hackerangriff deutlich. Die Risikomatrix zeigt, dass sich die Eintrittswahrscheinlichkeit von ursprünglich 62 % auf aktuell 18 % verändert hat. Die Priorität der Scada-Systeme hat sich durch diese Maßnahme nicht verändert.

Die Verbesserung resultiert daraus, dass der Angreifer nun gezwungen ist, erheblich mehr Aufwand zu investieren, um das Firewallsystem zu umgehen und eine Verbindung zur Industrieanlage aufzubauen. Dies betrifft zwei Firewallsysteme, zum einen die im Office-Bereich und zum anderen die innerhalb der Industrieanlage. Aufgrund der Änderungen an den Firewallsystemen verändern sich auch die Wege, die ein Angreifer wahrscheinlich nutzt. Insgesamt hat die Verbesserung der Firewallsysteme dazu geführt, dass die Router weniger interessant für Hackerangriffe geworden sind.

Die Kritikalität der Netze ist jedoch gleichgeblieben, da sich am Aufbau der Infrastruktur nichts verändert hat. So ist das Internet nach wie vor ein hoch riskantes Netzwerk, da aus diesem der Angreifer heraus agiert. Parallel ist das Netz 100 nach wie vor hoch riskant, da alle Scada-Systeme im gleichen Netzwerk betrieben werden und so ein erfolgreicher Angriff auf das erste Scada-System einen potenziell ebenfalls erfolgreichen Angriff auf weitere Scada-Systeme bedeutet. Eine sinnvolle Erweiterung der Systemsicherheit kann deshalb eine Netzwerksegmentierung im Bereich der Scada- und Steuersysteme sein, um redundante Netzwerke aufzubauen, sofern die Produktionsumgebung dies erlaubt.

Im zweiten Szenario entsteht die Gefährdung durch den Anschluss einer infizierten Engineering-Workstation (EWS): den Laptop eines Dienstleisters, eines USB-Speichersticks, über die Fernwartungszugänge der Maschinenlieferanten oder vergleichbarer Schnittstellen.

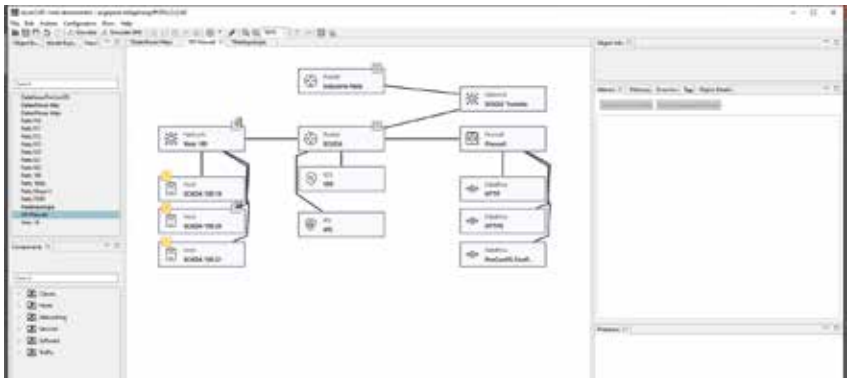
Zur Verhinderung dieser Gefährdung dient hier eine weitergehende Netzwerksegmentierung der einzelnen Netzwerke (vgl. Beispiel Scada-Netz 100 zu Steuerungsnetz 22). Wie auch im ersten Szenario kommen mögliche Konfigurationsänderungen der Router (NAC, VLAN) zum Einsatz oder zusätzliche Firewalls an den Übergängen der Segmente. Voraussetzung für die ergänzende Implementierung von Funktionen IDS/IPS ist wiederum, dass die eingesetzten Systeme die genutzten IT-/OT-Protokolle vollumfänglich verstehen.

Auch in diesem Szenario alarmiert Irma als spezialisiertes passives OT-Monitoringsystem mit Anomalieerkennung bei außergewöhnlichen Veränderungen im Netzwerk. Beim Einsatz einer zusätzlichen IPS-Funktionalität ist zunächst in der Risikoanalyse abzuwägen, welche Auswirkungen auf den Produktionsprozess bei sogenannten „false positives“ toleriert werden können. Eine rückwirkungsfreie Angriffsdetektion und automatisierte Alarmierung ermöglichen es, umgehend geeignete Gegenmaßnahmen zu ergreifen. Durch diese Maßnahmen verändert sich das gemessene Risiko, also die Eintrittswahrscheinlichkeit für einen Hackerangriff, von ursprünglich 76 % auf aktuell 31 % (**Bild 5**).

Diese Verbesserung ist darauf zurückzuführen, dass der Angreifer nun gezwungen ist, deutlich mehr Aufwand zu investieren, da er sich in den Netzwerken der Produktionsanlage nicht mehr frei bewegen kann. Ein Hackerangriff auf das Büronetzwerk hat somit keinen unmittelbaren Einfluss mehr auf die Produktion.

Durch die Segmentierung verändern sich über das Risiko hinaus auch die Wege, die ein Angreifer ausnutzen kann. Diese haben die Kritikalität von wichtigen Produktionsnetzen gemildert. Die neu eingeführte Netzwerksegmentierung ist unmittelbar Teil der aktuellen Angriffsvektoren.

Trotz dieser nennenswerten Verbesserungen gibt es weitere Risiken, die weiter minimiert werden können, um die Gesamtinfrastruktur sicherer zu machen. Beim Design neuer Abwehrmechanismen ist darauf zu achten, dass die neu eingeführten Maßnahmen nicht nur risikominimierend



05 Die Eintrittswahrscheinlichkeit für einen Hackerangriff, konnte von ursprünglich 76 % auf aktuell 31 % reduziert werden

sind. Sie müssen potenziellen Gefahren auch möglichst lange standhalten.

Mithilfe von alternativen Infrastruktur-Modellen ermöglicht Securicad den Vergleich von Maßnahmen bereits vor der technischen Umsetzung. Anhand der Eintrittswahrscheinlichkeit lässt sich quantitativ belegen, welchen Mehrwert die Maßnahme für die aktuelle Infrastruktur bringt. Entscheidungen lassen sich auf Basis der Risiko-Minimierung treffen und dokumentieren.

Ergebnisse

Um die bestmögliche Entscheidung bezüglich der Verbesserung der Infrastruktur treffen zu können, werden die verschiedenen Modellszenarien miteinander verglichen. Beim externen Szenario gibt es zwei Modelle: das der aktuellen Infrastruktur und die Erweiterung der Infrastruktur durch eine Firewall direkt am Übergang. Der Vergleich zeigt die Änderung der Risikowerte an. Im zweiten Szenario kommt der Angreifer aus einem inneren Netz. Der Risikovergleich zeigt die aktuelle Infrastruktur mit dem Risiko eines internen Angreifers und die Veränderung durch die Netzwerksegmentierung innerhalb der Produktionseinheiten.

Aus den oben beschriebenen Prozessen ergaben sich für das Unternehmen auch einfache Maßnahmen, die eigenständig umgesetzt werden konnten. Hierzu zählen die Anpassungen der Konfiguration der Firewallsysteme, die Einführung komplexerer Passworte ohne häufigen Wechsel bei den Systemen in der Produktion sowie die Erstellung von Vorgaben für Dienstleister und Maschinenlieferanten.

Positiv ist aufgefallen, dass unmittelbar nach der Installation von Irma bereits zielführende Maßnahmen identifiziert wurden, eine grundsätzliche Angriffserkennung möglich war und sofort erste Berechnungen zu potenziellen Angriffswegen und -wahrscheinlichkeiten erfolgen konnte.

Der Informationsexport aus Irma in das Securicad-Modell stellt dabei sicher, dass alle relevanten Informationen zur Risikoeinschätzung betrachtet wurden. Die Möglichkeit, den aktuellen Zustand der Infrastruktur auf Knopfdruck zu exportieren, führt zu einem dauerhaften zyklischen Risikomanagement, welches auf tagesaktuelle Daten zugreift und sich durch die Datenübernahme in einen dauerhaften Risikoprozess einbetten lässt.

Irma überwacht kontinuierlich sämtliche 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. Securicad sorgt mit der Messmethodik dafür, dass stets der gleiche Weg zur Quantifizierung des System-Risikos benutzt wird. Dieser Weg lässt sich beispielsweise auch in einem Audit oder einer bevorstehenden Zertifizierung darlegen.

In der Kombination von Irma und Securicad liefern die Daten eine Entscheidungsvorlage zur Beschreibung des aktuellen Risikos und zur Identifikation der effektivsten Maßnahmen zur Risikominimierung. Mithilfe dieses dauerhaften Risikomanagements lässt sich die Verfügbarkeit der Produktionsanlage erhöhen und die Anfälligkeit gegenüber technischen Risiken verringern.

Die Geschäftsführung hat bereits im Verlauf des Projekts aktuelle Informationen zur Möglichkeit eines Cyberangriffs erhalten. Die Wahrscheinlichkeit eines Cyberangriffs und somit das unternehmerische Risiko eines Betriebsstillstands wurden fundiert gemessen und konnten bewertet werden. Die differenzierte Betrachtung der zwei Szenarien und die identifizierten Maßnahmen erhöhten die Resilienz der Produktionsanlage. Die Anpassungen der finanziellen Rückstellungen für einen Produktionsstillstand finanzierten nicht nur die Security-Maßnahmen. (hz)

Literatur

[1] Irma von der Videc GmbH, Bremen: www.videc.de/produkte/irma-cybersecurity-risikomanagement-intrusion-detection-system/

[2] Barelmann, D.: Monitoring und Erkennung von Anomalien in Anlagen. etz elektrotechnik & automation 140 (2020) H. 8 S. 42 - 43

[3] Industrieanlagenreilienz direkt aus der Infrastruktur: https://securithon.de/industrieanlagen-resilienz-direkt-aus-infrastruktur-daten/

[4] Securicad-Schnittstelle zu Irma: https://securithon.de/schnittstelle-irma/

Autoren

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

Jens Bußjäger ist Geschäftsführer der Achtwerk GmbH & Co. KG in Bremen.
jens.bussjäger@acht-werk.de