



Informationsdienst

# SCADA-Sicherheit

IT-Security für Systeme der Automatisierungs-, Leit- und Steuertechnik

*Industrielle Malware*

## Gezielte Attacken

Interview mit Michael Hoos von Symantec über Bedrohungen für Produktionssysteme nach Stuxnet

*Seite 5*

*Schwachstellen in der Leittechnik*

## Augen zu und durch? Das hilft nicht!

Sicherheitslücken und Design-Schwachstellen müssen bei der Absicherung industrieller Kontrollsysteme berücksichtigt werden.

*Seite 11*



**IT-Grundschutz**  
Informationsdienst

**<kes>**

Die Zeitschrift für  
Informations-Sicherheit

**Wik**

Zeitschrift für die Sicherheit der Wirtschaft



*Sicherheitslücken begegnen*

## Die ICS-Security- Fata-Morgana

Automatisierungshersteller reden Sicherheitsschwachstellen in ihren Produkten gerne klein.

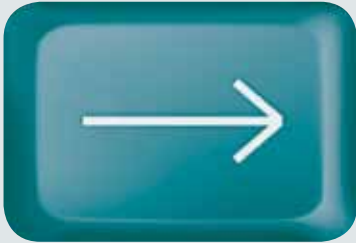
*Seite 16*



**SecuMedia**

Der Verlag für  
Sicherheits-Informationen

# ping - - - und aus dem Takt!



**Produktionsprozesse sind leicht aus dem Gleichgewicht zu bringen. Stuxnet hat gezeigt: Bedrohungsszenarien sind bereits zur Realität geworden. Informieren Sie sich jetzt, um Schaden rechtzeitig abzuwehren:**

Der neue Informationsdienst SCADA-Sicherheit liefert für Verantwortliche in IT und Produktion umfassende Information über Gefahrenpotenziale und entsprechende Gegenmaßnahmen.

## **Basis-Paket print**

Verschaffen Sie sich fundiertes Basiswissen und einen Überblick über Technik und Maßnahmen zur Absicherung von Systemen der Automatisierungs-, Leit- und Steuertechnik.

Mit dem Basis-Paket erhalten Sie 2 x jährlich grundsätzliche Berichte zum Schutz verschiedener Industriearbeitssysteme aus allen Branchen als Printausgaben.

## **Basis-Paket print**



2 Ausgaben  
print / Jahr  
**12,00 €**

## **Premium-Paket print + online**

So bleiben Sie das ganze Jahr auf dem Laufenden und können aktuelle Entwicklungen sofort in die Praxis umsetzen.

Erhalten Sie aktuelle Informationen zur Absicherung von Industriearbeitssystemen aller Branchen als Gesamtpaket print + online:

2 x jährlich Print-Ausgabe

2 x jährlich Online-PDF Ausgabe

6 x jährlich Newsletter SCADA-Sicherheit

Exklusiv-Informationen wichtiger Institutionen und Behörden

Rabatt-Codes für verschiedene Veranstaltungen, Bücher, Videos usw.

## **Premium-Paket print + online**



**39,00 €**



[vertrieb@secumedia.de](mailto:vertrieb@secumedia.de)

[www.scada-sicherheit.de](http://www.scada-sicherheit.de)

Fax +49 6725 5994

**Halten Sie Ihre Systeme im Gleichgewicht! Bleiben Sie aktuell informiert.**

## **Bestellung**

- Basis-Paket** Ich abonniere das Basis-Paket Informationsdienst SCADA-Sicherheit (2 Printausgaben à ca. 24 Seiten) zum Jahresbezugspreis von **12,00 €** inkl. Versandkosten und MwSt
- Premium-Paket** Ich abonniere das Premium-Paket Informationsdienst SCADA-Sicherheit (2 Printausgaben à ca. 24 Seiten, 2 PDF-Ausgaben à ca. 10 Seiten, 6 x jährl. Newsletter, Sonderinformationen, Sonderrabatte auf Veranstaltungen, Bücher usw.) zum Jahresbezugspreis von **39,00 €** inkl. Versandkosten und MwSt

Das Abonnement wird jeweils jährlich im Voraus in Rechnung gestellt. Eine Kündigung ist jederzeit möglich. Die SecuMedia Verlags GmbH räumt mir das Recht ein, diese Bestellung innerhalb 14 Tagen ab Bestelldatum zu widerrufen. Ich kann das Abonnement jederzeit kündigen. Zuviel bezahlte Abo-Gebühren werden rückerstattet. Ich bin mit der Speicherung meiner Daten einverstanden. Ich bin damit einverstanden, dass die Deutsche Post AG eine eventuell geänderte Anschriftweiterleiten kann.

Ort / Datum: \_\_\_\_\_ Absender: \_\_\_\_\_

\_\_\_\_\_

Unterschrift: \_\_\_\_\_

\_\_\_\_\_



## **Es ist Zeit zu handeln**

Die Überwachung, Steuerung und Visualisierung von Prozessen mit Hilfe von SCADA-Systemen zählt zu den wichtigsten Bausteinen für den sicheren Betrieb kritischer Infrastrukturen. Technisch hochkomplexe Industrieanlagen können erst durch die intelligente Kopplung von Mess- und Regeltechnik sicher betrieben werden.

Durch die von Kunden und Herstellern vorangetriebene Prozessintegration proprietärer SCADA-Systeme sowie deren Anpassung an systemübergreifende Standardschnittstellen wurden der Automatisierungsgrad und damit auch der Informationsgehalt der Anlagen noch weiter gesteigert. Diese Öffnung zur Standard-IT öffnete jedoch auch Manipulationen und Datenabfluss Tür und Tor. Seit dem Angriff durch Stuxnet ist in der öffentlichen Wahrnehmung angekommen, dass die Sicherheit kritischer Infrastrukturen verbessert werden muss.

Da SCADA-Systeme oft mehrere Jahre im gleichen Systemzustand betrieben werden und nur selten abgeschaltet werden können, befindet sich noch immer eine Vielzahl von Altsystemen im Einsatz. Über deren Sicherheit und Bedrohungsresistenz kann keine gesicherte Aussage getroffen werden. Hinzu kommt, dass neue SCADA-Systeme oft in einem vom Hersteller empfohlenen und implementierten Standard-Auslieferungszustand verbleiben. Die vorhandenen Sicherheitsmechanismen sind unwirksam, da der Betreiber etwa Passwörter nicht ändert. An wichtigen Schnittstellen, etwa Ethernet und SAP, können gezielte Angriffe Systeme lahmlegen, Informationen abziehen oder schlimmstenfalls Störfälle mit Gefährdung von Menschenleben verursachen. Die Bedrohungen aus der „Office-Welt“ haben die Leittechnik erreicht.

Nun ist es wichtig, dass Hersteller und Integratoren eine nachhaltige Sicherheitspolitik implementieren. Security sollte dabei als Nutzen für den Unternehmenserhalt und nicht als bloßer Kostenfaktor betrachtet werden.

Nutzen Sie die Gelegenheit und machen Sie sich mit Risiken, Schadenspotenzialen, Lösungen und Praxistipps vertraut. Die Notwendigkeit, für mehr Sicherheit in der Leittechnik zu sorgen, haben Sie bereits erkannt. Eine Hilfe dazu halten Sie in Ihren Händen.

**Steffen Zimmermann**  
 Referat Security und Informationssicherheit  
 VDMA - Verband Deutscher Maschinen- und Anlagenbau e.V.

### **Mitherausgeber**





*Inhalt*

---

**Gezielte Attacken**

Interview mit Michal Hoos, Technischer Direktor Zentraleuropa bei Symantec, über die Bedrohungen für Produktionssysteme nach Stuxnet

Seite 5

---

**Rendezvous in der DMZ**

Maschinen und ganze Industrieanlagen lassen sich komfortabel und sicher über einen zentralen Rendezvous-Server fernwarten.

Seite 8

---

**Mobiler Zugriff? Na klar.**

Auf den ersten Blick scheint es so, als ob mobile Datenkommunikation und Sicherheit einen Widerspruch darstellen. Betrachtet man den Sachverhalt genauer, ergibt sich jedoch ein anderes Bild.

Seite 10

---

**Augen zu und durch? Das hilft nicht!**

Sicherheitsprobleme in der Prozessleittechnik beschränken sich nicht auf dort eingesetzte PC-basierte Komponenten. Das zeigen etwa die vielen kürzlich veröffentlichten Schwachstellen in Siemens-S7-Steuerungskomponenten. Die Problematik ist grundlegender Natur und erfordert ein generelles Umdenken.

Seite 11

**Ein ideales Spielfeld**

Im Gespräch mit Marcel Kisch, Manager bei KPMG, über Sicherheitsstandards in der Automatisierungstechnik und die Herausforderungen für das Risikomanagement von Unternehmen

Seite 14

---

**So nah und doch so fern:  
Die ICS-Security-Fata-Morgana**

Kommentar von Oliver Sucker, Inhaber der IT-Sicherheits- und Beratungsfirma Forensic Investigations, zu Sicherheitsschwachstellen in Kontrollsystemen und wie Anwender diesen begegnen können

Seite 16

---

**Malwareschutz für Produktionsnetze**

Da Malwareschutz auf Produktionssystemen häufig nicht genutzt werden kann, bietet es sich an, den Virenschutz auf externe Hardware auszulagern.

Seite 18

---

**Netzsegmentierungen in  
Prozessleitnetzen**

Netzwerksegmentierungen verhindern den ungefilterten Zugriff auf ein SCADA-System, wenn sich Corporate-LAN und Prozessleitnetz nicht strikt voneinander trennen lassen. Firewalls teilen das Netzwerk auf und filtern den Verkehr zwischen den einzelnen Segmenten.

Seite 20

---

**Hackern auf der Spur**

Im Gespräch mit Toralv Dirro, Security Strategist bei McAfee, über Malware-Gefahren für SCADA-Systeme

Seite 21

---

**Impressum**

Seite 22



„Erlangt ein Krimineller die Kontrolle über ein Produktionsnetz, kann er ein Unternehmen damit leicht erpressen“, warnt Michael Hoos von Symantec.

**SecuMedia: Herr Hoos, gibt es industrielle Malware jenseits von Stuxnet, die für SCADA-Systeme gefährlich ist?**

Michael Hoos: Ja, die gibt es. Stuxnet war eine gezielte Attacke gegen eine iranische Urananreicherungsanlage. Es war die erste Attacke gegen ein SCADA-System, die wirklich massiven Schaden anrichtete, öffentlich wurde und ein Umdenken in der Produktions-IT einleitete.

Allerdings gibt es seit mindestens 1982 in einer regelmäßigen Folge Angriffe auf SCADA-Systeme, die zumeist zielgerichtet verlaufen. In anderen Fällen werden solche Systeme versehentlich betroffen, wie etwa im Jahr 1982, als ein Trojaner-Angriff das Pumpensystem der transsibirischen Pipeline manipulierte und so eine Explosion auslöste.

---

*Anm.d.Red.: Bei diesem Vorfall handelt es sich um die angebliche Sabotage einer sowjetischen Gas-Pipeline durch die CIA im Jahr 1982, die in der Autobiografie des ehemaligen Leiters des US-amerikanischen Militärnachrichtendienstes NRO, Thomas C. Reed, beschrieben wird.*

---

# Gezielte Attacken

Thomas Heinen, freier Journalist aus Köln

**Interview mit Michal Hoos, Technischer Direktor Zentraleuropa bei Symantec, mit den Spezialgebieten IT-Risikomanagement sowie Unternehmenslösungen für die IT-Sicherheit, über die Bedrohungen für Produktionssysteme nach Stuxnet**

Ein anderes Beispiel ist der so genannte Slammer-Wurm, der in der Vergangenheit versehentlich SCADA-Systeme lahmlegte, die mit dem Internet verbunden waren.

---

*Anm.d.Red.: Der als Slammer bezeichnete Wurm tauchte erstmals im Jahr 2003 auf und nutzte eine Sicherheitslücke im Microsoft SQL-Server 2000 aus, um binnen kurzer Zeit hunderttausende von Rechnern weltweit zu infizieren. Auch heute noch melden Sicherheitsanbieter Slammer-Angriffe über das Internet.*

---

Heute geht der Trend dahin, dass zielgerichtet Malware für zielgerichtete Attacken kreiert wird. Art und Funktionsumfang der Malware sind letztlich nicht besonders spektakulär. Bei Stuxnet war das nicht anders, nur das Ziel und die Auswirkungen des Angriffs waren extrem. Die Vielzahl redundanter Technologien, die Stuxnet nutzte, waren fast alle bekannt. Aber deren Kombination war bisher einmalig.

**SecuMedia: Wie schätzen Sie persönlich die Bedrohungssituation nach Stuxnet für Unternehmen ein?**

Hoos: Es gibt zwei wesentliche Gründe, aus denen Angriffe erfolgen. Das sind einerseits politisch motivierte Taten, zu denen ich Stuxnet zähle, und andererseits monetär motivierte Taten, zu denen alle anderen Vorfälle zählen. Beide haben gemein, dass sie extrem gezielt stattfinden. Wenn ich mich frage, warum jemand eine Produktionsanlage beschädigen sollte, fällt mir sofort Erpressung als möglicher

Grund ein. Erlangt ein Krimineller die Kontrolle über ein Produktionsnetz, kann er ein Unternehmen damit leicht erpressen.

Mit einem Fahrzeughersteller haben wir im vergangenen Jahr ein Worst-Case-Szenario durchgespielt. Das Unternehmen verwendet einen Laser, der die Fahrzeuge zusammenschweißt. Dieser Schweißvorgang erfolgt rechnergesteuert und wird mit rund 15.000 Bildern pro Minute überwacht. Der Laser setzt dabei exakt so viel Energie ein, wie nötig ist, um die einzelnen Komponenten sicher miteinander zu verbinden. Manipulierte man diesen Vorgang, wäre die Festigkeit der Schweißnaht nicht mehr gewährleistet. Dem fertiggestellten Fahrzeug sähe man das nicht an. Wenn das Fahrzeug aber einen Unfall erlitt und sich dabei überschlugte, würde die Fahrgastzelle kollabieren und den Fahrer töten, anstatt ihn zu schützen.

Deutsche Automobilhersteller haben so starke Qualitätsstandards, dass ein solcher Mangel auch bei einer unbemerkten Manipulation des Lasers nach einer gewissen Produktionsmenge festgestellt würde. Unter Umständen wären dann aber bereits einige tausend Autos ausgeliefert. Ein solches Szenario kann sich kein Fahrzeughersteller erlauben.

**SecuMedia: Warum wird bei produktionsnaher IT kaum auf Sicherheit geachtet?**

Hoos: Traditionell haben Unterneh-

men ihre produktionsnahe IT abgeschottet in separaten Netzwerken betrieben, die nicht mit dem Internet verbunden waren. Da keine Verbindung zu anderen Netzen vorlag, hielten es die meisten Unternehmen für unnötig, besondere IT-Sicherheitsvorkehrungen zu treffen. Es musste nur dafür gesorgt werden, dass der Netzwerkbereich abgeschottet bleibt.

Das hat sich in den letzten Jahren grundlegend geändert. Um kosteneffizienter zu arbeiten, haben viele Unternehmen Office-IT und Produktions-IT miteinander verschmolzen. Erst durch den Stuxnet-Vorfall stellten diese Unternehmen fest, dass sie damit ein viel größeres Problem geschaffen haben, als sie an Effizienz gewinnen konnten.

Zudem möchten Unternehmen die Vor-Ort-Präsenz von Personal reduzieren, um teure Nacht- und Wochenendzuschüsse zu vermeiden. Da heute ohnehin alles auf Industriestandards wie IP basiert, kam man auf die Idee, remote auf Produktionsnetzwerke zuzugreifen. Heute kann man mit einem Remote-PC, etwa einem Smartphone oder einem iPad, nicht nur prüfen, welche Probleme eine Maschine hat, die einen Alarm nach außen sendet. Es ist auch möglich, diese aus der Ferne neu zu starten oder umzuprogrammieren, ohne dass ein Mensch vor Ort sein muss.

Das schafft eine zusätzliche Sicherheitslücke. Natürlich kann man viele tolle Mechanismen einbauen, um nur einen sicheren Zugang von solchen Geräten zuzulassen. Hundertprozentig absichern lässt sich das aber nicht.

Ein drittes großes Sicherheitsrisiko besteht, da bei diesen ganzen Effizienzverbesserungen viele externe Dienstleister eingesetzt werden. Das Einrichten, Erweitern oder Umprogrammieren von Anlagen wird nur noch sehr selten vom eigenen Personal vorgenommen. In aller Regel erledigen das externe Dienstleister.

### **SecuMedia: Welche Probleme verursacht das in der Praxis?**

Hoos: Ich kenne etwa einen größeren Fahrzeughersteller in Deutschland, der alleine in einem Werk bis zu 400 externe Dienstleister beschäftigt. Diese Herrschaften gehen dort täglich ein und aus. Bis vor dem Stuxnet-Vorfall mussten sie lediglich auf einem Zettel am Werktor unterschreiben, dass Notebooks und andere Systeme, die sie mit auf das Gelände bringen, virenfrei sind. Eine weiterführende Kontrolle gab es nicht. Auch kam bis dato niemand auf die Idee, deren USB-Sticks zu kontrollieren.

Mittlerweile hat der Hersteller mit einem riesigen Aufwand eingeführt, dass USB-Sticks bei der Anmeldung gescannt und PCs geprüft werden. Das ist zwar etwas sicherer, als bloß einen Haken auf dem Papier machen zu lassen, aber dennoch kann im Prinzip jeder mit einem ungeprüften USB-Stick bis an die Produktionsanlagen kommen, da keine Körperkontrollen oder dergleichen vorgenommen werden. Eine hundertprozentige Sicherheit gibt es da bei weitem nicht.

### **SecuMedia: Was sollten Unternehmen zunächst tun, um für mehr Sicherheit zu sorgen?**

Hoos: Jeder, der in diesen Tagen eine Produktions-IT betreibt, muss sich einen Überblick darüber verschaffen, wie abgeschottet sein Netz noch ist. Zunächst muss geprüft werden, welche Zugriffsmechanismen es gibt. Dann sollte man prüfen, wie existierende SCADA-Systeme gehärtet werden können. Es gibt Technologien für die System- und Applikationshärtung, mit denen die allermeisten Angriffe abgewehrt werden können, ohne dass weitere Technologien angeschafft werden müssen.

Virenschutz fällt in den meisten Produktionsumgebungen aus, da dieser Latenzzeiten verursacht, die nicht kalkulierbar sind. Standard-Virenschutz kann nur in Umgebungen eingesetzt werden, die nicht zeitkritisch sind.

Darum geht man häufig zur Systemhärtung über, die keinerlei Latenzzeiten erzeugt und ein System im Prinzip komplett abschließt, sodass es nicht manipuliert werden kann.

### **SecuMedia: Welche Strategien empfehlen Sie Unternehmen zur Absicherung ihrer SCADA-Systeme?**

Hoos: Im Augenblick gibt es einige spannende Ansätze, bei denen etwa Active-Directory-Strukturen in die Produktions-IT eingeführt werden. Diese kennt man aus dem Office-Netz-Bereich, in dem sie zur Benutzerauthentifizierung und Berechtigungsvergabe eingesetzt werden. Einer unserer Kunden hat sich eine komplett neue Sicherheitsarchitektur gebaut und nutzt Active Directory nun, um Maschinen und Personal innerhalb eines Produktionsnetzes zu authentifizieren. So stellt er sicher, dass einerseits nur autorisierte Mitarbeiter Zugriff auf das Netz erhalten und andererseits auch nur zugelassene Maschinen darin agieren dürfen.

### **SecuMedia: Gibt es grundlegende Sicherheitsmaßnahmen, die Sie jedem Unternehmen empfehlen würden, das solche Systeme betreibt?**

Hoos: Nein, dafür sind Produktionsstraßen zu unterschiedlich. Ich habe in den vergangenen 18 Monaten 40 oder 50 Kunden unterschiedlichster Ausprägungen getroffen. Darunter war etwa ein Schuhhersteller, der ein Gerät verwendet, das Plastiksohlen mit einem Laser zuschneidet. Das Gerät befindet sich im regulären Unternehmensnetzwerk und wird von der internen Entwicklungsabteilung angesteuert. Zunächst war es mit einem Virenschutz ausgestattet, der Latenzzeiten verursachte. Aus diesem Grund wurde der Laser so getaktet, dass er nach jedem erhaltenen Befehl zwei Sekunden wartete, bevor er einen Schnitt ausführte. Mit Critical System Protection von Symantec konnten die Latenzzeiten beseitigt werden. Dadurch erhöhte sich der Durchsatz an Schuhen, die durch diese Maschine bearbeitet werden. ■

Ihr Weg zur  
sicheren  
Produktions-  
Umgebung!



# Workshop

zur IT-Security  
industrieller  
Netzwerke

am 11., 12. und 13. Oktober 2011 im Messezentrum Nürnberg



**POWTECH 2011**



**TechnoPharm 2011**

laden Sie herzlich zum Workshop ein.

Erfahren Sie von namhaften Experten z. B. aus den Unternehmen  
KPMG, Volkswagen, RSA mehr über

- die Sicherheit von SCADA-Systemen
- die Umsetzung von IT-Security-Maßnahmen in industriellen Infrastrukturen
- Managementmöglichkeiten der IT-Security in Automatisierungsnetzen
- Risiken industrieller Infrastrukturen
- Praxisbeispiele

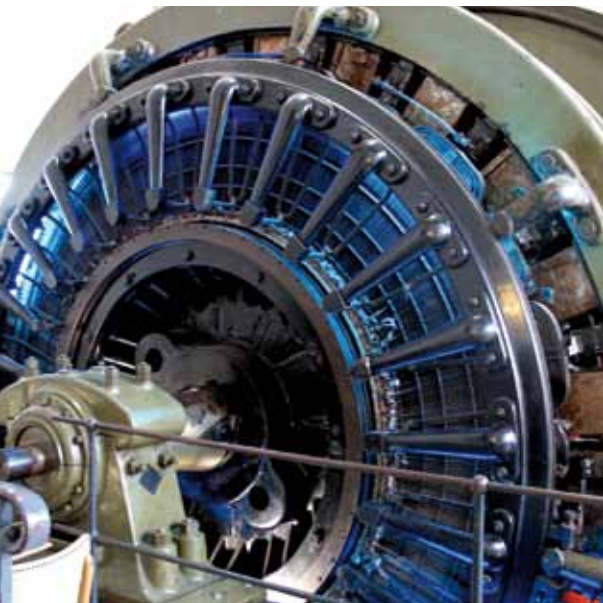
# Rendezvous in der DMZ

Dr. Michaela Harlander, Geschäftsführerin der GeNUA mbH

**Maschinen und ganze Industrieanlagen lassen sich komfortabel und sicher über einen zentralen Rendezvous-Server fernwarten.**

Wer große Anlagen wie Druckmaschinen, Fertigungsroboter, Stromgeneratoren oder Computertomografen für viel Geld beschafft, verlangt vom Hersteller die Zusicherung deren störungsfreien Betriebs. Denn sollte durch den Ausfall eines Systems etwa eine ganze Fertigungsstraße stillstehen, summieren sich die Kosten schnell auf beträchtliche Summen. Der Image-Verlust durch verspätete Lieferungen und verärgerte Kunden ist dabei nicht mitgerechnet.

Die geforderte hohe Betriebszuverlässigkeit können Hersteller nur durch ständige Betreuung ihrer Anlagen via Fernwartung garantieren. Solche Fernwartungslösungen sind dank moderner IT-Technologie, weltweiter Vernetzung und schneller Datenübertragung problemlos zu realisieren. Die Herausforderung stellt sich an anderer Stelle: Wie behalten große Industrieunternehmen, die Fernwartungs-Services von mehreren Herstellern nutzen, die zahlreichen Zugriffsmöglichkeiten auf ihre Netzwerke im Blick?



Wer etwa einen Stromgenerator betreibt, verlangt vom Hersteller dessen störungsfreien Betrieb.

Auf der anderen Seite stehen die Anlagenhersteller vor der Aufgabe, eine Vielzahl von Fernwartungs-Verbindungen zu ihren verschiedenen Kunden zu betreiben. Die zentralen Anforderungen sind hier: einfache Anwendung, flexible Einsatzmöglichkeiten, einheitliche Administration und vor allem auch zuverlässige IT-Sicherheit. Der Schadcode Stuxnet hat aufgezeigt, wie Produktionsanlagen weltweit massenhaft infiziert werden können, wenn diese komplett vernetzt, aber nicht ausreichend gesichert sind. Gelöst werden kann diese Aufgabe mit Fernwartungssystemen, die auf bewährten Standards und durchdachten Sicherheitskonzepten basieren.

Die Vorteile einer Fernwartungslösung liegen auf der Hand. Anlagen werden von erfahrenen Spezialisten des Herstellers fortlaufend überwacht und gewartet, ohne dass diese vor Ort sein müssen. Sollte trotz regelmäßiger Pflege eine Störung auftreten, können die Spezialisten via Wartungsverbindung zugreifen und die meisten Probleme umgehend lösen. Die erforderliche IT-Technologie ist ausgereift und schnelle Datenleitungen sind nahezu überall kostengünstig vorhanden. Fernwartungslösungen sparen somit Zeit und Geld. Davon profitieren sowohl der Wartungsdienstleister als auch der Anlagenanwender. Aus diesem Grund werden immer mehr Fernwartungslösungen in der Industrie, dem Gesundheitswesen und anderen Bereichen eingesetzt.

## Fernwartung mit Nebenwirkungen

Diese Vorteile sind überzeugend. Der zunehmende Einsatz von Fernwartungslösungen ist jedoch mit erheblichen Nebenwirkungen verbunden, da

die betreuten Anlagen in die lokalen Netze (LAN) der Anwender eingebunden sind. Für den Fernzugriff muss dem Dienstleister also ein Zugang in das LAN des Anwenders eingeräumt werden. Damit ist direkt der sensible Bereich der IT-Sicherheit bei der Anwenderfirma betroffen. Hier muss sichergestellt werden, dass über den Wartungszugang tatsächlich nur der Dienstleister in das LAN gelangt, nicht aber unbefugte Dritte.

Als weitere Sicherheitsstufe sollte der externe Zugriff auf das betreute Objekt begrenzt sein. Denn viele Unternehmen betreiben im Produktionsbereich ein flaches Netz, an das alle Systeme angebunden werden. Wer einmal Zugang erlangt hat, kann somit ungehindert im gesamten Kunden-LAN „herumsurfen“. So konnte etwa zuletzt der Schadcode Stuxnet innerhalb kurzer Zeit eine große Anzahl von Steuerungssystemen für Maschinenanlagen infizieren.

## Vielfalt an Lösungen erschwert Absicherung

Je mehr Wartungszugänge in ein LAN geführt werden, desto schwieriger ist dessen Absicherung. Das liegt daran, dass viele verschiedene Fernwartungslösungen verwendet werden, die über unterschiedliche Wege eine Verbindung zur betreuten Anlage aufbauen. Diese erfolgen über Modem, ISDN, DSL oder Internet sowie mit verschiedenen VPN-Standards (Virtual Private Network) zur verschlüsselten Datenübertragung. Industrieunternehmen mit größeren Maschinenparks verfügen zumeist über ein gewachsenes Konglomerat solcher Lösungen.

Für dieses Sammelsurium unterschiedlicher Lösungen müssen auf der Firewall wiederum eine Vielzahl an Ports freigeschaltet werden. Gelegentlich wird die Firewall sogar umgangen und die Verbindung direkt an die betreute Anlage im LAN gelegt. Mit jedem offenen Port und besonders natürlich durch die Umgehung der Firewall steigt die Gefährdung durch unberechtigte Zugriffe, Hacker-Attacken und Viren, die ganze Produktionsstraßen lahmlegen können.

Zu regelrechten Löchern werden diese Schwachstellen, wenn bei der Administration der diversen Zugänge Fehler unterlaufen oder die regelmäßige Pflege aufgrund des hohen Aufwands vernachlässigt wird. Dies kann schnell passieren, da jedes Fernwartungssystem andere Anforderungen stellt und einzeln betreut werden muss.

Am anderen Ende der Verbindung stehen die Wartungsdienstleister zumeist vor ähnlichen Problemen: Auch hier ist ein vielfältiges Portfolio an Fernwartungssystemen gewachsen, das umständlich zu bedienen ist und großen Aufwand bei der Administration erfordert. Mit welcher Software und welchem Modem die Anlage bei einem bestimmten Kunden zu erreichen ist, ist eine häufig gestellte Frage in Service-Centern. Auch für den Dienstleister ist es wichtig, dass sein Zugang in das Kundennetz zuverlässig gesichert wird. Sollte sich herausstellen, dass über diesen Weg etwa ein Virus in das Netz gelangt und Schäden anrichtet, würde sich dies mit Sicherheit auf die weitere Beziehung zu dem Kunden auswirken. Beide Seiten, Anwender und Dienstleister, haben somit ein großes Interesse an einer Fernwartungslösung, die folgende Kriterien erfüllt:

- Einfache Bedienung
- Komfortable Administration
- Hochwertige IT-Sicherheit
- Flexible Einsatzmöglichkeiten

### Sichere Lösung für alle Zugriffe: Rendezvous in der DMZ

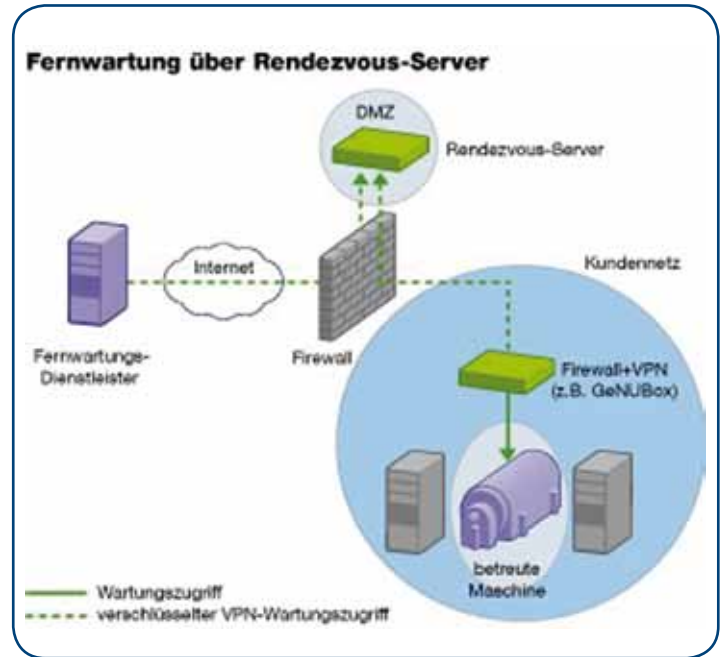
Zur Fernwartung von Maschinenanlagen in sensiblen Produktionsbereichen bietet etwa das deutsche IT-Sicherheitsunternehmen Genua eine Lösung, in dessen Mittelpunkt ein Rendezvous-Server steht. Dabei werden keine einseitigen Wartungszugriffe von Herstellern in das Netz des Industrieunternehmens zugelassen. Stattdessen führen alle Fernwartungszugriffe auf einen Rendezvous-Server, der in einem speziellen Bereich neben der Firewall, der so genannten demilitarisierten Zone (DMZ), installiert

ist. Hierhin kommt das Industrieunternehmen dem Hersteller mit einer Verbindung von innen aus dem Produktionsbereich entgegen. Erst wenn es auf dieser zentralen Wartungsplattform zum Rendezvous kommt, kann der Hersteller die jetzt durchgängige Verbindung zum Zugriff auf die betreute Anlage nutzen. Der Rendezvous-Server kann sowohl in der DMZ des Dienstleisters oder auch des Kunden eingerichtet werden. Da der Kunde zu einem verabredeten Zeitpunkt selbst aktiv werden muss, hat er stets den Überblick, wer wann in seinem Netz unterwegs ist.

Die Verbindungen zum Rendezvous-Server werden mit dem VPN-Verfahren SSH aufgebaut, das starke Verschlüsselungs- und Authentifizierungsmethoden bietet. So kann die Datenkommunikation nicht abgehört werden, und nur berechtigte Teilnehmer erhalten Zugang zur Wartungsplattform in der DMZ. Das Protokoll SSH unterscheidet sich zudem in einem wesentlichen Punkt vom dem VPN-Verfahren IPsec, das andere Hersteller häufig zum Aufbau von Fernwartungsverbindungen verwenden: IPsec erzeugt immer eine vollständige Kopplung zwischen den verbundenen Netzen. Sollte ein Rechner in einem Netz mit Schadcode infiziert sein, kann er in allen via IPsec angebotenen Netzwerken ungeschützte Systeme befallen und sich rasant ausbreiten. Mit SSH werden dagegen nur die tatsächlich notwendigen Verbindungen zwischen einzelnen Rechnern erzeugt, sodass Schadcode keine schnellen Verbreitungswege findet.

### Firewall isoliert Wartungsbereich

Bei der Lösung von Genua sorgt im Produktionsbereich zusätzlich die



Mit jedem offenen Port und durch die Umgehung der Firewall steigt die Gefährdung durch unberechtigte Zugriffe, Hacker-Attacken und Viren, die ganze Produktionsstraßen lahmlegen können.

Fernwartungs-Appliance Genubox für Sicherheit. Sie wird an der per Fernzugriff betreuten Anlage installiert und separiert mit einer Firewall-Funktion den Wartungsbereich von den anderen Systemen in diesem Netzbereich. So führt die SSH-Verbindung ausschließlich zum Wartungsobjekt. Zugriffe auf andere Systeme im Netz der Produktionsabteilung sind nicht möglich. Selbst wenn Schadcode bis hierhin vordringen sollte, kann er von dieser isolierten Anlage aus keine weiteren Systeme infizieren.

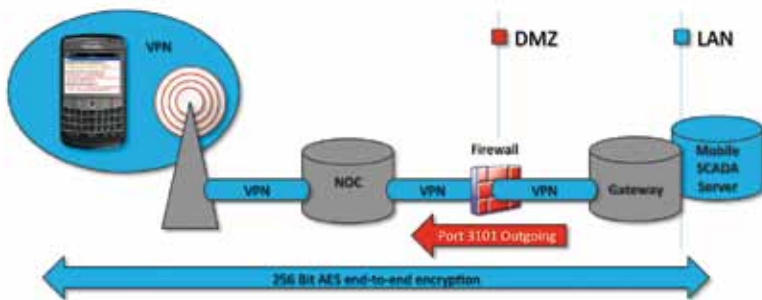
Über den Rendezvous-Server können beliebig viele Fernwartungsverbindungen zusammengeführt werden. Da Bedienung und Administration über einheitliche Oberflächen erfolgen, kann mit geringem Aufwand ein sicheres Fernwartungssystem mit vielen Teilnehmern aufgebaut und betrieben werden. Um neue Teilnehmer in die Lösung einzubinden, wird an der jeweiligen Gegenstelle lediglich eine Fernwartungs-Appliance installiert. Zahlreiche große Maschinenbauunternehmen wie der Motorenhersteller MAN Diesel und der Druckmaschinenspezialist Manroland nutzen diese Lösung, um ihre weltweit installierten Anlagen per Fernzugriff zu betreuen und ihren Kunden somit guten Service zu bieten. ■

# Mobiler Zugriff? Na klar.

Christian Schad, CEO der Schad GmbH

**Auf den ersten Blick scheint es so, als ob mobile Datenkommunikation und Sicherheit einen Widerspruch darstellen. Betrachtet man den Sachverhalt genauer, ergibt sich jedoch ein anderes Bild.**

Mobile Datenkommunikation kann heute mit einfachen Mitteln sicher konzipiert werden. Nur ein Beispiel ist die Ende-zu-Ende-Verschlüsselung auf Basis von 256-BIT-AES-Schlüsseln bzw. Hardwareverschlüsselung durch Smart-Card-Authentifizierung über zertifizierte Verfahren, wie sie etwa Giesecke & Devrient anbietet. Diese Verfahren bringen ein Sicherheitsniveau in die mobile Datenkommunikation, das häufig oberhalb der Anforderungen an kabelgebundene Datenkommunikation liegt. Mittlerweile wurde dies hinlänglich durch unabhängige Organisationen wie das Fraunhofer-Institut bestätigt. Ein erhöhtes Sicherheitsrisiko entsteht durch die Einführung dieser Technologien nicht, sofern die technischen Möglichkeiten hinsichtlich der Sicherheit ausgeschöpft und fachgerecht umgesetzt werden.



Das mobile SCADA-System EXTEND 7000 erfüllt etwa die im Artikel beschriebenen Anforderungen.

## Gelebte betriebliche Praxis

SCADA- bzw. Visualisierungssysteme und Bedienterminals arbeiten auch heute nur mit einer sehr dünnen Sicherheits-schicht gegenüber dem Benutzer. In der Regel sind die Systeme offen zugänglich, sodass jeder Mitarbeiter, der Zugang zum Eingabemedium hat, frei daran arbeiten kann – und das ungeachtet seiner Qualifikation. Benutzer-Authentifizierungen sind selten erforderlich. An den Stellen, wo dies der Fall ist, werden dennoch häufig offene Systeme vorgefunden, da die Mitarbeiter sich meist nicht aktiv

abmelden. Wir erleben dies täglich in Unternehmen unterschiedlichster Größe und in fast allen Branchen. Man kann hier sicherlich von gelebter betrieblicher Praxis sprechen. Die Systeme sehen nur in den seltensten Fällen unterschiedliche Berechtigungsstufen für unterschiedliche Mitarbeiter oder Mitarbeitergruppen vor. In den Fällen, in denen rollenbasierte Berechtigungen vergeben werden, geschieht dies nur sehr grob und ungenau, da häufig der Engineering-Aufwand innerhalb der Projektierungswerkzeuge sehr hoch ist. Auch Änderungen an den Berechtigungsstrukturen sind nur aufwändig durchzuführen und setzen meist den Einsatz externer Dienstleister voraus. Dies führt dazu, dass Berechtigungsstrukturen nicht mit den Veränderungen im betrieblichen Alltag Schritt halten und häufig auch zu einem späteren Zeitpunkt nicht nachgezogen werden. In der Natur der Sache liegt es dann auch, dass eine Protokollierung der Bedienvorgänge ohne Benutzerauthentifizierung recht sinnlos ist, da kein Nachweis geführt werden kann, wer diese vorgenommen hat.

## Ein Mehr an Sicherheit

Mit der Einführung mobiler SCADA-Systeme kann die Sicherheitsschicht bestehender SCADA-Systeme sinnvoll erweitert werden. So ist es möglich, dediziert und bis auf I/O-Ebene genau, einzelnen Benutzern bzw. Benutzergruppen Rechte zu gewähren oder zu verweigern. Auf diese Weise haben einzelne Mitarbeiter oder Mitarbeitergruppen Zugriff auf genau die Vorgänge, die von den jeweiligen Mitarbeitern beherrscht werden. Auf andere Prozesse können die Mitarbeiter nicht zugreifen und so auch keinen Schaden verursachen. Ermöglicht wird diese Erweiterung dadurch, dass unterschiedliche Mitarbeiter bzw. Mitarbeitergruppen über der Hardware des zugeordneten mobilen Endgerätes sicher identifiziert werden können. Die Hardware-ID des Endgerätes ist dem Mitarbeiter fest zugeordnet. Dadurch ist dem System zu jeder Zeit bekannt, welcher Mitarbeiter auf das System zugreift. Es kann somit die entsprechenden Berechtigungen aussteuern. Bei offenen Bediengeräten, die von unterschiedlichen Mitarbeitern verwendet werden, ist dies nicht möglich.

Zusätzlich ermöglicht diese Mitarbeitererkennung über Hardware-ID eine benutzerbezogene Protokollierung, was die Prozesse und Bedienvorgänge nachvollziehbar und damit nachhaltig macht - ohne dabei zusätzlichen Aufwand für die Mitarbeiter zu erzeugen. Sowohl im Positiven wie im Negativen kann der Nachweis erbracht werden, welche Vorgänge von welchem Mitarbeiter zu welchem Zeitpunkt ausgeführt wurden.

Sicherheit in IT-Systemen wird heute hauptsächlich in der externen Blickrichtung diskutiert: Ist ein System sicher vor Angriffen von außen? Die Frage der internen Sicherheit wird häufig vernachlässigt. Dabei übersteigt der durch Fehlbedienung der eigenen Mitarbeiter verursachte Schaden meist bei Weitem den Schaden durch externe Angriffe. Genau an dieser Stelle können mobile Systeme die Sicherheit von Gesamtsystemen sinnvoll ergänzen. ■

# Augen zu und durch? Das hilft nicht!

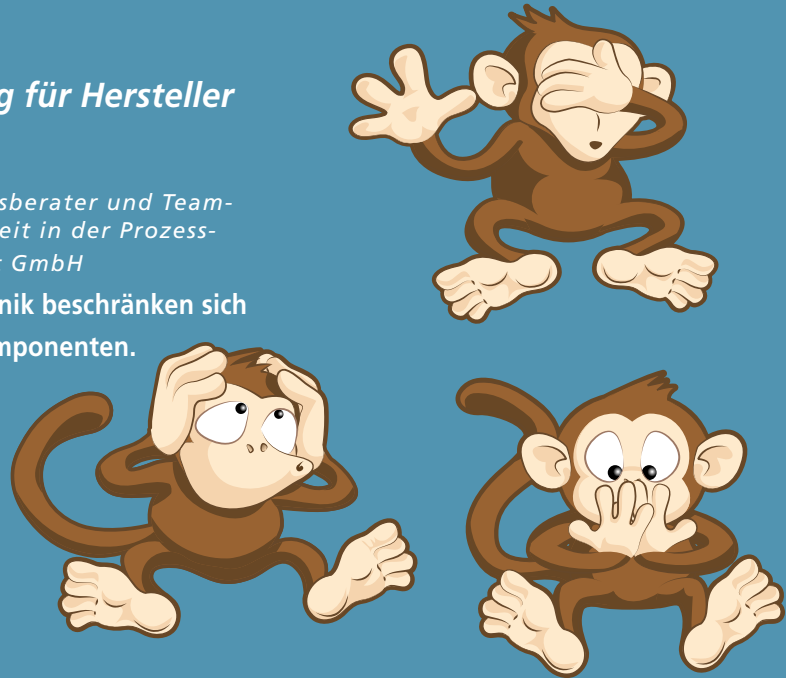
## IT-Sicherheit als Herausforderung für Hersteller und Betreiber

*Dr. Stephan Beirer, Informationssicherheitsberater und Teamleiter für den Bereich Informationssicherheit in der Prozessdatenverarbeitung bei der GAI NetConsult GmbH*

Sicherheitsprobleme in der Prozessleittechnik beschränken sich nicht auf dort eingesetzte PC-basierte Komponenten.

Das zeigen etwa die vielen kürzlich veröffentlichten Schwachstellen in Siemens-S7-Steuerungskomponenten.

Die Problematik ist grundlegender Natur und erfordert ein generelles Umdenken.



Auch in aktueller Leittechnik sind eine Vielzahl von Sicherheitslücken und Design-Schwachstellen vorhanden. Das Sicherheitsniveau der hier genutzten Technik hinkt im Vergleich zur „klassischen“ IT-Welt in Büroumgebungen und Rechenzentren um Jahre bis Jahrzehnte hinterher. Leider sind das bislang wenig thematisierte Tatsachen. In der Regel werden Sicherheitsvorfälle in diesen Bereichen nicht öffentlich gemacht. Experten diskutieren jedoch seit langem intensiv Systemausfälle aufgrund von Schadsoftwarebefall, Netzwerkstörungen und Manipulationsmöglichkeiten.

Durch Stuxnet wurde die Problematik im Jahr 2010 erstmals auch der breiten Öffentlichkeit bekannt. Allerdings entstand in der folgenden Diskussion allzu leicht der Eindruck, dass es sich bei den durch den Wurm ausgenutzten Lücken um kleinere Fehlkonfigurationen und Schwachstellen handelt, die primär nur die in der Leittechnik genutzten Windows-

Komponenten betrafen und laut Herstellerangaben inzwischen alle behoben sind. Zudem wurde häufig betont, mit welchem hohem Aufwand der Stuxnet-Angriff durchgeführt wurde und dass nur staatliche Organisationen die hierfür notwendigen Ressourcen besitzen würden.

### Vielzahl an Schwachstellen

Mit besonderer Spannung wurde deshalb der Vortrag des Sicherheitsforschers Dillon Beresford auf der diesjährigen Hacker-Konferenz Black Hat erwartet. Beresford hatte den Stuxnet-Vorfall zum Anlass genommen, sich bei eBay mehrere SIMATIC-S7-Steuerungskomponenten des Herstellers Siemens zu beschaffen und sie einem Sicherheitstest zu unterziehen. SIMATIC S7 ist die Siemens-Produktfamilie so genannter „Speicherprogrammierbarer Steuerungen“ (SPSen). Diese Automatisierungskomponenten werden weltweit in zahlreichen Branchen

zur Steuerung von verfahrenstechnischen und Produktions-Prozessen eingesetzt und stellen das Bindeglied zwischen einem PC-basierten Leitsystem und dem physikalischen Prozess dar.

Bei seinen Tests identifizierte Beresford auf Anhieb eine ganze Reihe von Schwachstellen, die verschiedene Modelle der S7-SPS-Familie betreffen:

- **Backdoor-Zugang**  
In bestimmten Firmware-Versionen der S7-300 SPS existiert ein fest einprogrammierter und undokumentierter Standard-Nutzeraccount.
- **DoS-Schwachstellen**  
Beresford präsentierte mehrere Möglichkeiten, mit denen sich S7-SPSen über das Netzwerk zum Absturz bringen lassen (DoS-/Denial-of-Service-Schwachstellen).
- **Nutzung unsicherer Netzwerkprotokolle**  
Alle S7-SPSen nutzen Protokolle



„Hersteller und Anlagenbetreiber müssen sich in Zukunft bedeutend intensiver mit der Informationssicherheitsproblematik auseinandersetzen“, sagt Dr. Stephan Beirer von der GAI NetConsult GmbH.

zur Netzwerkkommunikation, die keine hinreichenden Sicherheitsmechanismen bieten. Es ist deshalb möglich, den SPS-Speicher auszulesen und zu überschreiben; ebenso können beliebige Befehle an die SPS gesendet werden. Ein von Siemens vorgesehener Passwort-Schutz ist laut Beresfords Analysen völlig ineffektiv realisiert.

- **Easter Egg**

In mehreren S7-Firmware-Versionen fand Beresford ein so genanntes Easter Egg. Dabei handelt es sich um ein Bild tanzender Affen, das offensichtlich einer der Entwickler als Scherz im Firmware-Code hinterlassen hatte.

Werden diese Schwachstellen bei einem Zugriff auf das Automatisierungsnetzwerk ausgenutzt, können etwa die SPS-Ausgänge und damit der gesteuerte physikalische Prozess beliebig manipuliert werden. Es ist ebenfalls möglich, die SPS-Programmierung unberechtigt zu ändern, was ähnlich fatale Konsequenzen haben kann. Insbesondere für Automatisierungskomponenten sind die genannten DoS-Schwachstellen äußerst kritisch, da hierdurch ein durch die SPS

geregelter Prozess schlimmstenfalls in einen unkontrollierten Zustand geraten kann. Besonders problematisch ist dabei, dass die Abstürze auch bereits durch einfache Netzwerkstörungen oder Fehlzugriffe auftreten könnten. Das Easter-Egg stellt vermutlich keine direkte Sicherheitslücke dar. Allerdings wird hierdurch die Effektivität der in der Entwicklung angewandten Qualitätsmanagement-Prozesse deutlich in Frage gestellt.

Derzeit steht der Hersteller Siemens in Fachkreisen aufgrund seiner Informationspolitik bezüglich dieser Schwachstellen verstärkt in der Kritik. Anstatt die Problematik offensiv anzugehen, versuchen die Zuständigen offenbar seit längerem die Probleme kleinzureden. Mehrere Monate, nachdem Siemens Details zu den Schwachstellen bekannt waren, standen zur Mehrzahl der Probleme noch keine hinreichend detaillierten, offiziellen Aussagen zur Verfügung. Dies betrifft insbesondere die Risikobewertung der Schwachstellen, die betroffenen Modelle oder Firmware-Versionen sowie geplante Patches und Workarounds.

## Generelle Problematik

Bei der Bewertung der jetzt publizierten Schwachstellen und der technischen Hintergründe des Stuxnet-Vorfalles muss zunächst betont werden, dass es sich bei allen offengelegten Sicherheitslücken und Designschwächen keineswegs um Probleme handelt, die sich nur auf die Leittechnik eines bestimmten Typs oder Herstellers beschränken. Vielmehr sind sie exemplarisch für die Mehrzahl der derzeit am Markt verfügbaren Systeme. So ist in Fachkreisen bereits seit längerem bekannt, dass sich eine Vielzahl der gängigen Prozesstechnikkomponenten bei einem wie oben geschilderten Netzzugriff nahezu beliebig manipulieren oder zum Absturz bringen lassen.

Verschärft wird die Problematik zusätzlich dadurch, dass die IT-Umgebungen im Leittechnikbereich nur schwer auf einem aktuellen Sicherheitsniveau gehalten werden

können. So ist es in Produktivumgebungen etwa kaum möglich, Sicherheitsupdates für Betriebssysteme und Anwendungsprogramme zeitnah einzuspielen. Ebenso können Schutzprogramme wie Virens Scanner oft schon aus technischen Gründen (Bedarf nach Echtzeitfähigkeit, nicht unterstützte Betriebssysteme u.a.) nicht eingesetzt werden. Angesichts von Nutzungszeiträumen im Bereich von zehn Jahren und aufgrund der häufig fehlenden Unterstützung des Upgrades bereits installierter Anlagen sind die Betreiber teilweise auch gezwungen, veraltete Betriebssysteme und 3rd-Party-Komponenten einzusetzen. Da diese nicht mehr unterstützt und mit Sicherheitspatches versorgt werden, können aktuelle Sicherheitslücken häufig nicht behoben werden, bis die Leittechnik selbst aktualisiert wird.

Prinzipiell bieten diverse Leittechnikhersteller inzwischen Sicherheitskonzepte, in denen die bislang problematischen Themen wie Patchmanagement und Schadsoftwareschutz diskutiert werden. Allerdings ist immer wieder festzustellen, dass die empfohlenen Maßnahmen von Herstellern und Integratoren auch in Neuanlagen nicht oder nicht vollständig umgesetzt werden. Teilweise muss auch an der Praxisnähe der Konzepte gezweifelt werden, wenn zum Update der Antivirus-Signaturen wöchentlich eine komplette Anlagen-Außerbetriebnahme und anschließend ein vollständiger – und somit extrem aufwändiger – Funktionstest durch den Betreiber notwendig wäre. Das Gesamtrisiko erhöht sich signifikant, da Einzelanlagen zunehmend untereinander sowie mit Büroumgebungen vernetzt, Fernwartungszugänge genutzt und Fremdhardware in Prozesstechnikumgebungen eingesetzt werden. Zwar ist das durchaus notwendig und sinnvoll, die verwundbaren Systeme werden dadurch jedoch stark exponiert.

## Umdenken notwendig

Es ist offensichtlich, dass sich sowohl Hersteller als auch Anlagenbetreiber

in Zukunft bedeutend intensiver mit der Informationssicherheitsproblematik auseinandersetzen müssen. Hersteller und Integratoren müssen zunächst ihre Systeme nach dem Stand der Technik und dem hohen Schutzbedarfentsprechend absichern. Das von vielen Verantwortlichen als alleinige Schutzphilosophie oft noch praktizierte Inselprinzip, nach dem Prozessdatennetze als isolierte Welt betrachtet werden und ein Schutz nur am Netzübergang, etwa durch Firewalls, stattfindet, ist schon längst nicht mehr zeitgemäß. Allein durch die Vielzahl an Komponenten innerhalb der Prozessnetze selbst und die vielfältigen Wechselwirkungen mit externen Systemen stellen sie mittlerweile keine abgeschlossene Inselwelt mehr dar. Auch lassen sich die zahlreichen und häufig komplexen externen Schnittstellen nicht allein durch einfache Firewalls sichern. Generell müssen moderne Leittechniksysteme auch intern ein ihrer Kritikalität entsprechend hohes Sicherheitsniveau aufweisen. Die auch in Neusystemen leider noch viel zu häufig anzutreffenden Altlasten wie Standard-Passwörter, unsichere Kommunikationsdienste und ungehärtete Systemkonfigurationen müssen eli-

miniert und durch eine grundlegend sichere und robuste Systemarchitektur ersetzt werden. Insbesondere die Hersteller sind dazu aufgerufen, Lösungen für die zahlreichen Herausforderungen zu finden, die Anlagenbetreiber bei der Aufrechterhaltung eines dauerhaft sicheren Leittechnikbetriebs meistern müssen. Das betrifft etwa das Patchmanagement und den Schadsoftwareschutz. Die derzeitige Technik bietet hierzu leider kaum praktikable Lösungen.

Auch auf Betreiber- und Anwenderseite besteht verstärkter Handlungsbedarf, da die Sicherheitsproblematik nicht allein durch die Hersteller gelöst werden kann. So müssen bei Neubeschaffungen konkrete Sicherheitsanforderungen explizit ausformuliert werden. Der einfache Hinweis, nach dem das System sicher sein muss, ist im Hinblick auf die komplexe Thematik in der Regel nicht ausreichend. Ebenso muss die Prüfung auf Erfüllung von Sicherheitsanforderungen integraler Bestandteil von Abnahmetests werden. Durch individuell angepasste Maßnahmen müssen die Betreiber insbesondere alle Schnittstellen zu externen Systemen absichern, um eine bestmögliche Abschottung der sensiblen Pro-

zesstechniksysteme sicherstellen zu können. Dies betrifft neben direkten Netzwerkanbindungen besonders auch mobile Parametrier-Laptops. Das gilt vor allem, wenn diese auch in externen Umgebungen wie dem Büronetz genutzt werden.

Allerdings müssen neben rein technischen Maßnahmen in Zukunft auch organisatorische Aspekte berücksichtigt werden. Da die Sicherheitsproblematik nicht allein durch Technik gelöst werden kann, muss das Management der Informationssicherheit in die Betriebsprozesse und in die Organisation integriert werden. Hierfür ist auch im Prozesstechnikbereich der Aufbau eines Informationssicherheitsmanagementsystems (ISMS), beispielsweise nach ISO 27001 oder nach der derzeit noch im Entwurf befindlichen Norm IEC 62443, hilfreich.

Es ist nicht bekannt, ob der Siemens-Entwickler bei der Programmierung seines Easter Egg in mehreren S7-Firmware-Versionen an das japanische Sprichwort mit den drei Affen dachte, das wörtlich übersetzt so viel bedeutet wie „über Schlechtes weise hinwegsehen“. Sicherheitsverantwortlichen ist jedoch nicht zu empfehlen, diese Taktik bei der Absicherung industrieller Kontrollsysteme anzuwenden. ■

## KEINE ANGRIFFSFLÄCHE

### für Stuxnet & Konsorten



Unsere IT-Sicherheitslösungen schützen Ihre automatisierten und per Fernwartung betreuten Anlagen zuverlässig gegen Schadcode-Attacken.

Auf der it-sa in Nürnberg  
in Halle 12, Stand 422

**GeNUA**  
www.genua.de

# Ein ideales Spielfeld

Thomas Heinen, freier Journalist aus Köln

**Im Gespräch mit Marcel Kisch, Manager im Bereich IT Advisory, Risk Consulting, bei der Wirtschaftsprüfungs- und Beratungsgesellschaft KPMG, über Sicherheitsstandards in der Automatisierungstechnik und die Herausforderungen für das Risikomanagement von Unternehmen**

„Im industriellen Bereich müssen sich alle Sicherheitsmaßnahmen der Verfügbarkeit unterordnen“, weiß Marcel Kisch von KPMG.



**SecuMedia: Herr Kisch, welche IT-Sicherheitsstandards haben Unternehmen im industriellen Bereich zu berücksichtigen?**

Marcel Kisch: Es gibt eine Reihe internationaler Industriestandards, die sich aus verschiedenen Better Practices ergeben, wie sie etwa das BSI (Bundesamt für Sicherheit in der Informationstechnik) herausgibt. Allerdings existieren im europäischen Raum kaum gesetzliche Verordnungen bzw. Empfehlungen, die definieren, wie Industriesysteme abgesichert werden sollen. Im US-amerikanischen Raum sieht das im Übrigen anders aus. Die dort vorliegenden Standards sind uns um einige Jahre voraus.

**SecuMedia: Wie unterscheiden Unternehmen bei dieser Vielzahl zwischen guten und weniger guten Sicherheitsstandards?**

Kisch: Ein guter Sicherheitsstandard sollte zunächst klar in seiner Ausdrucksform und einfach zu verstehen sein. Inhaltlich sollte er alle bekannten und relevanten Risikobereiche abdecken und praktische Maßnahmen beschreiben. Abdeckungsgrad und Harmonisierbarkeit mit etablierten Standards sind insbesondere für eine effiziente Umsetzung wichtiger als der Detaillierungsgrad. Der ISO-27000-Standard ist hierbei vorbildlich.

**SecuMedia: Welche Probleme stellen sich Unternehmen, die einen Sicherheitsstandard etablieren wollen?**

Kisch: Ein großes Problem ist, dass Sicherheitsstandards für den industri-

ellen Bereich häufig bereits vorhandenen Sicherheitsstandards in den Unternehmen widersprechen oder Redundanzen verursachen. Zudem sind viele Industriestandards sehr detailliert und lassen sich daher kaum umsetzen.

Der BSI-Standard etwa hat mit Sicherheit große Vorteile. Allerdings ist er sehr konkret. Wollte ein Unternehmen ihn ganzheitlich umsetzen, müsste es tausende Kontrollen etablieren. Da das in der Praxis ineffizient ist, stellen sich Unternehmen früher oder später die Frage, welche Empfehlungen relevant sind. Im Ergebnis treffen sie selbst eine Auswahl, bei der sie große Fehler machen können.

**SecuMedia: Sind das die Probleme, mit denen sich das Risikomanagement im Unternehmen konfrontiert sieht?**

Kisch: Das Risikomanagement im Unternehmen sieht sich zwei großen Problemfeldern gegenüber: Wie sollen industrielle IT-Systeme geprüft werden und wer ist dafür verantwortlich? Bislang haben sich in diesem Bereich nur sehr wenige Unternehmen hervorgewagt. In der Regel bedarf es eines kritischen Sicherheitsvorfalls, damit ein Budget zur Verfügung gestellt wird und Sicherheitsverantwortliche aktiv werden können. Zumeist gibt es schlicht und ergreifend kein Sicherheitsbudget für Produktionsanlagen, die auf mehrere Jahre hin geplant werden. Das Sicherheitsbudget aus dem IT-Bereich wird in der Regel nicht für solche Anlagen verwendet, da sich der CISO (Chief Information

Security Officer) eines Unternehmens zumeist nicht für die IT-Sicherheit der Produktionsanlagen verantwortlich fühlt. Oft sind Werkleiter für die entsprechenden Systeme verantwortlich. Im Industriebereich kümmern sich also vorwiegend Ingenieure um die IT-Sicherheit, die in diesem Fachgebiet letztlich Quereinsteiger sind.

Das zweite Problemfeld stellt die wirklich große Zahl weltweit existierender Standards dar. Ich kenne etwa einhundert Industriestandards, die insbesondere hinsichtlich ihrer Umsetzbarkeit sehr große Qualitätsunterschiede haben. Darunter sind branchenspezifische Standards, übergreifende Standards, die sich nur auf SCADA-Systeme oder nur auf Infrastrukturen im industriellen Bereich beziehen. Bei dieser großen Zahl an Empfehlungen weiß das Risikomanagement oft nicht, wo es beginnen soll.

**SecuMedia: Können bereits vorhandene Sicherheitsstandards im Unternehmen, etwa die internationale Norm ISO 27001, nicht für Industrieautomationssysteme verwendet werden?**

Kisch: Die ISO-27001-Norm ist ein sehr gut nutzbarer Standard, der genügend Handlungsspielraum lässt und Sicherheitsmaßnahmen breit abdeckt. Mitunter bietet er relativ konkrete Maßnahmen und lässt sich prima umsetzen.

Allerdings ist dieser Standard auf IT-Systeme in der Verwaltung ausgerichtet und beinhaltet an einigen Stellen Empfehlungen, die im industriellen Bereich nicht umsetzbar sind. Ein Bei-

spiel dafür bietet der Schichtbetrieb, bei dem etwa vier oder fünf Personen über einen Tagesablauf hinweg mit dem selben IT-System arbeiten. In der Regel gibt es hier nur einen Benutzer-Login, was dem ISO-Standard bereits widerspricht, der personalisierte Logins erfordert. Man kann jedoch nicht verlangen, dass sich die Schichtarbeiter in der Fabrik jeweils mit einem eigenen Login anmelden, um die Systemzustände zu prüfen. Teilweise unterstützen die relevanten Applikationen das auch nicht. Die Anforderungen sind hier schlichtweg anders gelagert als in der Verwaltung.

**SecuMedia: Inwiefern unterscheiden sich die Anforderungen in Verwaltung und Industrie wesentlich voneinander?**

Kisch: Die drei großen Sicherheitsdogmen sind Vertraulichkeit, Verfügbarkeit und Integrität. Während die ISO-27001-Norm im Bereich Information Security auf die Integrität und Vertraulichkeit von Informationen abzielt, ist im industriellen Bereich die Verfügbarkeit das Wichtigste. Dort müssen sich alle Sicherheitsmaßnahmen der Verfügbarkeit unterordnen.

**SecuMedia: Welche Industriestandards sind für Unternehmen interessant?**

Kisch: Wirklich gut und anerkannt ist die Serie ISA-99 der International Society of Automation (ISA), die sich auf industrielle Automatisierungs- und Kontrollsysteme bezieht. Ebenfalls sehr interessant ist die Norm IEC 62443 der International Electrotechnical Commission (IEC), die den Titel „Security for Industrial Process Measurement and Control – Network and System Security“ trägt. Diese Norm baut auf ISA-99 auf und führt einen wichtigen Schritt durch, da sie sich mit bereits bestehenden anderen Standards harmonisiert. IEC 62443 integriert sich beispielsweise in einen vorhandenen ISO-27000-Standard. Ebenfalls erwähnenswert sind die Publikationen des National Institute of Standards and Technology (NIST)

sowie die VDI-Richtlinie 2182 als Sicherheitsstandard für die industrielle Automatisierung. NIST SP800-53 beinhaltet etwa Security-Maßnahmen für öffentliche IT-Systeme und basiert in Teilen auf ISA-99. Kein Standard, sondern eher eine Empfehlung zur Absicherung industrieller Kontrollsysteme, ist NIST SP800-82. Teile davon beinhaltet IEC 62443. Die Unterschiede liegen hier im Detail.

**SecuMedia: Der Standard IEC 62443, an dem ISA und IEC seit 2009 gemeinsam arbeiten, befindet sich immer noch im Entwurfsstadium. Würden Sie diesen Standard Unternehmen empfehlen?**

Kisch: Ja, nach heutigem Kenntnisstand würde ich IEC 62443 empfehlen, wenn er als offizieller Standard verabschiedet wird. Er beinhaltet eine ganze Reihe wirklich guter Zusammenfassungen der erwähnten Standards. Sein wesentlicher Vorteil ist, dass er versucht, sich mit der Normenserie ISO 27000 zu harmonisieren. Damit kann ein Unternehmen sowohl das Know-how als auch eventuell bereits vorhandene Managementsysteme für die Informationssicherheit gut adaptieren. Dadurch vermeidet es, widersprüchliche Sicherheitsstandards zu etablieren und kann sinnvolle Kontrollen aus dem Verwaltungsbereich im industriellen Bereich übernehmen. Zusätzlich kann es eigene Kontrollen ergänzen, die in IEC 62443 erwähnt werden.

**SecuMedia: Zählt es zu Ihren Aufgaben als Berater, ein Unternehmen dabei zu unterstützen, bereits vorhandene Sicherheitsstandards um einen Industriestandard zu ergänzen und so ein Sicherheitsniveau zu schaffen, das sich auditieren lässt?**

Kisch: Es wäre schön, wenn wir bereits so weit wären. Im Augenblick orientieren sich Unternehmen bestenfalls an der Normenserie ISO 27000. Wir prüfen, welche Maßnahmen sich aus dieser Serie im industriellen Bereich umsetzen lassen und welche man dort erwarten würde.

Leider gibt es noch keinen Industriestandard, der ähnlich wie ISO 27000 international anerkannt ist und umgesetzt werden kann. Allerdings ist es nur eine Frage der Zeit, bis das geschieht. Schließlich gibt es bereits viele Standards, die über sehr gute, partiell auch sehr spezifische Teile verfügen. Wichtig ist im Augenblick, dass die Sensibilität dafür wächst, dass der industrielle Bereich der eigentlich kritische ist.

Heute werden etwa Webserver und PCs mit zum Teil erheblichen Aufwand geschützt, während im Produktionsbereich nur sehr wenig umgesetzt wird. Häufig wissen die Unternehmen nicht, welche Bedrohungslage dort vorliegt, obwohl an dieser Stelle die eigentliche Wertschöpfung des Unternehmens liegt.

**SecuMedia: Muss noch ein weiterer Stuxnet-Vorfall stattfinden, damit die Sensibilisierung vorangetrieben wird?**

Kisch: Ich halte es durchaus für möglich, dass jemand den im Internet veröffentlichten Quellcode von Stuxnet nutzt, um eine Malware zu entwickeln, die Steuerungssysteme außer Kraft setzen oder umprogrammieren kann. Die Quellcode-Daten von Stuxnet sind ebenso leicht im Internet erhältlich wie etwa die Steuerungssoftware von Siemens. Für Hacker ist das ein ideales Spielfeld. Es bleibt bloß zu hoffen, dass ein dann möglicher Vorfall keine zu gravierenden Schäden hervorruft.

**SecuMedia: Für Unternehmen ist es also ganz klar an der Zeit zu handeln?**

Kisch: Ja, in meinen Augen ist es jetzt an der Zeit. Unternehmen sollten sich einfach die Frage stellen, wie sicher ihre Produktion ist und ob sie darüber überhaupt eine Aussage treffen können. Wenn sie diese Frage verneinen, ist es höchste Zeit, sich mit dieser Thematik auseinanderzusetzen und möglicherweise auch Zeit und Kosten zu akzeptieren, damit die Produktion auch zukünftig sicher läuft. ■

# So nah und doch so fern: Die ICS-Security-Fata-Morgana

Kommentar von Oliver Sucker, geprüfter und anerkannter EDV-Sachverständiger sowie Inhaber der IT-Sicherheits- und Beratungsfirma Forensic Investigations, zu Sicherheits-schwachstellen in Kontrollsystemen und wie Anwender diesen begegnen können.

Industrielle Kontrollsysteme (ICS) haben sich von autarken, ausschließlich analog auf elektrischer Ebene arbeitenden Systemen immer mehr hin zu digitalen, computergestützten Systemen entwickelt. In den letzten Jahren kam darüber hinaus der Trend zur Vernetzung mittels Industrial Ethernet auf, das herkömmliche Industriebusse und Standard-Netzwerktechnologie miteinander verzahnt. Dies ist Segen und Fluch zugleich, erleichtert es doch die Kommunikation, Projektierung und Wartung, führt aber auch zu einer größeren Angriffsfläche vormals isolierterer Kontrollsysteme.

Der Einzug dieser neuen Technologien bedingt zusätzliche Kompetenzen des Betriebs- und Wartungspersonals im IT-Bereich. In vielen Unternehmen sind jedoch die IT und der Anlagenbetrieb aus historischen Gründen organisatorisch voneinander getrennt. Daher können die zweifellos vielfach vorhandenen Kompetenzen nicht ihr optimales Potenzial entfalten. Nicht zuletzt schwächt dies die Position der Endanwender gegenüber Herstellern und Projektierern. Zwischen Normen für elektrische, physikalische und IT-Sicherheit klafft aus den selben Gründen

eine Lücke an verbindlichen Standards für Software-Sicherheit.

## Der Stuxnet-Vorfall

Vorfälle wie Stuxnet werden sich selbst durch die besten Sicherheitsmaßnahmen auch in absehbarer Zukunft nicht hundertprozentig verhindern lassen. Maßnahmen wie Whitelisting und Endpoint-Security-Lösungen helfen neben herkömmlichen Firewalls und Antivirus-Lösungen dabei, solche Risiken zu mindern. Allerdings stoßen auch diese beim Exploitschutz gegen rein speicherresidente Schadsoftware bzw. USB-Angriffe an ihre Grenzen, wie kürzlich auf der Black-Hat-Sicherheitskonferenz in Las Vegas gezeigt wurde.

Der Automatisierungshersteller Siemens machte in der Vergangenheit die Nachlässigkeit von Kunden sowie Fehler im Microsoft-Betriebssystem für den Stuxnet-Vorfall verantwortlich. Das war jedoch nur teilweise richtig. Auch die eigenen Produkte hatten Fehler wie etwa den berühmten WinCC-Datenbank-Bug, die nachhaltig behoben werden müssen, um solche Angriffe wirkungslos verpuffen zu lassen.

---

*Anm.d.Red.: Eine Datenbanksicherheitslücke im HMI-System WinCC ermöglicht einem Angreifer, sich unbefugt Administrator-Rechte zu verschaffen, unter Umständen auch durch Remote-Zugriff auf das System.*

---

Im vergangenen Jahr wurde Siemens von mir darauf aufmerksam gemacht, dass das Simatic Security Update zu Stuxnet diesen Mangel nicht vollständig behebt, sich leicht umgehen lässt und daher ineffizient ist. Nach letztem Kenntnisstand bestehen dieses und weitere Probleme nach wie vor. Näheres wird ein erneuter Test zeigen, der etwa ein Jahr nach der ursprünglichen Untersuchung stattfinden soll.

## Vernebelungstaktik und intransparente Kommunikation

Der Sicherheitsforscher Dillon Beresford deckte im Mai 2011 eine Reihe von Mängeln in speicherprogrammierbaren Steuerungen auf, die anschließend von Siemens per Salami-Taktik kommuniziert wurden. Zunächst gaben Sprecher des Unternehmens an, die Mängel beschränkten sich auf ein Nischenprodukt (S7-1200) und

seien nur unter „Laborbedingungen“ zustande gekommen. Zudem fehlte Beresford der Einblick in die Technologie. Angebotene Lösungsvorschläge erwiesen sich rasch als ebenfalls umgehbar. Erst als belegt war, dass die erste Argumentation des Anbieters sich nicht halten ließ und auch andere Produktserien betroffen waren, machte Siemens Zugeständnisse.

Nun tritt das ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) vor und konstatiert, es handle sich teilweise gar nicht um wirkliche Mängel, sondern offene Industriestandards (ISO-TSAP) seien die Ursache für vorhandene Sicherheitsdefizite. Ganz im Gegenteil ist jedoch das S7-Protokoll, eine proprietäre Siemens-Technik, die Ursache dafür, dass Schutzmechanismen nicht wie erwartet greifen. Selbst wenn die Probleme auf Standards zurückzuführen wären, bliebe die Frage offen, wer etwas daran ändern könnte, wenn nicht die marktführenden Hersteller.

Das ICS-CERT soll als Regierungsstelle Sicherheitsforscher und Hersteller koordinieren und Endanwendern als neutrale Instanz bei der Risikominimierung helfen. Nach mehr als drei Monaten sind jedoch leider immer noch keine vollständigen Angaben darüber verfügbar, welche SPS-Serien von welchen Problemen konkret betroffen sind oder nicht. Dabei wäre dies leicht zu ermitteln. Der amerikanische Kollege Dale G. Peterson mutmaßt, das ICS-CERT sei so sehr in Geheimhaltungsvereinbarungen mit den großen Herstellern verstrickt, dass es seine Aufgabe nicht effektiv erfüllen könne. Was auch immer die Gründe sein mögen, klar ist jedoch, dass die Endkunden die Leidtragenden sind, da sie weder vom Hersteller noch vom ICS-CERT vollständige Informationen erhalten.

Zu allem Übel wurde Beresford in dem Papier des ICS-CERT nicht einmal namentlich erwähnt. Vielleicht ist das die Konsequenz daraus, dass er auf der Black-Hat-Konferenz die Anmeldedaten für die Backdoor in der Firmware

der S7-300er-Serie veröffentlichte. Beresford hat die Zusammenarbeit daher vorläufig eingestellt und nannte es ein schlechtes Signal für andere, dass weder sein Name genannt noch Lohn für seine Arbeit bezahlt wird.

Die offengelegte Backdoor wurde in offiziellen Verlautbarungen als „Test- und Diagnosefunktion“ bezeichnet. In der Änderungshistorie heißt es dazu kryptisch: „Addressing the Web server after a firmware update no longer causes Defect Z1:8000“. Ein Advisory verfasste Siemens erst nach Beresfords Veröffentlichung. Transparente Kommunikation sieht meines Erachtens anders aus.

### Auswege aus dem Dilemma

Stehen Sicherheitsprobleme im Raum und bestreitet der Hersteller diese, sollten Kunden sich vom Hersteller schriftlich bestätigen lassen, dass entsprechende Aussagen unbegründet sind. Geboten ist das auch bei langjährigen Partnerschaften. Schließlich könnten Versicherungen Schadenersatzzahlungen verweigern, wenn eine eigentlich bekannte, aber nicht behobene Sicherheitslücke einen Schaden ermöglichte. Verfügt der Betroffene dann über schriftliche Garantien des Herstellers, kann er Schäden ihm gegenüber geltend machen.

Zudem sollten Service Level Agreements mit festen Fristen zur Beseitigung von Sicherheitsmängeln vereinbart werden, die auch über die Garantiezeit hinaus gelten. Das gewährleistet die zeitnahe Eliminierung von Risiken sowie den dauerhaft sicheren Anlagenbetrieb. Um die internen Kompetenzen und die eigene Position gegenüber den Herstellern zu stärken, sollte die Zusammenarbeit zwischen IT-Abteilung und Anlagentechnikern gefördert werden, beziehungsweise direkt eine interdisziplinäre Task Force eingerichtet werden. Vorbereitungen für den Tag X sind proaktives Risikomanagement und sollten ebenso Routine sein wie ein Feueralarm.

Darüber hinaus zeigen Security Audits und Penetration Tests durch externe Berater die Sicherheitslage im Unternehmen auf. Das schafft klare und nachvollziehbare Fakten, anstatt „Fear, Uncertainty and Doubt“ (FUD; Furcht, Ungewissheit und Zweifel). Ein Tag Consulting kostet nicht viel, eine Stunde Stillstand dagegen schon. Audits, die von den Herstellern bezahlt werden, wenden Methodiken an und fördern Ergebnisse zutage, die der Kunde weder erfährt noch nachprüfen kann. Mehr Sicherheit schafft daher die Kontrolle durch unabhängige Sicherheitsberater, da diese die Interessen des Kunden vertreten und nicht die Politik eines Herstellers.

Kunden sollten die Hersteller ihrer Systeme dazu auffordern, ein Bug-Bounty-Programm zu betreiben. Nur ein finanzieller Anreiz kann ein Gegengewicht zum Grau- und



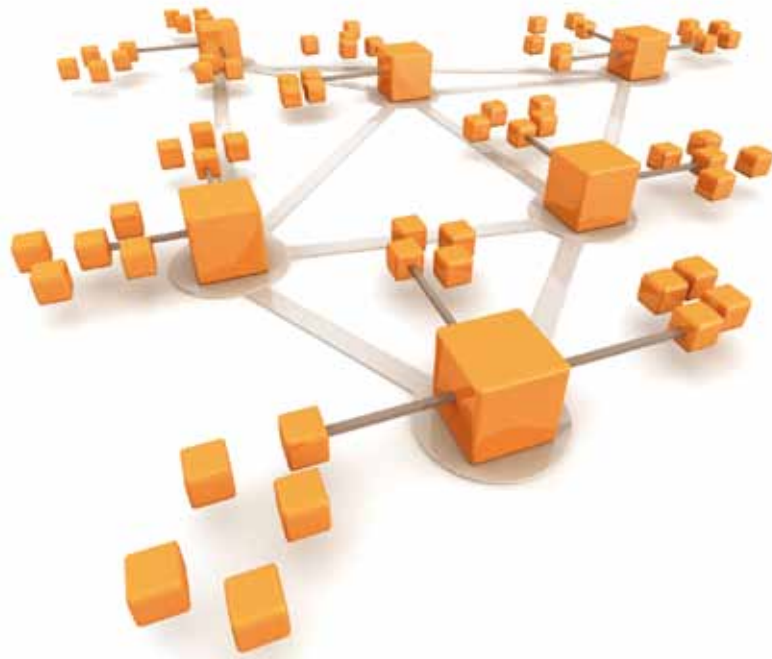
„Security Audits und Penetration Tests durch externe Berater zeigen die Sicherheitslage im Unternehmen auf“, empfiehlt Oliver Sucker, Inhaber der IT-Sicherheits- und Beratungsfirma Forensic Investigations.

Schwarzmarkt schaffen, auf dem viel Geld für Informationen über Sicherheitsschwachstellen bezahlt wird. Dort zirkulierende Exploits stellen eine erhebliche Bedrohung für alle Anwender dar. Bug-Bounty-Programme sorgen zudem dafür, dass unabhängige Sicherheitsforscher Zeit in die Untersuchung von Produkten mit unterschiedlichsten Methoden investieren können. Wer seine Produkte tatsächlich für sicher hält, kann leicht eine Prämie auf Sicherheitslücken aussetzen. Das praktizieren sogar einige nichtkommerzielle Open-Source-Projekte wie Mozilla in weit weniger sicherheitsrelevanten Bereichen. ■

# Malwareschutz für Produktionsnetze

Marcus Stahlhacke, Business Consultant bei der Norman Data Defense Systems GmbH

**Da Malwareschutz auf Produktionssystemen häufig nicht genutzt werden kann, bietet es sich an, den Virenschutz auf externe Hardware auszulagern.**



Nicht nur Office-Systeme, sondern auch Produktionsumgebungen müssen vor Malware geschützt werden. Da Schutzlösungen auf produktionsspezifischen Komponenten die Produktionsprozesse beeinträchtigen können, werden sie häufig nicht genutzt. Als Alternative bietet sich an, den Malwareschutz auf externe Hardware auszulagern und so bestehende Netzwerktopologien und Komponenten unangetastet zu lassen.

Malware-Angriffe beschränken sich heute längst nicht mehr auf die Office-Welt. Mit Stuxnet ist deutlich geworden, dass Produktionsumgebungen ein lohnendes Ziel für Angreifer darstellen und Angriffe erfolgreich sein können, da Prozesssteuerungssysteme traditionell nur wenig geschützt sind. Viele unterschiedliche Produkte im Segment und proprietäre Software mit geringem Bekanntheitsgrad waren über lange Zeit Schutz genug. Die Produktionssysteme blieben darüber hinaus relativ lange von der Außenwelt abgeschirmt, und ohne Verbindung zu Office-Rechnern und zum Internet bzw. abgeschottet durch eine Firewall war die Infektionsgefahr tatsächlich gering.

Inzwischen jedoch verbindet Industrial Ethernet die Office- mit der Produktionswelt und ermöglicht die zentrale Steuerung aller Prozesse direkt aus den PPS- (Produktionsplanungs- und Steuerungs-) und ERP- (Enterprise

Ressource Planning) -Systemen heraus. Malware, die über Lücken wie ungepatchte Schwachstellen oder infizierte mobile Geräte wie USB-Sticks, Notebooks oder Mobiltelefone ins Office-Netz eindringt, kann jetzt allerdings auch ungehindert bis in SCADA-Umgebungen und Produktionsnetze vordringen.

## Scanprozess kann Echtzeitprozesse stören

Die Office-Welt hat im langjährigen Kampf gegen Malware praktikable Schutzstrategien und -produkte entwickelt. Diese lassen sich jedoch nicht ohne weiteres auf Produktionsumgebungen übertragen: Die Praxis zeigt, dass etwa bestehende On-Access-Scanner auf Produktionsrechnern so gut wie nie genutzt werden, weil der Ressourcenbedarf des Scanprozesses den Verkehr der Produktivdaten beeinträchtigen und den Produktionsprozess zum Erliegen bringen kann. Weiterhin besteht die Gefahr, dass Virens Scanner Steuerungsprozesse stören. Als Echtzeitprozesse müssen diese auch im ungünstigsten Fall definierte Antwortzeiten einhalten, damit es nicht zu Personen- oder Sachschäden kommt.

Anders als in der Bürowelt, in der PCs unabhängig voneinander agieren und abends ausgeschaltet werden, sind Produktions-PCs zur Steuerung komplexer Maschinen und Anlagen

aufeinander abgestimmt und rund um die Uhr in Betrieb. Eine Unterbrechung des Gesamtablaufes durch ein Reboot-Update an Produktions-PCs hat deshalb Produktionsausfälle zur Folge und verursacht enorme Kosten. Bei PC-Systemen, die Bestandteil von Maschinensteuerungen sind, kann das Aktualisieren und Patchen der Software eine Veränderung des Systems darstellen, die zum Verlust der Herstellergarantie führt. Produktionsnahe PC-Systeme laufen deshalb meist mit älteren, seit Jahren nicht aktualisierten oder gepatchten Betriebssystemen und Anwendungen.

## Separate Hardware für den Malware-Scan

Angesichts transparenter Fertigung, die jederzeit Einblick in Ablauf und Status jedes Produktionsauftrages gewährt, kann und will kein Unternehmen zurück zu den Zeiten, in denen ein Mitarbeiter einmal täglich die Maschinendaten für das Update des PPS-Systems auf einen USB-Stick zog. Als Alternative zur herkömmlichen Trennung von Produktions- und Büronetz werden Schutzlösungen benötigt, die sich zügig und möglichst ohne Beeinträchtigung des Betriebs in eine bestehende Umgebung installieren lassen.

Hierfür eignen sich separate Hardware-Komponenten, die am Office-seitigen Zugang des Engineering-Plat-

zes installiert werden. Auf sie wird die die Scan-Lösung ausgelagert mitsamt den Prozessen, die auf den Produktionssystemen nicht erwünscht sind. Erforderlich für den Einsatz der Virenschutz-Appliance ist eine Gliederung des Netzwerks in Zonen unterschiedlicher Kritikalität, wie sie Richtlinien wie VDI/VDE 2182 auf nationaler Ebene und als quasi-internationale Norm ISA-99 der International Society of Automation im Rahmen der Maßnahmen und Vorgehensweisen für die sichere Erstellung und den sicheren Betrieb von Produktionsnetzen beschreiben.

Beim Malware-Scan mittels Appliances wird der Datenverkehr über zwei Netzwerkschnittstellen durch den Scanner geleitet und in beiden Fließrichtungen auf Malware geprüft. So wird nicht nur das Produktionsnetz vor Malware aus dem Office-Bereich geschützt. Es lassen sich auch bisher unerkannte Infektionen des Produktionssystems aufspüren. Eine dritte Schnittstelle, im Unterschied zu den beiden anderen mit IP-Adresse, dient als Administrationszugang bzw. zur Einbindung in SNMP-Konsolen und zum Absetzen von Alarmmeldungen. Vor allem aber ermöglicht sie die automatische Aktualisierung von Signaturen und Scan-Engine über das Internet. Die von Norman angebotene Lösung Norman Network Protection scannt alle für die Malware-Übertragung relevanten Protokolle wie CIFS, SMB/SMB2, HTTP, FTP, SMTP, POP3, RPC, TFTP und IRC, blockt BitTorrent und MSN und hat eine URL-Blockliste, die manuell gepflegt werden kann.

### Transparent und unabhängig

Wichtigste Voraussetzung für den Einsatz der Inline-Detection-Lösungen in Produktionsumgebungen sind Transparenz sowie Unabhängigkeit von Netzwerktopologien und bestehenden Komponenten. Sie werden deshalb in der Sicherungsschicht des OSI-Referenzmodells ausgeführt und müssen den Komponenten weder als

Proxy oder Gateway mitgeteilt werden noch Eigenschaften des Kommunikationsnetzes berücksichtigen. Sie arbeiten unabhängig davon, welches Betriebssystem oder welcher Rechnerartyp zu schützen ist. Da keinerlei Änderungen an bestehenden Systemen und Komponenten notwendig sind, werden Herstellergarantien nicht tangiert. Die Konfigurationsar-

beiten beschränken sich auf das Hinzufügen einer IP-Adresse zum Administrations-Port der Inline-Appliance – Installation und Inbetriebnahme sind also mit wenigen Handgriffen machbar. Die von Proxy-basierten Produkten bekannten Latenzzeiten werden durch paketbasiertes Scannen auf nicht wahrnehmbare Größenordnungen verringert. ■

### Es muss nicht gleich Stuxnet sein

Jede beliebige Malware kann einen Produktionsrechner infizieren und einen unter Umständen mehrstündigen Produktionsstillstand bis zur Bereinigung verursachen. In milchverarbeitenden Betrieben wie Royal FrieslandCampina verdirbt in einem solchen Fall Milch gleich hektoliterweise: Damit sie zu Joghurt, Frischkäse oder anderen Produkten werden kann, wird sie gekühlt, erhitzt, gerührt, gepresst, geknetet oder mit speziellen Bakterien oder Pilzen geimpft. Die Temperaturführung und die Dauer einzelner Arbeitsschritte dürfen dabei nicht über- oder unterschritten werden.



Kommt es bei Royal FrieslandCampina zu einem Produktionsstillstand, verdirbt Milch zur Käseproduktion gleich hektoliterweise.

Ein neunstündiger Stillstand bei der Käseherstellung, den Schadcode in einem der Betriebe verursacht hatte, zeigte FrieslandCampina die Verwundbarkeit der Produktionseinrichtungen und stieß deren Absicherung an. Die neue Lösung sollte keine Änderungen an den bestehenden Bestandteilen des Produktionsnetzes erforderlich machen, den Verkehr der Produktionsdaten nicht beeinträchtigen und nicht zu Zeitverzögerungen führen, da Milchverarbeitung automatisiert stattfindet und sekundengenau überwacht wird. Nach umfangreichen Tests entschied sich FrieslandCampina für Norman Network Protection. Gemeinsam mit Norman ermittelte FrieslandCampina die strategisch sinnvolle Positionierung der einzelnen Inline-Scanner in den Netzwerken und rollte sie in allen Betrieben aus. Ein Malware-bedingter Produktionsstillstand ist seither nicht wieder vorgekommen.

# Netzsegmentierungen in Prozessleitnetzen

Thomas Gronenwald und Florian Thiessenhusen, Security Consultants bei der Admeritia GmbH

**Netzwerksegmentierungen verhindern den ungefilterten Zugriff auf ein SCADA-System, wenn sich Corporate-LAN und Prozessleitnetz nicht strikt voneinander trennen lassen. Firewalls teilen das Netzwerk auf und filtern den Verkehr zwischen den einzelnen Segmenten.**

Automatisierungs- und Prozesssteuerungssysteme werden weltweit in nahezu allen Industrieunternehmen eingesetzt. Der Trend und die Entwicklung gehen dabei weg von proprietären und isolierten Feldbussystemen hin zu standardisierten und gekoppelten Netzwerken.

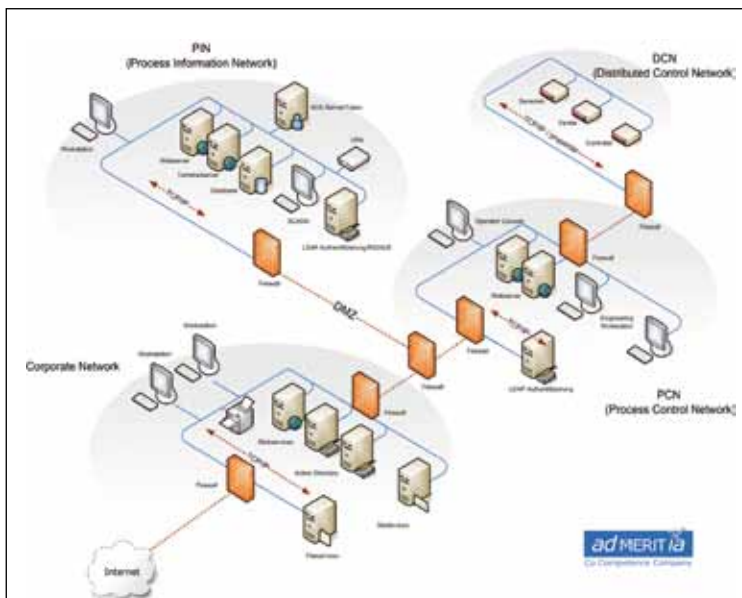
Doch welche Sicherheitsrisiken bergen solche Entwicklungen in der Automatisierungs- und Prozesssteuerungstechnik innerhalb von kritischen Infrastrukturen und wie können Unternehmen diesen entgegenwirken?

In der jüngeren Vergangenheit tauchten viele Schwachstellen in den Anlagen führender Industrieunternehmen auf. Dadurch rückt das Thema Sicherheit verstärkt in den Fokus von Verantwortlichen, Betreibern und Sicherheitsexperten. Einer der bedeutendsten Vorfälle war sicherlich der Stuxnet-Virus. Dieser Schadcode wurde von einer mutmaßlich kriminellen Vereinigung entwickelt, um Steuerungssysteme der Firma Siemens gezielt anzugreifen.

Im gegebenen Fall richtete sich der Schadcode gegen spezielle Frequenzrichter, die in verschiedenen Kraftwerken vorkommen. Das Ziel des Angriffs waren die Manipulation und somit die Zerstörung der Geräte. Einerseits basierte der Schadcode auf einer Schwachstelle innerhalb des Steuerungssystems, andererseits musste er sich bis an die entscheidenden Stellen weiterverbreiten. Dies kann nur dann funktionieren, wenn der Schadcode durch unsichere IT-Anlagen eingeschleust und durch fehlende Netzwerksegmentierungen weiterverbreitet werden kann. Beides ist selbst bei führenden Energieerzeugern noch heute möglich.

Die Anforderung der Bereitstellung von gesammelten Prozessdaten zu Abrechnungs- oder Überwachungszwecken bedingt eine Kopplung zum Corporate-LAN (Büronetz) und macht eine bestehende Netzwerkverbindung zu potenziell gefährlichen Netzen (Corporate, Internet) unausweichlich. Das BSI empfiehlt in seinen Maßnahmenkatalogen in solchen Fällen die strikte Trennung der Netze zumindest durch eine Firewall (Paketfilter). Jedoch ist dies in der Praxis vergleichsweise selten zu finden. Netztrennungen sind nicht vorgesehen oder gar mangelhaft implementiert. Ein direkter ungefilterter Zugriff vom Corporate-LAN zum SCADA-System ist so zumeist möglich.

Die wichtigste Maßnahme bei der Absicherung von Prozessleitnetzen ist somit die Absicherung der Basis, also des Netzwerks. Unter Zuhilfenahme von Firewalls wird dieses in Netzsegmente aufgeteilt. Die Firewall filtert den Verkehr zwischen diesen Segmenten.



## Netzsegmentierung zwischen Corporate-LAN und Produktionsnetz

Dieser Netzplan zeigt eine Segmentierung der einzelnen aufgebauten Netzwerkstrukturen zwischen Corporate-LAN und Produktionsnetz. Ein so genanntes Zonenmodell kommt zum Einsatz, bei dem Systeme und Systemgruppen klassifiziert und anschließend segmentiert werden.

Der Netzübergang zum Corporate-LAN wird durch drei Firewalls abgesichert. Eine Firewall davon stellt eine DMZ (Demilitarized Zone) zur Verfügung. Diese dient als Transfernetz von Daten, die zwischen Produktionsnetz und Corporate-LAN ausgetauscht werden müssen (Messdaten u.a.). Ein direkter Zugriff aus dem Corporate-LAN ins das DCN ist nicht möglich.

Zudem ist das DCN durch zwei Firewalls vom PCN getrennt. Die Besonderheit dabei ist, dass bei den Aktoren häufig proprietäre Protokolle zum Einsatz kommen. Das muss bei der Beschaffung und Implementierung der Firewall berücksichtigt werden.

In der Praxis sind solche Projekte nicht so einfach umzusetzen wie in vergleichbaren Büronetzwerken. Die Projekte sind wesentlich komplexer, dauern länger und bedingen eine größere Vorbereitung.



# Hackern auf der Spur

Thomas Heinen,  
freier Journalist aus Köln

**Im Gespräch mit Toralv Dirro,  
Security Strategist bei McAfee,  
über Malware-Gefahren für  
SCADA-Systeme.**



**SecuMedia: Herr Dirro, Stuxnet hat weltweit eine Vielzahl an Unternehmen infiziert. Welche Schäden richtete der Wurm dabei an?**

Toralv Dirro: Man muss bei Stuxnet zwischen der Gefahr durch dessen gezielte Schadensfunktion und der Angriffsfunktion durch die Infektion selbst unterscheiden.

Die Schadensfunktion von Stuxnet ist auf ganz bestimmte Systeme in ganz bestimmten Situationen eingegrenzt und vermutlich nur für die zunächst attackierten Unternehmensstandorte im Iran relevant.

Im Anschluss an diesen Vorfall hat sich der Wurm weiterverbreitet und die Systeme zahlreicher anderer Unternehmen infiziert, aber ohne dabei Industrieanlagen zu manipulieren.

**SecuMedia: Kamen bei diesen späteren Infektionen Stuxnet-Varianten zum Einsatz?**

Dirro: Nein, das war der Standard-Stuxnet. Er infizierte Systeme verschiedener Unternehmen, doch seine Schadensfunktion konnte nur in einer ganz bestimmten Konfiguration ausgelöst werden, die auf die Anlagen im Iran abgestimmt war.

**SecuMedia: Können Sie Beispiele anderer Infektionen und dabei agierender Würmer nennen?**

Dirro: Kürzlich wurde medizinisches Gerät in einem Krankenhaus infiziert, das ähnlich funktioniert wie Industriekontrollsysteme. Dabei wurden der vor einigen Jahren weitverbreitete Wurm Sapphire sowie der Wurm Conficker eingesetzt.

Größere Geräte oder Anlagen werden häufig mit normalen Standard-PCs gesteuert, die auf Betriebssystemen wie Microsoft Windows XP Embedded oder Windows CE basieren. Im genannten Fall steuern solche PCs die medizinischen Geräte des Krankenhauses. Die Sicherheitsprobleme bei Industrieanlagen sind dieselben wie bei den Steuerungssystemen für medizinische Geräte.

**SecuMedia: Warum sind diese Systeme anfällig für Malware?**

Dirro: Bei den infizierten Systemen handelt es sich um unternehmenskritische Systeme, die nicht gepatcht oder gewartet werden, weil sie schlichtweg zu wichtig sind, um sie mit jedem neuen Hotfix zu booten. Insbesondere im medizinischen Bereich sind bestimmte Konfigurationen zudem zertifizierte Systeme, deren Zertifizierung nach einem Update erlischt. Nach jedem Update müsste also eine neue Zertifizierung durch den SCADA-Software-Hersteller ausgestellt werden. Aus diesem Grund finden Betriebssystem-Updates, wenn überhaupt, in sehr großen Zeitzyklen statt.

**SecuMedia: McAfee unterhält ein forensisches Team, das Unternehmen unterstützt, die eine Malware-Attacke erlitten. Welche Aufgaben übernimmt dieses Team?**

Dirro: Wenn ein Unternehmen feststellt, dass es in größerem Umfang Opfer eines Hacks wurde und McAfee zu Hilfe ruft, versucht unser forensisches Team, die gesamten infizierten Systeme ausfindig zu machen sowie festzustellen, wie der Angriff erfolgte. Dabei wird geprüft, wie die Angreifer ins Unternehmen gelangt und sich darin vorgearbeitet haben. Nach Möglichkeit wird auch festgestellt, welche Daten entwendet und wohin diese geschickt wurden.

**SecuMedia: Welche Art von Schadsoftware kommt bei solchen Angriffen in der Regel zum Einsatz?**

Dirro: In der Regel werden Trojaner eingesetzt, um erste Systeme zu infizieren. Diese arbeiten sich über eine Fernsteuerung der Systeme weiter im Netzwerk vor, bis genügend Rechte vorhanden sind oder die passenden Rechner gehackt wurden, über die ein Angreifer Zugriff auf die gewünschten Zieldaten erhält.

**SecuMedia: Was sind die größten Sicherheitslücken, die zu einer Infektion von SCADA-Systemen führen?**

Dirro: In der Regel dienen Standard-Betriebssysteme, etwa das noch weit verbreitete Windows NT, als Grundlage für SCADA-Systeme. Im Laufe der Zeit werden verschiedene Sicherheitslücken für diese Betriebssysteme bekannt, die durch Patches behoben werden. Wenn Unternehmen diese Patches aus den oben genannten Gründen nicht einspielen können oder wollen, stehen sie vor einem Problem.

Ein weiteres Problem liegt darin, dass direkte Steuerungssysteme ursprünglich niemals dafür vorgesehen waren, an IP-Netzwerke angeschlossen zu werden. Im Laufe der Zeit wurden jedoch SCADA-Lösungen entwickelt, die es ermöglichen, diese Systeme in IP-Netzwerke einzubinden und Geräte darüber auszuwerten und anzusteuern, wodurch sich eine Reihe finanzieller Vorteile abbilden lassen.

Teilweise werden auf diesen Systemen auch überflüssige Dienste betrieben, die man bereits in der Design-Phase hätte abschalten sollen oder die man über lokale Firewalls absichern sollte.

Zudem sind solche Systeme für ganz andere Laufzeiten ausgelegt als normale Computer. Ein normaler Rechner wird in einem Unternehmen zwischen drei und fünf Jahre eingesetzt, bis er abgeschrieben und durch ein neues Gerät ersetzt wird. Im Prozesskontrollbereich sind Systeme hingegen für eine Laufzeit von zehn bis zwanzig Jahren ausgelegt. Dadurch summieren sich die Sicherheitsprobleme, die dort gefunden werden und ab einem bestimmten Zeitpunkt hören auch die Hersteller von Betriebssystem und SCADA-Software auf, ihre Software mit Updates zu versorgen.

**SecuMedia: Das Hauptproblem liegt also darin, dass SCADA-Systeme bzw. die Sicherheitslücken der PCs, auf denen diese betrieben werden, über IP-Netzwerke und das Internet erreichbar sind?**

Dirro: Das ist richtig. So werden einerseits die Kontrollsysteme und andererseits die eigentliche SCADA-Infrastruktur angreifbar. Die SCADA-Infrastruktur besteht außerdem häufig aus recht komplexer Software, bei deren Design wenig Rücksicht auf die Sicherheit genommen wurde. Hier konnten wir unterschiedliche Sicherheitslücken feststellen, die erst durch die Aufmerksamkeit der Öffentlichkeit nach Stuxnet geprüft wurden.

**SecuMedia: Wie sollte sich ein Unternehmen absichern, das vor Jahrzehnten ein SCADA-System implementiert hat, bei dem Design-Fehler hinsichtlich der Sicherheit begangen wurden, und das nun über ein IP-Netzwerk mit der Office-IT verbunden ist?**

Dirro: Unternehmen sollten sich zunächst eine Übersicht darüber verschaffen, welche Systeme vorhanden sind. Häufig ist einem Netzwerkadministrator nicht bekannt, welche Systeme im Steuerungsbereich eingesetzt werden. Dieser muss also mit den Menschen im Unternehmen zusammenarbeiten, die diese Systeme betreiben.

Optimalerweise sollten diese Systeme in einem komplett abgekapselten Netzwerk betrieben werden. In einigen Unternehmen mag es jedoch schwierig sein, das nachträglich zu realisieren. Ist das der Fall, sollten Unternehmen mit professioneller Unterstützung von Security Consultants prüfen, wie Teile des Netzwerks mit weiteren Zugriffsschutzkontrollen und Firewalls abgesichert werden können. Eventuell ist es möglich, eine kleine Firewall einzusetzen, die alles außer den absolut notwendigen Diensten vor einzelnen Systemen absichert. Systeme, die weiterhin über das Netzwerk erreichbar sind, können mit weiteren Technologien wie der Whitelisting-Lösung McAfee Application Control abgesichert werden. Diese Lösung hat Siemens etwa für seine Steuerungssysteme getestet und für gut befunden.

## Impressum

**Informationsdienst SCADA-Sicherheit**  
Sonderheft Informationsdienst IT-Grundschutz  
**ISSN 1862-4375**

**Herausgeber**  
Sebastian Frank

**Redaktion**  
Thomas Heinen, freier Journalist  
(verantwort. für den redaktionellen Teil)  
Tel.: +49 67259304-0  
E-Mail: redaktion@scada-sicherheit.de

**Verlag**  
SecuMedia Verlags-GmbH  
Lise-Meitner-Str. 4, 55435 Gau-Algesheim  
www.SecuMedia.de  
Beteiligungsverhältnisse (Angabe gem. §9, Abs.4 Landesmediengesetz RLP) Gesellschafter zu je 1/6 sind Gerlinde Hohl, Klaus-Peter Hohl, Peter Hohl (GF), Veronika Laufersweiler (GF), Nina Malchus (GF), Stefanie Petersen.  
Registereintragung: Handelsregister Mainz B 22282  
Umsatzsteuer-Identifikationsnummer:  
DE 148266233

**Abo-Service**  
Max Weisel, Veronika Strauß  
Tel.: +49 6725 9304-0  
Fax: +49 6725 5994  
E-Mail: aboservice@SecuMedia.de  
www.scada-sicherheit.de

**Anzeigenleitung**  
Birgit Eckert  
(verantwort. für den Anzeigenteil)  
Tel.: +49 6725 9304-20  
E-Mail: anzeigenleitung@SecuMedia.de  
Mediadaten

**Bezugspreise/Bestellungen/Kündigung**  
Erscheinungsweise 4 Mal jährlich  
Abopreis für Basis-Paket:  
2 Ausgaben Print / Jahr  
12,00 € inkl. MwSt. u. Versandkosten (Inland)  
Abopreis für Premium-Paket:  
Leistungen wie Basis-Paket +  
2 Ausgaben als PDF / Jahr (ca. 10 Seiten)  
6 x Newsletter  
Sonderinformationen  
Sonderrabatte auf Veranstaltungen, Bücher usw.  
39,00 € inkl. MwSt. u. Versandkosten (Inland)  
Auslandsangebote auf Anfrage: +49 6725 9304-27

Eine Kündigung ist jederzeit zur nächsten noch nicht gelieferten Ausgabe möglich. Überzahlte Beträge werden rückerstattet.

**Satz/Druckvorstufe**  
BLACKART Werbestudio Schnaas und Schweitzer,  
Stromberger Str. 47, 55413 Weiler

**Druck**  
Hofmann Druck Nürnberg GmbH & Co. KG  
Emmericher Straße 10, 90411 Nürnberg

Urheber- und Verlagsrechte: Alle in diesem Heft veröffentlichten Beiträge sind urheberrechtlich geschützt. Jegliche Verwendung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und Einspeicherung in elektronische Systeme.

Haftung/Gewährleistung: Die in diesem Informationsdienst veröffentlichten Beiträge wurden nach bestem Wissen und Gewissen zusammengestellt. Eine Gewähr für die Richtigkeit und Vollständigkeit kann seitens der Herausgeber nicht übernommen werden. Die Herausgeber haften ebenfalls nicht für etwaige mittelbare und unmittelbare Folgeschäden und Ansprüche Dritter.

Bildnachweis:  
Titelbild (groß) und S. 4:  
© Andrei Merkulov - Fotolia.com  
Titelbild (klein, unten):  
©iStockphoto.com/ Ian Hamilton  
S. 11: ©iStockphoto.com/Christos Georghiou  
S. 16: © khorixas - Fotolia.com  
S. 18: © Pei Ling Hoo - Fotolia.com  
S. 20: ©iStockphoto.com/beatrice preve

# SecuPedia

Die Plattform für Sicherheits-Informationen



## Gratis: Geprüftes Wissen für Ausbildung und Praxis.

SecuPedia ist die neue Plattform, die das gesamte Wissen zum Thema Sicherheit und IT-Sicherheit sammelt und gratis zur Verfügung stellt.

Grundlage ist das seit mehr als 25 Jahren bekannte „Sicherheits-Jahrbuch“, das ab sofort als Onlineversion freien Zugriff erlaubt. Alle Artikel sind redaktionell geprüft.

- Offene Plattform basierend auf dem Wiki-Konzept
- Redaktionelle Überprüfung garantiert
- Gratis Zugriff auf 2000 Schlüsselbegriffe
- Die Autoren: Anerkannte Experten
- Aktuell: Der Artikel des Tages

Lernen Sie die SecuPedia-Plattform kennen: Probieren Sie aus, ob das von Ihnen gesuchte Stichwort vorhanden ist.

[www.secupedia.info](http://www.secupedia.info)



Sponsored by



SecuMedia Verlags-GmbH  
Ingelheim, Tel. +49 6725 9304-0  
secupedia@secumedia.com

[www.secupedia.info](http://www.secupedia.info)



cutting through complexity

# Ihre Zahlen zeigen, welche Risiken auf Sie lauern.

Hackerangriffe nehmen weltweit zu. Viele Unternehmen bieten dabei offene Flanken. Von der Eingabe bis zur Serverspeicherung. Mit interdisziplinären Expertenteams entwickelt KPMG Lösungen, mit denen Sie auch digital auf Nummer sicher gehen. Sprechen Sie mit uns.

## Ihr Ansprechpartner

Jörg Asma  
T +49 221 2073-6233  
jasma@kpmg.com

[www.kpmg.de/risk&compliance](http://www.kpmg.de/risk&compliance)

