

# Industrielle Netzwerksicherheit

## Das Unangenehme mit dem Nützlichen verbinden

Investitionen in Netzwerksicherheit sind wie Versicherungsprämien: selten beliebt weil negativ motiviert, gibt man doch Geld dafür aus, dass Unerwünschtes nicht passiert bzw. der dadurch erlittene Schaden begrenzt bleibt. Der folgende Beitrag zeigt, wie Sie das Unangenehme mit dem Nützlichen verbinden und positive Mehrwerte aus einem sinnvollen Investment in die Sicherheit Ihrer industriellen Netzwerke ziehen können.

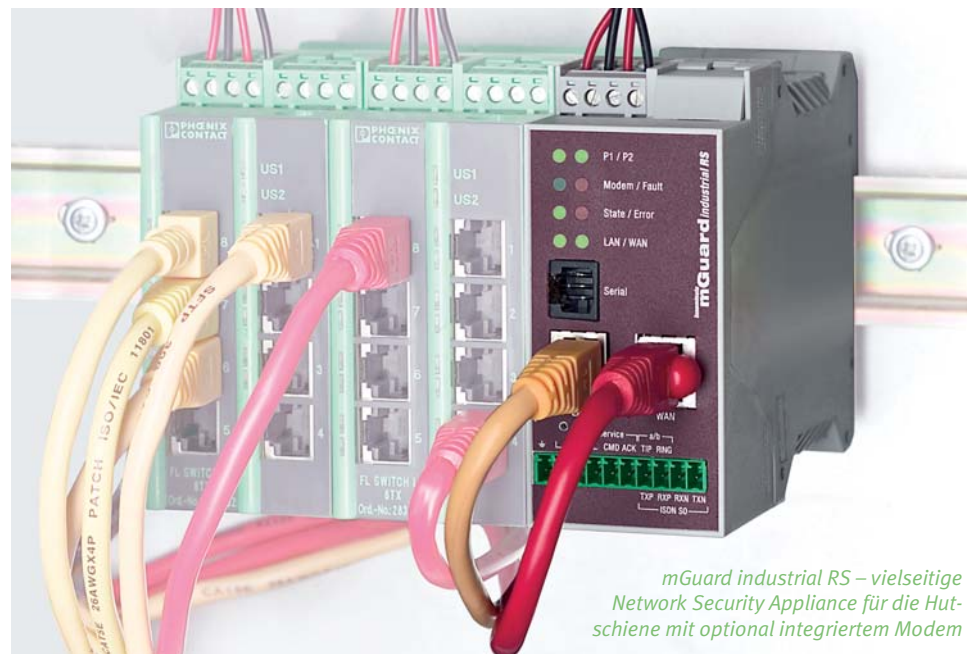
Torsten Rössel

Industrielle Systeme werden zunehmend auf Basis von Ethernet und TCP/IP-Protokollen vernetzt. Leider sind sie infolge dieser Vernetzung



Dipl.-Math.  
Torsten Rössel  
Director Business  
Development,  
Innominate  
Security Techno-  
logies AG

[www.innominate.com](http://www.innominate.com)



mGuard industrial RS – vielseitige Network Security Appliance für die Hut-schiene mit optional integriertem Modem

auch gefährdet. Während sich die Aufmerksamkeit besonders in Nordamerika unter den Schlagworten „Hacking“ und „Cyber Terrorism“ auf Bedrohungen durch gezielte Angriffe konzentriert, spielen in der Praxis eher als Unfälle einzustufende Ereignisse die weniger spektakuläre, aber maßgebliche Rolle: Netzüberlastung durch Defekte und Broadcast-Stürme, Fehlbedienung und das Eindringen oder Einschleppen von Schadsoftware. Die Risiken sind erheblich und reichen vom Produktionsausfall bis zu Gesundheits- und Umweltschäden. Wie z.B. Untersuchungen am Europäischen Forschungszentrum CERN zeigten, sind auch speicherprogrammierbare Steuerungen, die Klassiker der industriellen Automatisierung, durchaus anfällig für Störungen über

Ethernet-Schnittstellen. Hier wurden wiederholt marktgängige SPSen namhafter Hersteller unter Nutzung frei zugänglicher Werkzeuge einem Verwundbarkeitstest unterzogen. Mit neueren Firmware-Ständen fielen die Ergebnisse zuletzt in 2006 zwar etwas besser aus, die Tests führten aber immer noch bei 34% der Steuerungen zu Fehlfunktionen und bei 26% sogar zu Systemabstürzen!

Neben der Verbreitung von Ethernet nimmt auch die Verwendung von Standard IT-Komponenten im industriellen Umfeld zu. Die Systeme werden dadurch offener für gewünschte Integration, leider aber auch für unerwünschte Schädigung. Bekannte Verwundbarkeiten breiten sich aus Büronetzen in die Welt der Produktion aus. Was also tun?

### Defense-in-Depth: verteilter Schutz mit zentralem Management

Als Best Practice wird allgemein eine Defense-in-Depth Strategie empfohlen, die gestaffelt bis zum Schutz kritischer Zellen oder Einzelsysteme reicht, vergleichbar der mit Security Software auf PCs angestrebten Endpunkt-Sicherheit in Büronetzen. Eine Sicherung heterogener industrieller Systeme durch reine Software scheidet aber in der Regel aus, etwa wegen ungenügender Hardware-Ressourcen und weil der Grundsatz „never touch a running system“ permanente Sicherheits-Updates hier inakzeptabel macht.

Innominate hat sich auf die Anforderungen der industriellen Netzwerksicherheit spezialisiert und mit der mGuard Technologie innova-

tive Lösungen geschaffen, die hier einspringen: fertig konfektionierte Network Security Appliances mit integrierter Firmware. Eine Schlüsselrolle kommt der Kontrolle und Filterung von Netzwerkverkehr durch Firewall Appliances mit geeignetem Regelwerk zu. Dabei können unterschiedliche Bauformen als optimale Lösung infrage kommen. Die Palette reicht vom industrietypischen Hutchengerät für den Schaltschrank über integrierbare PCI-Karten für PC-basierte Bedien-Panels und Steuerungen bis zum 19" Chassis mit platzsparenden Blade-Einschüben. Dezentral verteilte Security Appliances lassen Freiheit beim Netzwerk-Design und sind dadurch flexibel und kostengünstig einsetzbar. Von Vorteil besonders für die Nachrüstbarkeit ist, dass die Geräte nicht nur als Router betrieben, sondern auch transparent in ein Netz bzw. vor ein System eingeschleift werden können („Stealth Mode“). Eine Management Software wie der Innominate Device Manager, mit der sich die verteilten Appliances von zentraler Stelle aus umfassend administrieren und weitgehend automatisiert konfigurieren lassen, ist unverzichtbar, um diese Vorteile in großem Stil auszuspielen zu können.

## Firewall-Regeln kann man lernen

Doch wie kommt man zu einem wirksamen Firewall-Regelwerk, besonders bei Nachrüstung in Bestandsanlagen ohne ausreichende Dokumentation? Hier können mGuard Appliances helfen, ein geeignetes Regelwerk buchstäblich zu erlernen. Im „Learning Mode“ werden zunächst alle Verbindungsversuche zugelassen und protokolliert. Mithilfe eines Tools lassen sich diese Verbindungsdaten dann auf eine Essenz von Regeln konzentrieren, die manuell plausibilisiert und schließlich „scharf“ geschaltet werden können. Unbekannte und unerwünschte Verbindungen werden fortan zuverlässig blockiert.

## Mehrwert 1: Effiziente Vernetzung von Zellen mit 1:1 NAT Routing

Die Strukturierung komplexer Produktionsabläufe in vernetzte

Zellen ist weithin geläufig. Dabei hat es große Vorteile, die internen Zellennetze gleichförmig zu gestalten, wenn gleichartige Zellen ihren Dienst in einer Linie verrichten oder mehrere Anlagen des gleichen Typs gebaut werden. Erhebliche Aufwände, die bei Lieferanten und Betreibern für Engineering, Programmierung, Dokumentation und Inbetriebnahme individualisierter Zellennetze erforderlich wären, werden durch dieses „Klonen“ der Zellen vermieden, indem diese intern ein immer gleiches Netz und die Komponenten darin jeweils feste Adressen verwenden.

Dem steht jedoch oft entgegen, dass aus dem übergeordneten Produktionsnetz gezielt mit einzelnen Knoten in den Zellen kommuniziert werden muss. Ein Router mit simpler Network Address Translation (NAT) am Übergang vom Zellennetz zum Produktionsnetz wird dieser Aufgabe nicht gerecht, da die Knoten im Zellennetz von außen dann nicht adressierbar sind. Benötigt wird vielmehr ein Router mit der Fähigkeit, die internen Zellennetze nach außen durch sogenanntes 1:1 NAT ganz oder teilweise auf eindeutige, virtuelle Netze abzubilden. Dies gilt umso mehr, wenn auch die Vernetzung zellinterner Ein/Ausgabe- und Sensor/Aktor-Komponenten nicht mit Feldbussen sondern mit Industrial Ethernet erfolgt, wodurch die Anzahl von IP-Knoten nicht selten auf das 10- bis 20-fache explodiert.

Innominate mGuard Security Appliances leisten diese 1:1 NAT Router Funktionalität mit flexibler Konfigu-

ration und „Wire-Speed“ Performance von 100 MBits/s, verbinden diese gegenüber reinen Routern aber mit der Netzwerksicherheit durch die integrierte Firewall. So bleibt der Zugriff auf die Zellen sauber unter Kontrolle.

## Mehrwert 2: Sicherer Teleservice über Internet

Motive für Teleservice gibt es in allen Lebensphasen einer Maschine oder Anlage: Ferndiagnose und -wartung können Inbetriebnahmen unterstützen, vermeidbare Gewährleistungs- und Service-Einsätze vor Ort einsparen sowie Systemverfügbarkeit und Produktivität optimieren. Dementsprechend ist Teleservice weit verbreitet und wird seit Mitte der 90er Jahre bis heute noch meist über Wählverbindungen per Modem angeboten. Die neue Herausforderung besteht nun im sich abzeichnenden Übergang zu gesicherten Internet-Verbindungen, für den als wesentliche Beweggründe die Stichworte Kosten, Verfügbarkeit, Sicherheit, Bandbreite und Stabilität zu nennen sind.

Innominate mGuard Security Appliances können hier für eine sehr elegante Lösung eingesetzt werden und Maschinen über betreiberseitig initiierte Virtual Private Networks (VPNs) mit entsprechenden Service-Zentren verbinden. Eine solche Lösung erfüllt vielfältige Anforderungen von Anbietern und Betreibern. Das beiden Seiten gemeinsame Bedürfnis nach Netzwerksicherheit wird durch End-to-End VPNs zwischen

Service Center und Anlage erfüllt. Die Zugriffe durch die VPN-Tunnel stehen dabei unter der Kontrolle von Firewall-Regeln.

Anbieter erhalten eine einheitliche, skalierbare Lösung mit zentralem Management, die auch bei im Feld befindlichen Systemen nachgerüstet werden kann und dabei keine Eingriffe in deren Hardware oder Software erfordert. Ferner können IP Adresskonflikte zwischen den privaten Netzwerken der Betreiber durch virtuelle Adressierung überwunden werden. Betreiber erhalten eine nachweislich sichere Lösung auf Basis des führenden offenen VPN-Standards IPsec, die nur minimale Eingriffe in ihre Netzwerke und Firewalls erfordert und Ihnen absolute Kontrolle über die Teleservice-Verbindung gibt.

## FAZIT

Vernetzte industrielle Systeme sind schutzbedürftiger als vielfach angenommen. Dennoch wird der Schutzbedarf allein bisweilen noch nicht als ausreichender bzw. lohnender Investitionsgrund anerkannt. Wir haben als Mehrwert zwei praxisrelevante Anwendungen vorgestellt, die mit der grundlegenden Sicherheitsfunktion dezentraler Security Appliances kombiniert werden können. Das gleiche Infrastrukturinvestment bringt so mehrfachen Nutzen. Mit dem Innominate Device Manager und auf Basis der mGuard Firmware steht hierfür eine vielfach bewährte Familie von zentral managebaren industriellen Network Security Appliances zur Verfügung.

