

# Dezentrale Lösungen bevorzugt

## Industrial Ethernet – Chancen und Risiken

*Die Vernetzung von Produktionssystemen über offene Schnittstellen und Protokolle nimmt deutlich zu. Ethernet und TCP/IP haben nun auch die bisher von Bussystemen dominierten Produktionshallen erreicht und Kommunikationsgrenzen zwischen Office-Netzwerk und Produktionsnetz werden durchlässiger.*

Andreas Beierer und  
Torsten Rössel

■ Synergien und verbesserte Zugriffsmöglichkeiten auf Produktionssysteme sind die gewünschten Effekte, eine durchgängige Sicherheitspolitik die daraus folgende Notwendigkeit.

Denn mit dem Zusammenwachsen von beiden Netzwerkwelten ergeben sich auch Risiken durch das Eindringen von Schadprogrammen oder Fehlbedienungen von innerhalb des Unternehmens. In diesem Beitrag werden geeignete Security-Konzepte für die Produktion betrachtet.

### Perimeter Security vs. Endpoint Security

Nicht von außen – hier schützt in den meisten Fällen eine Unter-

nehmens-Firewall am Internet Zugang – sondern von innerhalb des Unternehmensnetzwerks stammen die meisten Schadprogramme, die Automationsanlagen lahm legen. Der durchschnittliche Schaden, den ein Sicherheitsvorfall durch Viren oder Würmer anrichtet, liegt bei etwa 1,5 Millionen Euro pro Vorfall. Dies berichten die Management-, System- und Technologieberater der PA Consulting Group in einem aktuellen Report.

Die Bedrohungen sind real und müssen in der Sicherheitsstrategie produzierender Unternehmen berücksichtigt werden. Auch die vom CERT (Computer Emergency Response Team) Coordination Center registrierten Störfälle und die dort gemeldeten Sicherheitslücken nehmen seit 2000 mit ca. 50 – 100 Prozent pro Jahr deutlich zu. Für Störfälle im industriellen Bereich sind die Folgen jedoch wesentlich gravierender, als bei Ausfällen im Office-Netzwerk. Fällt eine Produktionsstraße für Stunden aus, so kostet dies in den meisten Fällen sehr viel mehr, als PC-Abstürze im Büro an Schaden verursachen.

Intelligente „Eindringlinge“ können äußere Sicherungssysteme, welche Firmennetze als Ganzes schützen, umgehen. Externe Servicetechniker sind mit Ihren Laptops in der Regel innerhalb von Firmennetzwerken tätig, befinden sich wie auch alle internen Mitarbeiter folglich bereits hinter den zentralen Unternehmens-Firewalls. Die sog. „Perimeter Security“ von Sicherheitssystemen am Rand oder an Übergängen von Netzwerken kann Produktionszellen daher nicht ausreichend schützen.

Dazu bedarf es dezentral wirksamer Konzepte, in der Literatur auch als „Defence-on-depth“ und „Endpoint Security“ bezeichnet, und entsprechender Systeme für die Endgeräte-Sicherheit. Prinzipiell können hierfür Architekturen mit größeren zentralisierten oder kleineren verteilten Sicherheitssystemen zum Einsatz kommen.

### Security Appliances für industrielle Netze

Für die individuelle Absicherung von Produktionszellen unterstützen die mGuard Industrie-Firewalls von Innominate eine dezentral verteilte Architektur. Die mGuard Security Appliances wurden speziell für den Einsatz im industriellen Umfeld konzipiert. Sie kombinieren die Eigenschaften einer Stateful Inspection Firewall, die mit den Optionen für verschlüsselte, authentifizierte Kommunikation über Virtual Private Network Verbindungen (VPNs, insbesondere auch für die sichere Fernwartung über Internet von Interesse). Ihre besondere Tauglichkeit für industrielle Anwendungen wird deutlich in der Erfüllung relevanter Industriestandards und der Integrationsfähigkeit in industrielle Steuerungs- und Bediensysteme (Controller, IPCs, Panel PCs) sowie Maschinen- und Anlagennetze.

Die mGuard Industrie-Firewall kann als eigenständiges System in das Netzwerk integriert werden und schützt dort ein Teilnetz, eine Produktionszelle oder ein einzelnes Automatisierungsgerät. Entscheidender Vorteil des Konzepts ist dabei die völlige Rückwirkungsfreiheit der



Andreas Beierer ist  
Director Marketing &  
Alliances bei  
Innominate Security  
Technologies AG

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



Torsten Rössel,  
Director Business  
Development bei  
Innominate Security  
Technologies AG



**Innominate mGuard bladePack zur platzsparenden, individuellen Absicherung von bis zu 12 Produktionszellen in einem 19“-Gehäuse**

Firewall auf das geschützte System selbst. Dieses von Innominate patentierte Prinzip wird als „Stealth Mode“ Firewall bezeichnet und kann seine Wirkung – auch bei Updates – ohne Eingriffe in das zu schützende System entfalten. Deshalb ist auch eine Nachrüstung bestehender Systeme problemlos möglich. Im Router Mode mit sog. NAT-Funktion (Network Address Translation) können die Geräte als weiteres typisches Szenario auch zur sicheren Anbindung zahlreicher Produktionszellen mit identischem internen Adressraum an ein übergeordnetes Netzwerk genutzt werden.

### Produktbeispiele für Firewalls im industriellen Umfeld

mGuard bladePack ist eine industrielle Sicherheitslösung für den Einbau in 19“-Schränke. Das System ist modular aufgebaut und kann mit bis zu zwölf mGuard blade Einschüben bestückt werden. Um die höchstmögliche Verfügbarkeit zu garantieren, enthält die mGuard bladeBase serienmäßig eine redundante Stromversorgung, die von einer Überwachungseinheit kontrolliert wird und bei Problemen sofort Alarmmeldungen über SNMP Traps an den Administrator leitet. Zusätzlich wird jedes eingesetzte mGuard blade Modul erkannt und überwacht (siehe Bild oben).

mGuard PCI bietet integrierbaren Firewall-Schutz z.B. für Industrie-PCs und auch Roboter, deren Steuer-einheiten häufig auf Standard PC-Systemen basieren. Diese kompakte Firewall Appliance hat PCI Kartenfor-

mat und wird über den PCI Bus des Host Systems mit Strom versorgt. mGuard PCI ist dabei wie alle mGuard Systeme treiberlos (ohne Datenkommunikation über den PCI Bus), völlig transparent und rückwirkungsfrei nutzbar. Alternativ kann mGuard PCI mit Treiber als Netzwerkkarte und Firewall in einem fungieren (siehe Bild unten).

### Verteilte Sicherheitsarchitektur vorteilhaft

Eine 2006 durchgeführte Studie des industriellen Netzwerkplaners Röwaplan AG hat die Gesamtkosten von verteilten und zentralisierten Sicherheitsarchitekturen miteinan-

der verglichen. Beim zentralisierten Ansatz entstehen hohe Investitionskosten, da in diesem Fall sternförmig zu den Produktionssystemen verkabelt werden muss. Die Konzentration von Datenendgeräten je Grundfläche in der Fertigungshalle ist meistens gering, so dass die Auslastung der Switch/Router Module bei der zentralisierten Lösung nicht hoch genug ist, um einen kosteneffektiven Einsatz zu ermöglichen.

Das folgende Beispiel zeigt ein typisches Produktionsszenario mit 44 Produktionssystemen (Datenendgeräten) die auf einer Grundfläche von ca. 30.000 m<sup>2</sup> aufgestellt sind. Die Kosten für Anschaffung und Betrieb über 3 bzw. 5 Jahre sind mit der dezentralen Security-Architektur von Innominate um 50-60 Prozent günstiger als bei Einsatz zentralisierter Netzwerk- und Security-Komponenten.

### Fazit

Über Ethernet werden Maschinen und Produktionssysteme mit der Außenwelt vernetzt. Durch die Standard Netzwerkschnittstellen und die Zugänge zum Firmennetz / Internet werden sie angreifbar. Eine wirtschaftliche Lösung für ausreichende Sicherheit bieten hier nur dezentral wirksame Schutzeinrichtungen mit verteilter Architektur. Damit die erweiterte Sicherheits-Infrastruktur keinen höheren Verwaltungsaufwand nach sich zieht, sind zusätzlich einfach zu bedienende, zentrale Management-Systeme zur Administration und Rechtevergabe gefragt. Spezialisten wie Innominate bieten Lösungen an, die auf die neuen Rahmenbedingungen abgestimmt sind. Eine mGuard-gesicherte Produktionsinfrastruktur gewährleistet, dass Unternehmen das Potenzial der vernetzten Infrastrukturen gefahrlos nutzen können.

### WIR ÜBER UNS

Die Innominate Security Technologies AG ist Markt- und Technologieführer für Embedded Security in industriellen Anwendungen. Der deutsche Security-Spezialist ist in zwei strategischen Geschäftsfeldern tätig: „Industrial Ethernet Security“ und „Secure Remote Maintenance“ für Maschinen und industrielle Anlagen. Mit seiner mGuard Produktfamilie, ergänzt durch eine Device Management Software, bietet Innominate Hardware Firewall-, VPN- und Virenschutz-Funktionalitäten. mGuard Lösungen werden über OEM Partner (Original Equipment Manufacturer) und über ein Netzwerk von nationalen und internationalen Partnern vertrieben.



**Security Appliance mGuard PCI von Innominate ermöglicht integrierbare sichere Vernetzung von IPCs, Panel-PCs u.a. industriellen Systemen**