

# „Leibwächter für Maschinen“ Sichere IT in der Produktion

Konvergenz und Standardisierung sind derzeit die prägenden Trends in der Netzwelt. Kommunikationsbarrieren werden beseitigt, einst klar getrennte Teilnetzwerke wachsen zusammen und sprechen nun die selbe Sprache: TCP/IP und Ethernet sind auf dem Vormarsch und haben jetzt auch die bisher von Bussystemen dominierten Produktionshallen erreicht.

Andreas Beierer



Synergien und verbesserte Zugriffsmöglichkeiten auf Produktionssysteme sind die gewünschten Effekte, eine durchgängige Sicherheitspolitik die daraus folgende Notwendigkeit. Denn mit den „Sprachgrenzen“ verschwinden auch die natürlichen Barrieren für Schadprogramme oder Fehlbedienungen innerhalb des Unternehmens. Dedizierte Lösungen sind gefragt, um die neuen Lücken zu schließen.

## Industrial Ethernet - Chancen und Risiken

6,7 Mio. Industrial Ethernet-Devices - das prognostizieren die Marktforscher der ARC Advisory Group - werden im Jahr 2009 weltweit ausgeliefert („Industrial Ethernet Market Outlook Study“, April 2005). 2004 lag die Menge noch bei weit unter einer Million Geräte. Im Zuge der stetigen Prozessoptimierung treiben immer mehr produzierende Unternehmen die vertikale Integration ihrer Netzwerke voran. Wachstumsraten von jährlich über 50% spiegeln den Wunsch nach nahtlosen Zugriffsmöglichkeiten auf Produktionsdaten und einer effizienten zentralen Produktionssteuerung wider. Industrial Ethernet führt durch standardbasierte Komponenten zu Synergieeffekten und Kosteneinsparungen. Ein ver-

bessertes Supply-Chain-Management wird durch unternehmensweit effizientere Prozesse in Planung, Logistik, Fertigung und Vertrieb erreicht.

Doch die schöne neue vernetzte Welt hat auch ihre Schattenseiten. Nicht nur geplante und erlaubte Zu- und Eingriffe auf und in Produktionsprozesse werden über das gemeinsame Ethernet-Protokoll vereinfacht, auch die Gefahr von Fehlbedienungen steigt. Dort, wo früher die Inkompatibilität der Protokolle Produktionsnetze wie Inseln innerhalb der Unternehmens-IT geschützt hat, sind nun neue Kontrollinstanzen notwendig, die Zugriffe regeln und überwachen. Maschinenausfälle, die durch versehentliche - oder auch mutwillige - Fehlbedienungen an Wartungs- oder Steuerungssystemen verursacht werden, führen schnell zu sehr hohen Kosten. Die Vorfälle werden selten bekannt, doch Szenarien wie dieses entstammen der Realität:

Ein Wartungstechniker versucht, die Verbindung zwischen seinem Notebook und der Steuerung eines Industrieroboters herzustellen. Bei der Eingabe der 12-stelligen IP-Adresse unterläuft ihm ein Zahlenendreher. Der Techniker schickt die neue Konfigurationsdatei über das interne Netzwerk nicht an den zu wartenden Rechner, sondern

an einen Roboter einer anderen Fertigungslinie des Unternehmens. Da dieser Roboter mit der neuen Konfiguration nichts anfangen kann, geht er in Störung, die ganze Linie steht still. Kein Einzelfall: 70-80% aller Störfälle werden nicht durch Angriffe von außen, sondern durch unerlaubte, fahrlässige oder einfach nur unachtsame Zugriffe und Handlungen an Systemen innerhalb des Netzwerks verursacht.

## Dedizierte Sicherheitslösungen gefragt

Nicht von außen - hier schützt in den meisten Fällen die zentrale Unternehmensfirewall - sondern innerhalb des Unternehmensnetzwerks stammen auch die meisten Schadprogramme, die Automationsanlagen lahm legen. Der durchschnittliche Schaden, den ein Sicherheitsvorfall durch Viren oder Würmer anrichtet, liegt bei etwa 1,5 Mio. Euro pro Vorfall. Dies berichten die Management-, System- und Technologieberater der PA Consulting Group in einem aktuellen Report. Ihrer Ansicht nach zieht die Prozessautomatisierung außerdem zunehmend die Aufmerksamkeit von Hackern auf sich. Bereits 13% der Sicherheitsvorfälle in diesem Umfeld von 2002 bis 2005 können als Sabotage klassifiziert werden.

Die Bedrohungen sind real und müssen in der Sicherheitsstrategie produzierender Unternehmen berücksichtigt werden. Office-Lösungen wie Software-Firewalls eins zu eins auf die Produktion zu übertragen funktioniert nur bedingt. Die Anforderungen sind zu verschieden, spezialisierte Lösungen gefragt. Entscheiden sich Unternehmen für den Einsatz dedizierter Lösungen zum Schutz der Einzelnetze, müssen sie außerdem darauf achten, dass ein einfaches und unternehmensweites Management aller Zugriffsrechte und Regeln immer noch möglich ist.

**Produktionsspezifische Anforderungen an die Security**

Ein grundlegendes Verständnis der Rahmenbedingungen in der Automatisierung ist die Voraussetzung für die richtige Wahl einer effizienten, unternehmensweiten Sicherheitslösung.

- Zum Teil werden in der Produktion - aus Kostengründen und weil sie verlässlich die benötigte Performance bieten - ganz bewusst ältere Prozessortechologien oder Betriebssysteme eingesetzt. Allein dieser Umstand schließt bereits den Einsatz von Software-Sicherheitslösungen aus, weil für sie die vorhandenen Systemeigenschaften und -leistungen nicht ausreichen oder sie vom älteren Betriebssystem nicht unterstützt werden.
- Eine rein softwarebasierte Sicherheitslösung, die von zentraler Stelle auf alle IT-Systeme aufgespielt wird, eignet sich für manche Branchen ohnehin nicht. In Chemie- oder Pharma-Industrie müssen bestimmte Maschinen validiert werden, bevor sie überhaupt den Betrieb aufnehmen

	Büro	Produktion
Zuverlässigkeit	Gelegentliche Fehler tolerierbar „Beta Test“ im Feld üblich	Unterbrechungen nicht hinnehmbar Ausgiebige Qualitätssicherung vorausgesetzt
Risiko	Verlust von Daten	Verluste bei Produktion, Anlagen oder möglicherweise Gesundheit und Leben
Performance	Hoher Durchsatz Lange Laufzeiten im Netz akzeptabel	Geringerer Durchsatz hinnehmbar Lange Laufzeiten kritisch
Wiederanlauf	Lange Zeiten für Wiederherstellung/-anlauf akzeptabel	Schneller Wiederanlauf/Austausch essentiell
Risiko-Management	Wiederanlauf durch Reboot Safety spielt keine Bedeutung	Hohe Fehlertoleranz erforderlich
Homogenität	In der Regel homogenes Umfeld (Betriebssystem etc.)	Sehr heterogen
Security	Zentrale Firewall Gateway-Ansatz	Dezentrale Sicherung von Systemen

Anforderungen an IT-Sicherheit in Büro und Produktion

dürfen. Jede Veränderung - beispielsweise durch regelmäßig notwendige Sicherheits-Patches - zöge erneut den Zertifizierungsprozess nach sich, während dessen die Maschine zwei Wochen oder länger nicht einsatzfähig wäre.

- Entscheiden sich Unternehmen für Hardware-Lösungen, so gilt es, die speziellen Rahmenbedingungen zu beachten: notwendige Robustheit und Ausstattung um Vibrationen, Hitze und Staub zu widerstehen, eine Versorgungsspannung von meist 24 Volt anstatt von 220 Volt im Büro - diese Bedingungen machen den Einsatz von Security-Lösungen aus der Bürowelt unmöglich.

Der Logik dieses Ausschlussverfahrens folgend, erscheinen Hardware-Lösungen, die direkt vor die einzelne Maschine oder die Maschinengruppe geschaltet werden können, als geeignete Lösung zur Absicherung hochsensibler und teurer Produktionsanlagen.

**Industrial Ethernet Security**

Mittlerweile sind sogenannte Security Appliances am Markt, die den Datenverkehr auch in Produktionsnetzen absichern können. Die Hardware-Firewall mGuard industrial wurde beispielsweise speziell für den Einsatz im industriellen Umfeld konzipiert. Sie kombiniert die Eigenschaften einer Stateful Inspection Firewall, die eingehende und ausgehende Datenpakete an Hand vordefinierter Regeln überwacht, mit der Möglichkeit einer sicheren und vertraulichen Kommunikation über Virtual Private Network-Verbindungen (VPN) und Virenschutz. Ihre besondere Tauglichkeit für industrielle Anwendungen wird auch in der Erfüllung relevanter Industriestandards, der Hutschienenmontage und der einfachen Bedienbarkeit deutlich.

Die Industrie-Firewall kann als eigenständiges System in das Netzwerk integriert werden und schützt ein Teilnetz, die Produktionszelle oder das einzelne Automatisierungsgerät. Eine entscheidende Komponente des Konzepts ist die völlige Rückwirkungsfreiheit der Firewall auf das System selbst.

Die patentierte „Stealth Mode“-Firewall des Berliner Sicherheitsspezialisten Innominat wird transparent der Maschine vorgeschaltet und nutzt die IP-Adresse der Maschine - für mögliche Angreifer ist die Firewall dadurch unsichtbar. Die Stealth-Firewall kann ihren Schutz entfalten, ohne dass sie das zu schützende System berührt. Eingriffe in das Betriebssystem oder Konfigurationen an der Maschine sind auch bei Sicherheitsupdates nicht notwendig. Des-



Innominat mGuard bladePack zur Absicherung einer großen Zahl verschlüsselter Übertragungskanäle

# Industrie-Netzwerke: Harte Bandagen fürs Ethernet

Der Erfolg eines Unternehmens hängt heute maßgeblich von der Intelligenz und Geschwindigkeit seiner Geschäftsprozesse ab. Auch die Produktion ist längst ein Wettlauf gegen die Zeit geworden, der mit bisher üblichen Bussystemen nicht mehr zu gewinnen ist.

Der schnelle Ethernet-Standard, umgelegt auf industrielle Anwendungen, kann hier Abhilfe schaffen. Das ursprünglich für den Betrieb in Büroumgebungen entwickelte Ethernet muss sich allerdings im harten Einsatzgebiet der Industrie neuen Herausforderungen stellen.

Die Netzwerkkomponenten stoßen in der Industrie auf ungleich härtere Belastungen als im Bürobetrieb. Staub, Schmutz, Flüssigkeiten, Öle, Vibrationen und mechanische Belastungen sind die häufigsten. Sie können den Datenfluss ernsthaft gefährden und sogar gänzlich zu Fall bringen. Der Schweizer Cabling-Spezialist R&M hat daher eine entsprechende Produktpalette entwickelt - mit dem Ziel, maximale Datensicherheit für Industrial Ethernet zu erreichen.

Das Programm umfasst verschiedene Schutzklassen für unterschiedliche Anwen-



Spezielle Produkte von R&M schützen Ethernet-Verbindungen in der rauen Welt der Industrie

dungen: vom Einsatz in Werkstätten (geringe Belastung) über feucht-nasse Bereiche (z. B. Spritzwasser, Schmutz) bis zu harten Belastungen (z. B. gänzlich untertauchen, feiner Staub, Öl). Die R&M-Produkte schützen Netzwerkanschlüsse sowohl bei offenen als auch bei geschlossenen Verbindungen vor dem Eindringen von Feuchtigkeit oder schädlichen Substanzen. Darüber hinaus sorgen sie auch bei mechanischen Einflüssen wie Vibrationen oder Gewaltanwendung dafür, dass das Netzwerk voll verfü-

bar bleibt. Das modulare, einheitliche System gibt es für Kupfer- ebenso wie für Glas- und Polymerfaserverbindungen.

Weitere Informationen zu den innovativen Produkten für Industrial Ethernet erhalten Sie bei R&M Austria. Ihr Ansprechpartner: Norbert Likan.

R&M Austria GmbH  
Seybelgasse 6-8, 1230 Wien  
Tel. 01 / 865 32 00-105  
E-Mail: [norbert.likan@rdm.com](mailto:norbert.likan@rdm.com)  
[www.rdm.com](http://www.rdm.com)

PROMOTION

Security Appliance  
mGuard industrial von  
Innominate ermöglicht  
sicheren Datenverkehr  
im Industrial Ethernet.



halb ist auch eine Nachrüstung bestehender Systeme problemlos möglich.

Gesicherte Maschinen können über DSL direkt an Fernwartungs- und Fernwirkanwendungen angeschlossen, Automatisierungsgeräte durch einen sicheren VPN-Tunnel über das Intranet erreicht werden. Wartungstechniker können nun über das Internet die Fernwartung eines Systems bei einem Kunden durchführen, ohne dass die

Gefahr der Ausspähung, des Angriffs oder des Missbrauchs besteht. Die sichere Datenübertragung kann über den gebräuchlichen Standard IPsec - optional getunnelt über HTTPS und Proxy Server - realisiert werden.

## Fazit

Über Ethernet werden Maschinen und Produktionssysteme mit der Außenwelt vernetzt. Durch die Schnittstellen und die gemeinsame Sprache werden sie angreifbar, weshalb ihnen „Leibwächter“ zur Seite gestellt werden müssen. Damit die erweiterte Sicherheits-Infrastruktur keinen höheren Verwaltungsaufwand nach sich zieht, sind zusätzlich einfach zu bedienende, zentrale Management-Systeme zur Administration und Rechtevergabe gefragt.

Der Markt für Industrial Ethernet ist jung, aber stetig wachsend. Es ist wichtig,

„Office-Lösungen wie Software-Firewalls eins zu eins auf die Produktion zu übertragen funktioniert nur bedingt.“ -

**Andreas Beierer**

ist Director  
Marketing &  
Alliances  
Innominate

Security Technologies AG -  
[www.innominate.com](http://www.innominate.com)



gerade zu Anfang parallel zur Phase der Planung und Implementierung der neuen Netzwerkinfrastrukturen ein unternehmensweites Sicherheitskonzept zu verwirklichen und kostspielige Vorfälle von Anfang auszuschließen. Nur so können alle Entscheidungsebenen im Unternehmen Vertrauen in die neuen Möglichkeiten fassen. □