

# Virenfänger auf der Hutschiene

Zusätzliche Sicherheit durch Virenschutz in der Automatisierungstechnik



Bild 1: Innominate mGuard industrial ist die erste Firewall für die Automatisierungstechnik mit integriertem Virenschutz.

Auch in der Automatisierungstechnik erhält Netzwerksicherheit durch die fortschreitende Verbreitung von Industrial Ethernet einen hohen Stellenwert. Dabei lassen sich herkömmliche Security-Lösungen aus der Bürowelt in den seltensten Fällen direkt auf die Automatisierungswelt übertragen. Nachdem sich die ersten Hersteller des Themas Zugriffsschutz (Firewall) und Verschlüsselung (VPN) für industrielle Anwendungen angenommen haben, ruft die rasante Verbreitung von Windows in der Automatisierung auch nach Lösungen gegen das Vordringen von Viren.

**D**urch das hohe Innovationstempo in der Informationstechnologie werden die offenen Standards Ethernet und TCP/IP zunehmend für alle Bereiche der industriellen Kommunikation bis zur Feldebene relevant. Die erheblich geringeren Kosten für Standardkomponenten tragen zum weiteren Siegeszug von Ethernet in der Automatisierung bei. Der heute schon für viele Automatisierungsgeräte weit verbreitete Bedienungszugang über Internet-Browser wurde beispielsweise erst

durch eine durchgängige Nutzung von TCP/IP möglich. Der Einsatz von Ethernet als „Industrial Ethernet“ mit seinen leider nicht hundertprozentig kompatiblen Spielarten wie Profinet, Ethernet Powerlink und Ethernet/IP wird sich in den nächsten Jahren auch für harte Echtzeitanwendungen empfehlen. Dabei ist abzusehen, dass die stärkere Standardisierung und Vernetzung in der Automatisierung auch zu einer höheren Anfälligkeit dieser Netze gegenüber Schadprogrammen führt.

## Was die Automatisierung von der IT lernen kann

Das Thema Netzwerksicherheit wird in der Büroumgebung schon lange groß geschrieben - zu oft haben Viren und Würmer bereits komplette Firmennetze zum Erliegen gebracht. Anders in der Automatisierungstechnik: Hier stellt sich das Problembewusstsein erst langsam ein - und das, obwohl der Ausfall einer Maschine oder Anlage enorme Kosten nach sich ziehen kann. Wenn ein Schadprogramm z.B.

einen Leitrechner durch massive Überflutung mit Verbindungsanfragen (so genannten Denial of Service-Attacken) angreift und die Bandbreite in Richtung der darunter liegenden Steuerrechner und Produktionsroboter deutlich reduziert, dann gehen diese in Störung, und die gesamte Produktionslinie ist lahm gelegt. In der vernetzten Bürowelt dagegen hat ein solcher Angriff auf die Verfügbarkeit zwar in der Regel auch ärgerliche, aber nicht immer derart fatale Auswirkungen.



Bild 2: Der patentierte Stealth-Mode des Innominate mGuard industrial macht die Firewall für Angreifer unsichtbar.

Eine abgeschaltete Produktionsstraße verursacht ungleich höhere Kosten als z.B. der vorübergehende Ausfall eines Mailservers. Hinter vorgehaltener Hand

erfährt man von vielen Fertigungsunternehmen, dass es bereits erheblich mehr Sicherheitsvorfälle im Fertigungsumfeld gegeben hat, als öffentlich

bekannt wird. Fälle von Produktionsunterbrechungen von mehr als einem Tag haben geholfen, das Sicherheitsbewusstsein zu schärfen. Insbesondere der Sasser-Wurm, der letztes Jahr grassierte, hat größeren Schaden bei einer Reihe von Industrieanwendungen angerichtet.

### Security-Lösungen für den industriellen Einsatz

Um den Anforderungen an die Netzwerksicherheit im Bereich der Automatisierungstechnik gerecht zu werden, kommen im zunehmenden Maße Firewall-Systeme zum Einsatz, die für den Einsatz im industriellen Umfeld konzipiert wurden. Stateful Inspection Firewalls, wie sie sich auch im Büroumfeld durchgesetzt haben, stellen dabei den Stand der Technik dar. Das heißt: Eingehende und ausgehende Datenpakete werden an Hand vordefinierter Regeln überwacht. Damit ist gewährleistet, dass nur autorisierte Verbindungen entgegengenommen werden. So entsteht ein Schutz vor schädlichem Netzwerkverkehr. Die Industriefirewall wird als eigenständiges System in das Netzwerk integriert und schützt ein Teilnetz, die Produktionszelle oder das einzelne Automatisierungsgerät. Durch den Einsatz von Bridging- oder Stealth-Technologien kann ein solches Gerät in das Produktionsnetz eingebracht werden, ohne dass die Netzwerktopologie geändert werden muss. Die Security Appliance wird einfach in den bestehenden Datenstrom der zu schützenden Maschine „eingeschleift“. Neben dem Schutz durch Firewallfunktionalität ist es sinnvoll, Virtual Private Networks (VPN) für den verschlüsselten, sicheren Datenverkehr etablieren zu können. Dabei steht aber nicht nur die Verschlüsselung von Daten beim Transfer über öffentliche Netze (wie z.B. Fernwartung über das Internet) im Vordergrund. Zunehmend werden VPNs auch genutzt, um Daten-

kommunikation im Inneren (also im Produktionsnetz) zu schützen. Die Eigenschaft, dass beide Kommunikationspartner sich gegenseitig ausweisen müssen (Strong Authentication), kann zur deutlichen Erhöhung der Sicherheit in Produktionsnetzen führen. Auch hierfür sind industrielle Firewall/VPN-Appliances verfügbar, die beide Funktionen verknüpfen. Beispiele für solche Security-Lösungen sind Scalance S von Siemens und Eagle von Hirschmann. Beide bieten Firewall- und VPN-Funktionalität für den Zugriffsschutz und die Verschlüsselung von Daten in Produktionsnetzen.

### Würmer und Viren in der Automatisierung

Würmer und Viren, die das eine oder andere Büronetz schon für Tage lahm gelegt haben, drohen in Zukunft auch verstärkt Automatisierungsnetze zu befallen. So wird hie und da hinter vorgehaltener Hand auch schon darüber berichtet, wie Viren oder Würmer, die sozusagen die „Artengrenze“ überschritten haben, Produktionsabläufe empfindlich gestört haben. Auch Servicetechniker mit Zugang zu durchgängig vernetzten Steuerungen und Maschinen stellen ein Risiko für die Netzwerksicherheit dar. Ein wichtiger Grund für die zunehmende Verbreitung von Viren: In demselben Maß wie Ethernet und TCP/IP in der Automatisierung Einzug halten, setzt sich auch Windows (Embedded) als maßgebliche Plattform für die Entwicklung von Steuerungen, Robotern etc. durch. Zunehmende Standardisierung, leichte Einarbeitung und eine mächtige Funktionsbasis sprechen für einen solchen Schritt. Allerdings verschärft sich damit auch die Problematik von Viren und Würmern in der Automatisierung. Obwohl Firewalls und VPNs grundlegende Sicherheitsfunktionen bereitstellen, können diese allein keinen umfassenden Schutz vor Viren bieten.

## Glossar

**TCP/IP:** Transfer Control Protocol / Internet Protocol = gebräuchlichstes Kommunikationsprotokoll in der Datenübertragung

**VPN:** Virtual Private Network = Methode zur Verschlüsselung und eindeutigen Identifizierung bei Datenübertragungen

**DoS:** Denial of Service = Attacken, bei denen IT-Systeme durch massive Überlastung über den gezielten Überlauf von Sitzungsinformationen angegriffen werden

**Stealth:** Methode, bei der Sicherheitsfunktionen unsichtbar für den potenziellen Angreifer und das zu schützende System ausgeführt werden

**http:** Hypertext Transfer Protocol = Das dem WWW zugrunde liegende Übertragungsprotokoll

**FTP:** File Transfer Protocol = Das gebräuchlichste Protokoll für den Dateitransfer im Internet

**Firewall:** Geräte oder Software zur Kontrolle erlaubter Datenverbindungen

**SMTP:** Simple Mail Transfer Protocol = Gebräuchlichstes Protokoll für den Versand von eMails

**Wurm:** Ein dem Computervirus ähnliches Schadprogramm, das im Gegensatz zum Virus aber nicht auf die Weiterverbreitung durch einen Anwender wartet, sondern sich selbst weiterverbreitet (Beispiele: Sasser, MyDoom)

**Appliance:** Kombination aus Hardware und Software, die eine einzige Aufgabe (hier: IT-Sicherheit) erfüllt

**Stateful Inspection:** de-facto Standard für Firewalls, bei dem Datenpakete der Hin- und Rückrichtung einem logischen Datenstrom zugeordnet werden

## Software oder Hardware?

Prinzipiell kann der Schutz vor Viren - ähnlich wie in der Bürowelt auch - über Software- oder Hardwarelösungen (so genannte Appliances) erfolgen. Bei Softwarelösungen handelt es sich um Antiviren-Programme, die auf - in der Regel Windows-basierten - Steuerungen, Robotern oder Industrie-PCs installiert werden. Wegen der großen Heterogenität und der Gefahr von Rückwirkungen auf das zu schützende System, werden Hardwarelösungen in Form so genannter All-in-one Security Appliances in der Automatisierung eine sehr wichtige Rolle spielen. Der höhere Preis für die Anschaffung wird in der Regel durch die geringeren Betriebskosten und die höhere Sicherheit aufgehoben. Ein Beispiel eines

Unternehmens der Prozessautomatisierung aus den USA zeigt die Problematik: Die auf einem Industrie-PC in der Leittechnik installierte Anti-Virus-Software hat durch ein Fehlverhalten die Notabschaltung eines wichtigen Kesselsystem verhindert. Der Schaden war entsprechend groß. Ein Hersteller von Antivirus-Software kam jüngst in die Schlagzeilen, weil ein fehlerhaftes Virenupdate dazu führte, dass Tausende von PCs, auf denen der Virenschutz installiert war, nicht mehr booten konnten. Ein vergleichbarer Vorfall im Produktionsumfeld wäre fatal.

## Erster Virenschutz für die Hutschiene

Die Berliner Innominate Security Technologies AG hat diese

Lücke erkannt und bietet mit ihrem Produkt mGuard industrial die weltweit erste Security Appliance für die Hutschiene mit Virenschutz. mGuard ist in der Lage, Viren in Protokollen wie HTTP, SMTP und FTP zu erkennen. Diese Funktion erweitert die Firewall- und VPN-Fähigkeiten des Innominate-Produktes durch einen leistungsfähigen und schnellen Virensch scanner, der auf der bewährten Technologie von Kaspersky Lab basiert. Virensignaturen können über das Internet oder einen speziellen Relay-Server im Produktionsnetz aktualisiert werden. Durch das Software Developer Kit lassen sich weitere Kommunikationsprotokolle hinzufügen, die ebenfalls nach Viren untersucht werden. Viele weitere Industriemerkmale (z.B. IP20-

Gehäuse, elektrischer Signalkontakt, 24V Spannungsversorgung) machen mGuard industrial zu einer universellen Security-Lösung für industrielle Anwendungen. ■



*Autor: Olaf Siemens ist Vorstand der Innominate Security Technologies AG, Berlin.*

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