

Durch den Einzug von Standardtechnologien wie Ethernet oder TCP/IP werden auch Automatisierungsnetze anfällig für Viren und Würmer.

Steuerungstechnik

Netzwerksicherheit in der Automatisierungstechnik

von **Andreas Beierer**
Produktion Nr. 39, 2005

BERLIN (jv). Seit langem sind die Gefahren bekannt, die von Viren und Würmern in Office-IT-Umgebungen ausgehen. Genauso lange werden diese Gefahren mittels vielseitiger organisatorischer und technischer Maßnahmen bekämpft. Anders stellt sich die Situation in der Automatisierungsbranche dar.

Nachdem die Nutzung vorwiegend proprietärer Kommunikationsprotokolle hier in der Vergangenheit für weitgehende Isolation und somit auch zu relativer Sicherheit führte, stellt der Vormarsch von Standardtechnologien wie Industrial Ethernet und TCP/IP die Verantwortlichen in der Automatisierung vor neue Herausforderungen. Denn plötzlich ist die ‚Security by Obscurity‘ gefährdet, Viren und Würmer können über Ethernet und TCP/IP auch in diesem Bereich Einzug halten. „Die Sicherheitsrisiken beim Einsatz von Industrial Ethernet werden von vielen Unternehmen noch nicht wirklich ernst genommen. Dabei verursacht ein Systemausfall in der Fertigung ganz erhebliche Kosten“, weiß Olaf Siemens, CEO der Innominate Security Technologies AG.

Der Ausfall einer Maschine oder Anlage kann sehr viel größere Schäden nach sich ziehen, als es im Büroumfeld möglich ist. So können Steuerrechner oder Roboter durch massive Überflutung mit Anfragen lahmgelegt und dadurch ganze Produktionslinien gestört werden. Die Tatsache, dass Microsofts Betriebssystem Windows auch in der Automatisierung immer verbreiteter wird, erhöht die Notwendigkeit für grundlegende Lösungen zur Sicherstellung der Funktionsfähigkeit von Industrial-Ethernet-Netzwerken. Auch Servicetechniker mit Zugang zu durchgängig vernetzten Steuerungen und Maschinen stellen ein Risiko für die Sicherheit dar.

Damit heißt das Gebot der Stunde: Bei der Planung und Implementierung neuer Netzwerkinfrastrukturen muss das Thema Sicherheit von Anfang an berücksichtigt werden. Allerdings stammen viele der derzeit verfügbaren Lösungen aus der Bürokommunikation und taugen in der Regel nur bedingt für die Automatisierung. Fernwartungszugänge beispielsweise bedürfen einer durchgängigen Kommunikation. Für die Absicherung dieser übergreifenden Infrastruktur ist es nicht damit getan, eine zentrale Firewall zum Schutz des Übergangs zwi-

schen Büro- und Automatisierungsnetz zu betreiben. Die Sicherheit muss bis zum Endgerät gewährleistet werden.

Um den vielfältigen Anforderungen an die Netzwerksicherheit gerecht zu werden, kommen deshalb im zunehmenden Maße Firewall-Systeme zum Einsatz, die speziell für den Einsatz im industriellen Umfeld konzipiert wurden. Die Firewall ‚m-Guard industrial‘ von Innominate beispielsweise lässt sich mit Hilfe der ihr eigenen Stealth-Technologie in das Produktionsnetz einbringen, ohne dass die Netzwerkkonfiguration geändert werden muss. Die Firewall schützt ein Teilnetz, die Produktionszelle oder das einzelne Automatisierungsgerät und wird einfach in den bestehenden Datenstrom der Maschine ‚eingeschleift‘. Das erleichtert die Konfiguration und den Einsatz verteilter Sicherheitssysteme auch in großen Netzwerken.

m-Guard, Eagle und Scalance S sorgen für Sicherheit im Netz

Neben dem Schutz durch die Firewallfunktionalität bietet m-Guard auch die Möglichkeit, Virtual Private Networks (VPN) für den verschlüsselten, sicheren Datenverkehr zu etablieren. Dabei steht nicht nur die Verschlüsselung von Daten beim Transfer über öffentliche Netze wie beispielsweise bei der Fernwartung über das Internet im Vordergrund. Zunehmend werden VPNs auch genutzt, um Datenkommunikation im Inneren – also im Produktionsnetz – zu schützen. Zusätzlich zur Firewall- und VPN-Funktionalität ist der Viren-

schutz bei m-Guard bereits integriert. Viren und Würmer haben so keine Chance mehr.

Auch bei der Hirschmann Automation and Control GmbH hat man früh erkannt, dass bezüglich der Sicherheit von Industrienetzwerken Handlungsbedarf besteht. „Unser Ziel ist eine Strukturierung der Produktionsnetze in so genannte Security Compartments. Um diese geschützten Netzbereiche in vorhandene Anlagen ohne tiefgreifende Änderungen implementieren zu können, haben wir 2004 in Kooperation mit Innominate mit dem ‚Eagle‘ den ersten industrietauglichen Security-Router auf den Markt gebracht“, erklärt Ralf Kaptur, Produktmanager Industrial Networking. Zudem werden von der neuen Generation der Hirschmann-Switches standardisierte Sicherheitsfunktionen wie IEEE-802.1X-Authentifizierung und verschlüsselte Managementzugänge wie SNMPv3 (Simple Network Management Protocol Version 3) und SSH (Secure Shell) unterstützt. „Last but not least setzen wir auf eine möglichst einheitliche Security Policy für die Office- und Factory-Welt sowie einen nahtlosen Workflow zwischen diesen beiden Administrationbereichen“, so Kaptur.

Siemens setzt auf einfache Handhabung

Eine weitere Hardware-basierte Lösung wird vom Nürnberger Siemens-Bereich Automation and Drives angeboten. „Auch die Scalance-S-Module lassen sich rückwirkungsfrei auf die Adressierung des restlichen Netzes einfach an strategisch günstigen Stellen einfügen, schützen das abgekoppelte Teilnetz durch eine Firewall und bauen untereinander VPN-Tunnel zum Schutz der Kommunikation auf“, sagt Dietmar Herian, Leiter industrielle Kommunikation bei Siemens A&D. Dabei wird auch die im Automatisierungsumfeld häufig verwendete Layer-2-Kommunikation mit erfasst und übertragen. Großes Augenmerk legte Siemens dabei auf die einfache Handhabbarkeit der Module. Über ein komfortables Projektierungstool können die erlaubten Kommunikationsbeziehungen in Gruppen zusammengefasst und per Knopfdruck an die Module übertragen werden, ohne dass spezielles Wissen über die Security-Mechanismen benötigt wird. Neben dieser Minimalconfiguration gibt es auch erweiterte Einstellmöglichkeiten, die bei Bedarf genutzt werden können, z. B. die Firewall-Projektierung oder die Einbindung anderer VPN-Teilnehmer. Die kombinierten VPN- und Firewall-Funktionen bieten neben einer erhöhten Sicherheit auch die Möglichkeit, differenziertere Zugangsbeschränkungen zu realisieren.



Bild: Innominate Security Technologies AG

Die Firewall m-Guard industrial von Innominate bietet einen umfassenden Virenschutz für Produktionsnetze.