

Ethernet-Kommunikation und Zugriff unter Kontrolle

Torsten Rössel



Torsten Rössel
Director Business
Development
Innominate Security
Technologies AG
12489 Berlin
Kontakt:
www.innominate.de

»Der Schutz kritischer vernetzter Automatisierungssysteme ist weniger ein technisches Problem, sondern primär ein Zielkonflikt zwischen den Kosten der Security-Maßnahmen sowie den Risiken, wenn diese nicht ergriffen werden. Wirtschaftliche, effizient managbare Lösungen wie die mGuard-Technologie tragen dazu bei, diesen Konflikt zugunsten einer höheren Sicherheit zu lösen.«

Security – Sicherheit in der Automatisierung

Industrielle Systeme werden zunehmend auf Basis von Ethernet und TCP/IP-Protokollen vernetzt. Neben der internen Kommunikation der Maschinen und Anlagen sowie Überwachungs- und Leitfunktionen spielt dabei der Datenaustausch mit Drittsystemen eine wachsende Rolle. Deshalb ist es umso wichtiger, die Netzwerke mit adäquaten Sicherheitsmaßnahmen vor Überlastung durch technische Defekte und Broadcast-Stürme, unbeabsichtigte Fehlbedienungen sowie gezielte Angriffe von innerhalb und außerhalb des Unternehmens zu schützen. Perimeter-Schutz an den Grenzübergängen eines Netzes bietet allein keine ausreichende Sicherheit, da er weder vor internen Angriffen schützt noch die weitere Ausbreitung von eingedrungenen Schädigungen eindämmen kann. Als geeignete Maßnahme wird hier eine Defense-in-Depth-Strategie empfohlen, mit der sich auch kritische Zellen oder Einzelsysteme absichern lassen. Eine Schlüsselrolle kommt dabei der Kontrolle und Filterung des Netzwerkverkehrs durch Firewalls zu. Die Sicherung heterogener industrieller Systeme nur durch Software scheidet aber in der Regel aus, da die regelmäßig notwendigen Updates auf den Systemen nicht praktikabel sind. Darüber hinaus reichen die Hardware-Ressourcen und die Prozessorleistung meist nicht aus, um ohne Beeinträchtigung der Nutzfunktion zusätzliche Sicherheitsaufgaben zu übernehmen.



Der Innominate Device Manager (IDM) übernimmt das zentrale Geräte-Management der »mGuard«-Produktfamilie.
Foto und Grafik: Innominate.

Eine zentralisierte Absicherung vieler Zellen oder Einzelsysteme durch eine entsprechend groß dimensionierte Sicherheitskomponente würde eine sternförmige Verkabelung voraussetzen, die deutlich teurer als eine mit kleineren Switches realisierte Baum- oder Linientopologie mit kurzen Kabelstrecken ist. Deshalb setzt die Innominate Security Technologies AG auf eine dezentrale Architektur mit verteiltem Schutz durch kleine Security-Appliances sowie völliger Freiheit im Netzwerk-Design, die in fast allen industrietypischen Szenarien mit geringeren Investitions- und Betriebskosten umsetzbar ist. Die »mGuard«-Produktfamilie stellt entsprechende Komponenten in unterschiedlichen Formfaktoren zur Verfügung: als Hutschienengerät, im PCI-Kartenformat oder als 19-Zoll-Rack-System mit Blade-Einschüben. Von Vorteil insbesondere für die Nachrüstung ist, dass die Geräte nicht nur als Router betrieben, sondern auch transparent in ein Netz oder vor ein System eingeschleift werden können (»Stealth Mode«). Mit 1:1 NAT (Network Address Translation) unterstützen die »mGuard«-Komponenten die flexible Einbindung von Anlagen in Betreiber-netze ohne Anpassungen am internen Adressraum der Maschinen. Ihre optionale VPN-Funktion (Virtual Private Networking) erlaubt den Aufbau sicherer Teleservice-Verbindungen für die Ferndiagnose und -wartung via Internet.

Zentrales Geräte-Management

Die dezentrale Architektur führt bei konsequenter Anwendung in größeren Applikationen zu einer drei- oder vierstelligen Zahl von Security-Geräten, deren individuelle manuelle Administration und Konfiguration nicht praktikabel ist. Ihre Vorteile lassen sich nur dann aus-

spielen, wenn es ein zentrales Geräte-Management gibt, über das selbst tausende verteilter Geräte von einer Stelle aus umfassend beherrschbar sind. Mit dem Innominate Device Manager (IDM) können mehrere Benutzer an Vorlagen und Gerätedaten arbeiten. Fertige Konfigurationen oder Updates werden aktiv vom IDM auf die Geräte gespielt (Push-Verfahren) oder auf einem Web-Server zum automatischen Download bereitgestellt (Pull-Verfahren). Beide Verfahren nutzen sichere Protokolle (SSH beziehungsweise HTTPS) und spielen Status-Informationen zurück, die eine zentrale Überwachung aller verwalteten Komponenten ermöglichen. Dabei lässt sich durch eine Vorlagen- und Vererbungstechnik ein hoher Automatisierungsgrad für die Konfiguration einzelner Geräte erzielen. In der Praxis finden sich oft größere Gruppen von zu schützenden Systemen mit ähnlichem oder identischem Kommunikationsverhalten. Für Einzelgeräte müssen dann nur noch wenige individuelle Einstellungen vorgenommen werden. Ein Security-Administrator gestaltet die Vorlagen, während die Techniker die Komponenten nach kurzer Einweisung mit Hilfe passender Vorlagen in Betrieb nehmen können.

»mGuard«-Geräte unterstützen auch bei der Erstellung eines wirksamen Firewall-Regelwerks. Im »Learning Mode« werden zunächst alle Verbindungsversuche zugelassen und durch einen Syslog-Server protokolliert. Bei intensiver Kommunikation können hier derart große Datenmengen anfallen, dass sie manuell nicht mehr auswertbar sind. Mit einer Software lassen sich diese aber auf einige Regeln konzentrieren, die der Anwender manuell plausibilisieren kann. Dieser Vorgang wird iterativ wiederholt, bis keine unbekannteren Verbindungen mehr auftreten.