

## Industrial Firewalls:

# Kommunikation und Zugriff über Ethernet unter Kontrolle

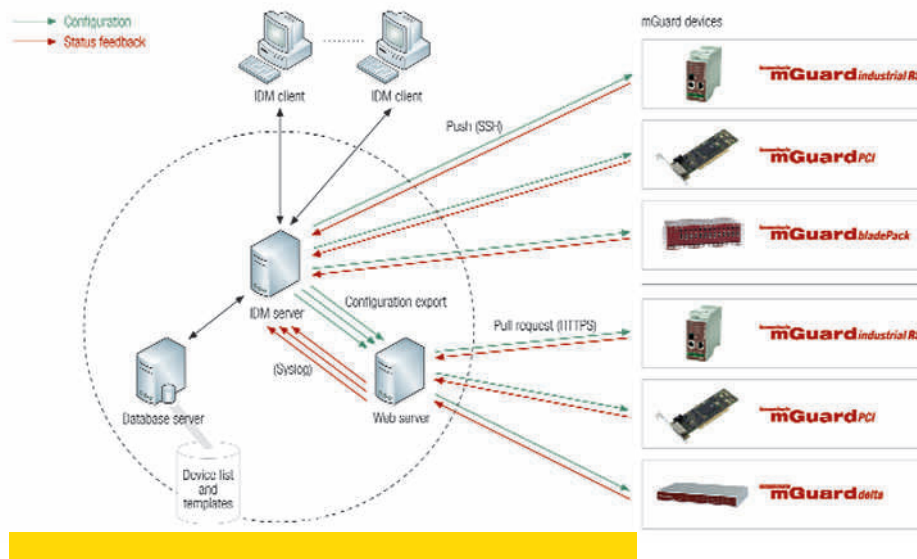


Bild 1: Mit dem Innominate Device Manager (IDM) für die mGuard Geräte-Familie ist ein zentrales Geräte-Management verfügbar mit dem selbst tausende verteilter Geräte von einer Stelle aus umfassend beherrscht werden können.

Industrielle Systeme werden zunehmend auf Basis von Ethernet und TCP/IP-Protokollen vernetzt. Neben der internen Kommunikation von Maschinen und Anlagen sowie Überwachungs- und Leitfunktionen spielt dabei der Datenaustausch mit Drittsystemen eine wachsende Rolle. Beispiele sind automatisierte Datensicherung, Langzeitarchivierung von Qualitätsdaten, Zugriff aus CAD/CAM-Programmierung und SPS-Projektierung über Netz auf die Zielkomponenten sowie Anbindungen an MES- und ERP-Systeme.

Leider sind industrielle Systeme infolge der zunehmenden Vernetzung auf Basis von Ethernet und TCP/IP-Protokollen auch vielfältig gefährdet. Das Spektrum reicht von Überlastung durch technische Defekte und Broadcast-Stürme über unbeabsichtigte Fehlbedienung und argloses Einschleppen von Schadsoftware bis zu gezielten Angriffen von innen und außen zum Zwecke der Sabotage, Spionage und anderen kriminellen Motiven. Erhebliche Risiken wie Produktionsausfall, Gesundheits- und Umweltschäden, Verlust von Intellectual Property, Compliance

und Image sind die Folge. Die Netzwerk-Einbindung von Maschinen und Anlagen sollte daher nicht ohne adäquate Sicherungsmaßnahmen erfolgen.

### Industrielle Steuerungen sind unsicherer, als Sie denken!

Entgegen ihrer vermeintlichen Robustheit sind auch Speicherprogrammierbare Steuerungen mit Ethernet-Schnittstellen durchaus anfällig für netzbasierte Störungen. So wurden in 2005 am Europäischen Forschungszentrum CERN 25 marktgängige SPSen von sieben Herstellern einem Si-

cherheitstest mit generischen Angriffstechniken unterzogen. Genutzt wurden die frei zugänglichen Werkzeuge Nessus, ein Penetrations- und Verwundbarkeits-Scanner und Netwox für die Simulation von Denial-of-Service Attacks. Selbst ohne jede sonstige Belastung führten 39% der Tests zu einer Fehlfunktion, in bis zu 32% der Fälle sogar zu Systemabstürzen. Bei einer Wiederholung mit neueren Firmware-Ständen fielen die Ergebnisse Ende 2006 zwar etwas besser aus, nach wie vor führten aber 34% der Tests zu einer Fehlfunktion und bis zu 26% der Fälle weiterhin

zum Absturz der Steuerungen. Ferner zeigten Stichproben, dass Störungen unter produktions-typischer Last noch sehr viel wahrscheinlicher sind. Mit ähnlichem 'Aha-Erlebnis' wurde von Langner Communications im Rahmen einer kürzlich gemeinsam mit Innominate veranstalteten Industrial Security Roadshow eindrucksvoll vorgeführt, wie SPSen ohne geheimes Insiderwissen oder spezifische Projektkennnisse unbefugt manipuliert werden können. Bis hin zum völligen Stopp und Löschen des Programmspeichers führen die Steuerungen einfach aus, was über-durchaus protokollkonforme an

## Defense-in-Depth-Strategie und Endpunkt-Sicherheit

Perimeter-Schutz an den Grenzübergängen eines Netzes allein kann keine ausreichende Sicherheit bieten, da er weder vor internen Angriffen schützt noch die weitere Ausbreitung von eingedrungenen Schädigungen eindämmen kann. Als Best Practice wird daher eine sogenannte Defense-in-Depth-Strategie empfohlen, die gestaffelt bis zum Schutz kritischer Zellen oder Einzelsysteme reicht, vergleichbar der mit Security Software auf PCs angestrebten Endpunkt-Sicherheit in Büronetzen. Eine Schlüsselrolle kommt dabei der Kontrolle und Filterung von Netzwerkverkehr durch Firewalls zu. Maxime: „Was nicht explizit erlaubt ist, ist verboten!“ Eine Sicherung heterogener industrieller Systeme rein durch Software sofern denn überhaupt verfügbar scheidet aber in der Regel aus. Zum einen sind die bei Security Software regelmäßig notwendigen Updates auf den Systemen selbst nicht praktikabel (Grundsatz: „Never touch a running system!“). Zum anderen reichen auch Hardware-Ressourcen und Prozessorleistung meist nicht aus, um ohne Beeinträchtigung der Nutzfunktion zusätzliche Sicherheitsaufgaben zu übernehmen. So war z.B. die Freude bei

manchem Anwender Windows XP-basierter Steuerungen über die mit Service Pack 2 verfügbare Software-Firewall von kurzer Dauer: Schon ein trivialer Denial-of-Service-Angriff ließ die Systeme einfrieren oder besser gesagt durchglühen, da sich ihre CPU zu 99% nur noch mit Firewall-Funktionen beschäftigte.

## Verteilter Schutz mit zentralem Geräte-Management

Innominate hat sich auf die Anforderungen der industriellen Netzwerksicherheit spezialisiert und mit der mGuard-Technologie innovative Lösungen geschaffen, die hier einspringen: fertig konfektionierte Security Appliances mit eigenen Ressourcen und integrierter Firmware. Eine zentralisierte Absicherung vieler Zellen oder Einzelsysteme durch eine entsprechend groß dimensionierte Sicherheitskomponente würde eine sternförmige Verkabelung voraussetzen, die im industriellen Umfeld untypisch und deutlich teurer ist als eine mit kleineren Switches realisierte baum- und linienförmige Topologie mit kurzen Kabelstrecken. Deshalb setzt Innominate auf eine dezentrale Architektur mit verteiltem Schutz durch kleine Security Appliances und völliger Freiheit im Netzwerk-Design. Diese ist nachweislich in fast

allen industrietypischen Szenarien mit geringeren Investitions- und Betriebskosten realisierbar. Je nach Typ des zu schützenden Systems können Appliances in unterschiedlichen Formfaktoren prädestiniert sein. Für die Absicherung von Automatisierungstechnik im Schaltschrank wird man ein Hut-schienengerät bevorzugen. Für PC-basierte Bedien-Panels oder Steuerungen eignen sich Appliances im PCI-Kartenformat sehr gut. Auch ein 19"-Rack-System mit Blade-Einschüben ist als platzsparende Lösung für den Netzverteilteraum verfügbar. Von Vorteil insbesondere für die Nachrüstung ist, dass die Geräte nicht nur als Router betrieben, sondern auch transparent in ein Netz bzw. vor ein System eingeschleift werden können (sogenannte 'Stealth Mode'). Mit 1:1 NAT (Network Address Translation) unterstützen mGuard-Appliances die flexible Einbindung von Anlagen in Betreiber-netze ohne Anpassungen am internen Adressraum der Maschinen. Und mit ihrer optionalen VPN-Funktion (Virtual Private Networking) bilden sie 'ganz nebenbei' die Grundlage hochsicherer Teleservice-Verbindungen für Ferndiagnose und Fernwartung via Internet. Die dezentrale Architektur führt bei konsequenter Anwendung zu einer drei- oder gar vierstelligen Zahl von Appliances



Bild 2: Für die Absicherung von Automatisierungstechnik im Schaltschrank werden Hut-schienengeräte wie der mGuard industrial RS bevorzugt.

ihren Projektierungsort gesendete Datenpakete verlangt wird ohne jede Überprüfung des Absenders und seiner Autorisierung. Parallel zur Vernetzung nimmt die Verwendung von Standard-IT-Komponenten im industriellen Umfeld zu: PC-basierte Steuerungen und Bediensysteme, Microsoft Windows Betriebssysteme und Applikations-Protokolle für File Sharing, Datenbanken und Web-Oberflächen sind typische Beispiele. Die Systeme werden dadurch offener für gewünschte Integration, leider aber auch für unerwünschte Schädigung. Verwundbarkeiten der Büronetze breiten sich in die Welt der Produktion aus. Über 1.000 neue Schwachstellen und zugehörige Exploits pro Jahr werden von den internationalen Computer Emergency Response Teams (CERTs) gemeldet. Was also tun?



Bild 3: Auch ein 19"-Rack-System mit Blade-Einschüben ist als platzsparende Lösung für den Netzverteilteraum verfügbar.

# Sichere Automation



Bild 4: Für PC-basierte Bedien-Panels oder Steuerungen eignen sich Appliances im PCI-Kartenformat.

im Feld eines größeren Betreibers. Diese einzeln manuell zu administrieren und auf Dauer in Firmware und Konfiguration aktuell zu halten, ist nicht praktikabel. Ihre Vorteile lassen sich also nur ausspielen, wenn ein zentrales Geräte-Management verfügbar ist, mit dem selbst tausende verteilter Geräte von einer Stelle aus umfassend beherrscht werden können. Genau dies leistet der Innominate Device Manager (IDM) für die mGuard-Geräte-Familie. Mehrere Benutzer können an Vorlagen und Gerätedaten arbeiten. Fertige Konfigurationen ebenso wie spätere Updates können aktiv vom IDM auf die Geräte gespielt (Push-Verfahren) oder auf einem Web Server zum automatischen Download für die Geräte bereitgestellt werden (Pull-Verfahren). Bei beiden Verfahren werden sichere Protokolle (SSH bzw. HTTPS) genutzt und Status-Informationen zurückgespielt, die eine zentrale Überwachung aller verwalteten Geräte ermöglichen. Dabei lässt sich ein hoher Automatisierungsgrad für die Konfiguration einzelner Geräte erzielen, etwa durch eine Vorlagen- und Vererbungs-

technik. In der Praxis finden sich oft größere Gruppen von zu schützenden Systemen mit ähnlichem oder gar identischem Kommunikationsverhalten. Der gemeinsame Kern einer Security-Konfiguration für diese Systeme kann in einer Vorlage gekapselt und von dieser auf hunderte von Appliances vererbt werden. Für Einzelgeräte müssen dann – wenn überhaupt – nur noch wenige individuelle Einstellungen vorgenommen werden. Diese Elemente ermöglichen auch eine praxisnahe Arbeitsteilung. Ein Security-Administrator mit tieferer Expertise gestaltet die Vorlagen, während Techniker nach kurzer Einweisung Geräte mithilfe passender Vorlagen ausrollen und in Betrieb nehmen können.

## Firewall-Regeln kann man lernen

Doch wie kommt man überhaupt zu einem wirksamen Firewall-Regelwerk, besonders bei Nachrüstung in Bestandsanlagen ohne ausreichende Dokumentation? Hier können mGuard Appliances helfen, ein geeignetes Regelwerk

buchstäblich zu erlernen. Im 'Learning Mode' werden zunächst alle Verbindungsversuche zugelassen und durch einen Syslog-Server protokolliert. Bei intensiver Kommunikation fallen hier zwar schnell größere Datenmengen an als ein Mensch noch auswerten könnte. Mithilfe einer Software lassen sich diese aber auf eine Essenz von Regeln konzentrieren, die manuell plausibilisiert werden können. Dieser Vorgang wird iterativ wiederholt, bis keine unbekannteren Verbindungen mehr auftreten. Dann ist der Lernprozess abgeschlossen und das Regelwerk kann 'scharf' geschaltet werden. Unzulässige Verbindungsversuche werden fortan blockiert. Das gelernte Regelwerk kann auch in eine Vorlage des Geräte-Managements importiert und von dort auf andere Appliances mit gleichartigen Schützlingen verteilt werden.

## Fazit

Der Schutz kritischer, vernetzter Automatisierungssysteme ist weniger ein technisches Problem, sondern primär ein Zielkonflikt zwischen Kosten (der Sicherheit) und

Risiken (der Unsicherheit). Wirtschaftliche, effizient managebare Lösungen wie die Innominate mGuard-Technologie tragen bei, diesen Konflikt zugunsten von mehr Sicherheit zu mildern. ■



Autor: Torsten Rössel ist Director Business Development bei der Innominate Security Technologies AG in Berlin.