

Hardware-Firewall sorgt für Sicherheit im Industrial-Ethernet

Virenschutz für die Automatisierungstechnik

Seit Industrial Ethernet Einzug in die Produktion hält, ist die Welt der Fertigungsautomatisierung keine sichere Oase mehr. Doch für viele Unternehmen gilt es, überhaupt erst ein Problembewusstsein für die Netzwerksicherheit zu entwickeln. Hierfür bietet Innominate passende Sicherheitslösungen, die sich jetzt auch für Produktionsnetze eignen.

Immer mehr Ethernet-basierte Kommunikationssysteme erreichen in der Automatisierungstechnik die Feldebene. Proprietäre Datenprotokolle und Netzwerktechnologien werden in der Produktionssteuerung nach und nach von den im Office-Bereich seit langem verbreiteten Standards Ethernet und TCP/IP abgelöst. Office- und Produktionsnetze wachsen auf der Basis dieser gemeinsamen Infrastruktur zusammen. Das eröffnet Industrieunternehmen große Effizienzpotenziale, weil sich die Produktionssteuerung unmittelbar mit ERP-Systemen (Enterprise Resource Planning) und dem Supply Chain Management verbinden lassen. Außerdem ist nur eine technische Infrastruktur aufzubauen und zu warten.

Andererseits öffnet die reichsübergreifende Infrastruktur auch Tür und Tor für Viren, Trojaner und Hackerangriffe, die in den bis dato relativ sicheren - weil isolierten - Industrienetzen nahezu unbekannt waren. Sicherheitsprobleme, denen die Bürowelt schon lange ausgesetzt ist: Würmer und Viren haben schon so manches komplette Büronetz lahm gelegt. Nun drohen sie auch in Zukunft verstärkt, Automatisierungsnetze zu befallen. Doch hier stellt sich das Problembewusstsein erst langsam ein: »Es hat auch uns überrascht, wie blauäugig die Anwender oft noch mit den neuen Sicherheitsrisiken beim Einsatz von Industrial Ethernet umgehen«, sagt Sicherheitspezialist Olaf Siemens, CEO von Innominate Security Technologies. Und das, obwohl der Ausfall einer Maschine oder Anlage in der Fertigung enorme Kosten verursachen kann. Eine abgeschaltete Produktionsstraße verursacht au-

ßerdem wesentlich höhere Kosten als beispielsweise der vorübergehende Ausfall eines Mailservers.

Auch die Tatsache, dass Windows sich in der Automatisierung immer weiter verbreitet, erhöht die Notwendigkeit für grundlegende Lösungen zur Sicherstellung der Funktionsfähigkeit Ethernet- und TCP/IP-basierender Netzwerke. Außerdem sollte durch das Verschmelzen der Office- und Produktionsnetze eine Sicherheitslösung die Anforderungen aus beiden Netzwerkwelten erfüllen.

Das Berliner Unternehmen Innominate, das sich speziell auf Security spezialisiert hat, hat diese Lücke erkannt und entwickelt Produkte, um diese Sicherheitsproblematik zu lösen. Die einzelnen Mitglieder der Produktfamilie »Innominate mGuard« sind für den entsprechenden Einsatz in



Der patentierte Stealth-Mode des »mGuard industrial« von Innominate macht die Firewall für Angreifer unsichtbar.



Olaf Siemens, Innominate

» Die Sicherheitsrisiken beim Einsatz von Industrial Ethernet nehmen viele Unternehmen noch nicht wirklich ernst genug. «

Büro- oder Produktionsumgebungen zugeschnitten. Wichtiger Schwerpunkt: »Wir wollen Sicherheitslösungen für die industrielle Produktion anbieten, die durch fortschreitende Standardisierung und Vernetzung gekennzeichnet ist«, erklärt Siemens.

Unsichtbarer Virenschutz für die Hutschiene

So hat Innominate seine Produktpalette für »device attached security« um eine Lösung für IT-Systeme in der industriellen Fertigung ergänzt. Der »mGuard industrial« ist eine Hardware-Firewall, die sich auf DIN-Hutschienen montieren lässt. Er schützt Einzelsysteme oder funktionelle Gruppen im industriellen Ethernet vor Angriffen von Außen und vor unberechtigten Zugriffen von Innen. Als erstes Gerät für Produktionsnetze bietet der »mGuard industrial« optional einen umfassenden Virenschutz. »Unsere konfigurierbare Firewall mGuard industrial schützt Automatisierungsnetze und Industriemaschinen individuell und unabhängig vom Betriebssystem gegen unbefugte Zugriffe und Schädlinge aller Art«, beschreibt Siemens.

Das Sicherheitsgerät wird einfach zwischen Ethernet-Schnittstelle und Fertigungsmaschine geschaltet und übernimmt deren MAC- und IP-Adresse. Mittels des patentierten »Stealth Mode« wird er für Eindringlinge von Außen unsichtbar, erhält so eine Art Tarnkappe. Die mGuards erkennen die jeweilige IP- und MAC-Adresse »ihres« geschützten Rechners und übernehmen diese für sich selbst. Somit lässt sich die Firewall unter der Adresse ihres Rechners im Netzwerk erreichen und konfigurieren. Für Hacker jedoch werden mGuards dadurch unauffindbar. »Das System kann nicht umgangen werden, weil es direkt an der Ethernet-Schnittstelle der Maschine angeschlossen ist«, hebt Siemens hervor. Der Stealth Mode ermöglicht außerdem die Integration eines mGuard, ohne dass die Konfiguration des Gesamtnetzwerks geändert werden muss.

Durch die Absicherung jeder einzelnen Maschine mit einer eigenen Firewall - Innominate nennt dieses Prinzip »device attached security« - bleibt ein Produktionsnetzwerk selbst im Falle einer Fehlbedienung oder Vireninjektion einer Maschine betriebsbereit. Neben dem Schutz vor Hackern erlaubt der mGuard industrial auch verschlüsselte Verbindungen zwischen einzelnen Systemen. Diese »Virtual Private Networks« (VPN) machen eine punktgenaue Zugriffskontrolle möglich. Gezielt eingerichtete VPNs in Verbindung mit individuell abgestimmten Sicherheitspolicies verhindern versehentliche Falscheingaben durch eigene Mitarbeiter. Externen Wartungstechnikern können zudem Zugriffsrechte für einzelne Maschinen gewährt werden. Alle anderen Systeme bleiben für sie unzugänglich.

Ebenfalls einzigartig für die industrielle Automation ist der »Security Configuration Manager« (ISCM) von Innominate, mit dem sich die Sicherheitseinstellungen zentral per drag and drop für alle

mGuard-Systeme auf der grafischen Benutzeroberfläche festlegen und anschließend auf die einzelnen »mGuard Firewalls« laden lassen. Außerdem sind VPN-Verbindungen zwischen einzelnen mGuards oder anderen Gateways ebenfalls leicht zu konfigurieren.

Weil der mGuard industrial keine Lüfter oder andere bewegliche Teile hat, bleibt er bis zu fünfzehn Jahre einsatzfähig. Das Gerät ist in zwei Ausführungen verfügbar: »mGuard industrial enterprise FW« (Firewall) ist über die weltweiten

Partner von Innominate zu einem Listenpreis von 690 Euro erhältlich, »mGuard industrial enterprise XL« (Firewall plus VPN) für 940 Euro.

Der Sicherheitsspezialist, der innerhalb von zwölf Monaten vier neue Produkte entwickelt hat, arbeitet derzeit neben Wireless-Security unter anderem auch an der Unterstützung des Realtime-Standards Ethernet-Powerlink. Der Vorteil: Wegen der hier eingesetzten Standard-Prozessoren und -ASICs lässt sich dieselbe Hardware nutzen. (in) ■

Explosionsschutz Signalgeräte von Werma

Signale für die Sicherheit

In den vergangenen Jahren haben sich die Bestimmungen zum Explosionsschutz und die Anforderungen an explosionsschutzgeschützte Signalgeräte stark verändert. Deshalb hat Werma Signaltechnik neue Ex-Signalgeräte entwickelt. Das Programm reicht von Ex-Signalsäulen über optische bis hin zu akustischen Ex-Signalgeräten,

treidemühlen, Gesundheitswesen, Lebensmitteltechnik, chemische und petrochemische Industrie.

Drei leuchtstarke Ex-Signalleuchten 738, 783 und 784 ergänzen jetzt das bestehende Sortiment von Werma:

Die kompakte Ex-Doppelblitzleuchte 738 hat eine hohe Blitzleistung von 15 Ws, die sich durch die Zündung von zwei Blitzen kurz hintereinander erreichen lässt. Ein verschleißarmer Reibradantrieb sorgt bei der Ex-Drehspiegelleuchte 783 für eine hohe Lebensdauer. Die Ex-Rundumleuchte 784 erreicht eine optimierte Fernwirkung aufgrund der Lichtbündelung durch 3 Fresnel-Linsen.

Alle neuen Ex-Leuchten haben einen Durchmesser von 195 mm und eine Höhe von 305 mm. Darüber hinaus verfügen sie über eine druckfeste Kapselung mit Anschlussraum. Das Gehäuse in Schutzart IP 66 ermöglicht es, dass sich die Leuchten sowohl innen als auch außen einsetzen lassen. Um mutwilligem Vandalismus oder auch der versehentlichen Zerstörung der Leuchten vorzubeugen, kann ein robuster Drahtschutzkorb aus rostfreiem Stahl angebracht werden. (in)



Werma warnt, schützt und leitet in explosionsgefährdeten Bereichen mit optischen und akustischen Signalen.

die sich sowohl in gas- als auch in staubexplosionsgefährdeten Bereichen (Zone 1 und 2, Zone 21 und 22) einsetzen lassen. Dazu zählen beispielsweise Raffinerien, Abfüllanlagen, Sägewerke, Möbelfabriken, Bergwerke, Ge-