

Modulare Konzepte als wirtschaftliche Alternative

Design for Security

Ob in den einschlägigen Fachmedien, bei Messen und Kongressen oder in der Arbeit der mit industrieller Automation und Kommunikation befassten Normungsgremien: Das Thema der industriellen Netzwerksicherheit erfährt parallel zur Verbreitung von Industrial Ethernet-Installationen seit einigen Jahren wachsende Aufmerksamkeit.



Die verständlichen Forderungen nach definierten Standards für mehr Sicherheit vor IT- und netzwerkbasiereten Schäden münden dabei nicht selten in der (Wunsch-)Vorstellung, Hersteller sollten ihre Automatisierungs- und Infrastrukturkomponenten so inhärent sicher gestalten, dass sie sich quasi von selbst zu sicheren Systemen zusammenfügen. Das wird sich in absehbarer Zeit jedoch weder technisch noch wirtschaftlich realisieren lassen. 'Design for Security' ist eine systemische Aufgabe und nur mit modularen Konzepten sinnvoll zu lösen. Dabei geht es um mehr als reine Informations- oder IT-Sicherheit. Bedroht sind nicht nur Daten, sondern die Kontrolle physischer Prozesse sowie die Qualität und Verwertbarkeit der

hergestellten Produkte. Ferner wird Netzwerksicherheit (Security) zunehmend auch zur Voraussetzung für die funktionale Sicherheit (Safety) vernetzter Systeme.

Ursachen für Sicherheitslücken

Die Ursachen der Verwundbarkeit sind vielfältig und von Anwenderseite kaum aus der Welt zu schaffen. So finden sich Schwachstellen häufig verwendeter Basiskomponenten – wie Betriebssysteme oder Embedded Web Server – in zahlreichen Produkten. Unter dem Kostendruck begrenzte Prozessor- und Speicher-Ressourcen machen Komponenten bei Denial-of-Service(DoS)-Attacken anfällig für Überlastung. Unvollständig und nicht ro-

bust implementierte Protokoll-Stacks führen zu Fehlreaktionen und Abstürzen, wenn unerwarteter Datenverkehr im Netzwerk auftritt. Ferner lässt das Fehlen von Authentifizierungs- und Autorisierungsmechanismen in den meisten Steuerungen auch protokollkonforme Daten zum Risiko werden, sofern diese von falschen, nicht berechtigten Absendern kommen. All dies erweist sich infolge der zunächst einmal unbeschränkten, offenen Kommunikation in Ethernet-Netzwerken als problematisch. Jeder Teilnehmer kann an jeden anderen Teilnehmer beliebige Pakete senden und damit gewollt oder ungewollt Schwachstellen treffen und Schäden auslösen. Wie also lässt sich ein höheres Sicherheitsniveau erreichen?

Denkbare Lösungsansätze

Als Maßnahmen kommen prinzipiell eine verbesserte Härtung und intrinsische Sicherheit der Netzwerkteilnehmer sowie die Kontrolle und Beschränkung der Kommunikation zwischen den Teilnehmern in Betracht. Eine Umsetzung dieser Maßnahmen auf den Automatisierungskomponenten selbst würde der Vorstellung von sicheren Endgeräten entsprechen. Als alternativer Ansatz sind eine künftig weitreichendere Integration von Sicherheitsfunktionen in die Netzwerk-Infrastruktur (Switches) oder der Einsatz dedizierter Sicherheitsmodule (Firewalls und Security Appliances) denkbar. Dabei lassen sich Beiträge zu den verschiedenen Aspekten der Netzwerksicherheit jeweils nur auf den geeigneten Ebenen des OSI-Schichtenmodells leisten. So kann über die Teilnahme am Netzwerk bereits auf dem Data Link Layer-2 entschieden werden, während die Festlegung prinzipiell möglicher Kommunikationsbeziehungen auf dem Network Layer-3 sowie konkret zulässiger Verbindungen auf dem Transport Layer-4 erfolgt. Die Berechtigungen einzelner Teilnehmer auf der Anwendungsebene werden erst jenseits dieser Layer bestimmt.

Sichere Endgeräte

Es ist durchaus vorstellbar, dass komplexere Automatisierungskomponenten den Port-Security-Standard IEEE 802.1X unterstützen und die korrekte Authentifizierung und Autorisierung ihrer Kommunikationspartner etwa auf Basis von Transport Layer Security (SSL/TLS) und Berechtigungskonzepten überwachen. Darüber hinaus sind der generellen Realisierung sicherer Endgeräte jedoch enge Grenzen gesetzt. Die Implementierung einer 'Personal Firewall' auf jeder einzelnen Steuerung, Busklemme oder Sensor/Aktor-Komponente wäre allein aus Ressourcen- und Kostengründen technisch und/oder wirtschaftlich nicht darstellbar. Außerdem hätte ein solcher Schutz eine übertrieben hohe Granularität. Sinnvoller wäre es, Maschinen, Fertigungszellen und andere Steuerungsbereiche als Ganzes vor unbefugten Zugriffen abzusichern. Die innerhalb solcher Einheiten installierten Komponenten können dann bei geeigneter Abschirmung von einer 'freundlichen' Umgebung ausgehen.

Sichere Netzwerk-Infrastruktur

Heute am Markt erhältliche Switching-Komponenten zum Aufbau industrieller Ethernet-Netzwerke reichen von nicht (Unmanaged) oder nur begrenzt (Lean Managed) konfigurierbaren Geräten bis zu Managed Layer-2- und -Layer-3 Switches. Letztere verfügen bereits über Fähigkeiten zur Segmentierung von Netzwerken durch VLANs (Virtual Local Area

Network) und Routing in Verbindung mit Access-Control-Listen (ACLs) für die Paketfilterung, gehören aber einem Preis-Leistungs-Segment an, das üblicherweise erst ab der Leitebene und im Backbone von Netzwerken vorzufinden ist. Je weiter solche Sicherheitsfunktionen jedoch im Netzwerkbaum nach oben verlagert werden, desto geringer wird die mögliche Granularität der Kontrolle bei gleichzeitig zunehmender Komplexität der auf dem einzelnen Switch zu konfigurierenden Regeln. Außerdem stellen, die in dieser Switch-Klasse angebotenen Paketfilter, keine Firewall nach aktuellem Stand der Technik (Stateful Packet Inspection) dar. Zeitgemäße Layer-3 Security-Funktionen in die, für die unteren Ebenen entwickelten, Switches zu integrieren, würde aufgrund der großen Variantenvielfalt in diesem Segment und der dafür benötigten höheren Prozessorleistung eine erhebliche Herausforderung bedeuten. Nachdem schon der vergleichsweise geringe Aufpreis für herkömmliche Managed Switches viele Anwender von der Verwendung solcher Geräte auf der Feldebene abhält und nicht jeder Switch-Port als schutzbedürftig betrachtet wird, ist das Angebot eines kompletten Portfolios von 'Security Switches' für die Feld- und Steuerungsebene zu marktfähigen Stückkosten kaum vorstellbar.

Modulare Lösung

Im Gegensatz zu sicheren Endgeräten oder einer sicheren Netzwerk-Infrastruktur lassen sich dedizierte Sicherheitsmodule wie die FL MGuard Security Appliances von Phoenix Contact flexibel und dezentral auf allen Netzwerkebenen einsetzen. Unabhängig von der jeweiligen Topologie und Verkabelung bringen sie Sicherheit genau dorthin, wo sie gebraucht wird. Dank Stateful Inspection Firewall und Quality-of-Service-Funktionen für das Band-

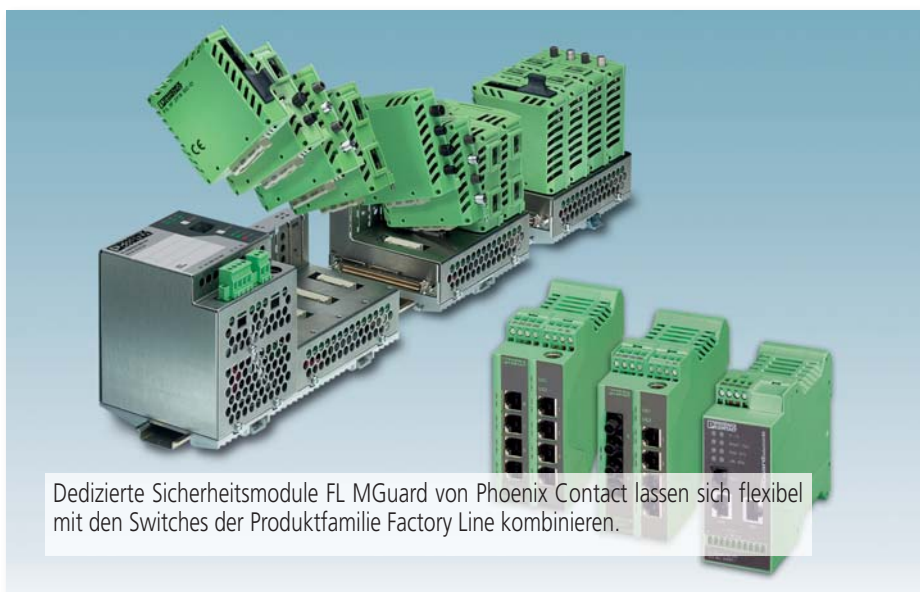
breiten-Management erlauben die Security Appliances eine präzise Kontrolle und Filterung der Kommunikationsverbindungen. Die dafür je Gerät zu konfigurierenden Regeln bleiben überschaubar, da sie meist nur lokal für ein Schutzobjekt (Maschine, Zelle) wirken sollen. Trotz ihrer physischen Verteilung im Feld können die Sicherheitsmodule FL MGuard durch eine Device-Management-Software zentral und effizient administriert werden. Sofern die Schutzobjekte einen Router zur Netzwerk-Integration benötigen, was häufig der Fall ist, belaufen sich die Mehrkosten für die gewonnene Sicherheit auf weniger als 200 Euro pro Security Appliance, die anstelle eines einfachen Routers installiert wird. Das modulare Konzept unterstützt bei der Begrenzung der Variantenvielfalt und Stückkosten.

Fazit

Intrinsische IT- und Netzwerksicherheit durch umfassende Härtung aller Automatisierungskomponenten ist technisch und wirtschaftlich nicht sinnvoll erreichbar sowie in dieser Form auch nicht erforderlich. Die Netzwerk-Infrastruktur kann grundlegende Port Security und Segmentierung leisten, stellt aber keine ausreichend präzise und feine Kontrolle der Kommunikation zur Verfügung. Flexibel kombinierbare dedizierte Security-Module bieten daher konzeptionell den leistungsfähigsten und kostengünstigsten Ansatz für die Sicherheit vernetzter Systeme sowie einen interessanten Mehrwert in den Bereichen Routing und sichere Fernwartung. ■

Autor Dipl.-Math. Torsten Rössel, Director Business Development, Innominate Security Technologies AG, Berlin.

www.innominate.de



Dedizierte Sicherheitsmodule FL MGuard von Phoenix Contact lassen sich flexibel mit den Switches der Produktfamilie Factory Line kombinieren.