

Netzwerksicherheit im Feld

Würmer und Viren stellen die Automatisierungstechnik vor neue Herausforderungen

Das Thema Netzwerksicherheit wird in der Büroumgebung schon lange groß geschrieben – zu oft haben Viren und Würmer bereits komplette Firmennetze zum Erliegen gebracht. Anders in der Automatisierungstechnik. Hier erreichen zwar immer mehr Ethernet-basierte Kommunikationsstrukturen die Feldebene, doch in Sachen Sicherheit muss erst noch ein Problembewusstsein entstehen. Schließlich kann der Ausfall einer Maschine oder Anlage enorme Kosten nach sich ziehen. OLAF SIEMENS



EAGLE 2TX – erstes Hirschmann-Produkt mit integrierter Innominate mGuard-Technologie



Dipl.-Inf. Olaf Siemens ist Vorstand der Innominate Security Technologies AG in Berlin
Tel.: 030/6392-3300
Mail: osiemens@innominate.com

Klassische Automatisierungsanwendungen sind Insellösungen mit sehr speziellen Aufgaben und einem örtlich begrenzten Einsatzgebiet. Doch während sich auf Fabrikebene in der Regel PCs als Engineering-Stationen und lokale Netzwerke mit Internetanschluss befinden, ist die Verbreitung von Kommunikationsstandards aus der Bürowelt in der Leit- und der Feldbustechnik bisher noch nicht annähernd so weit vorgedrungen.

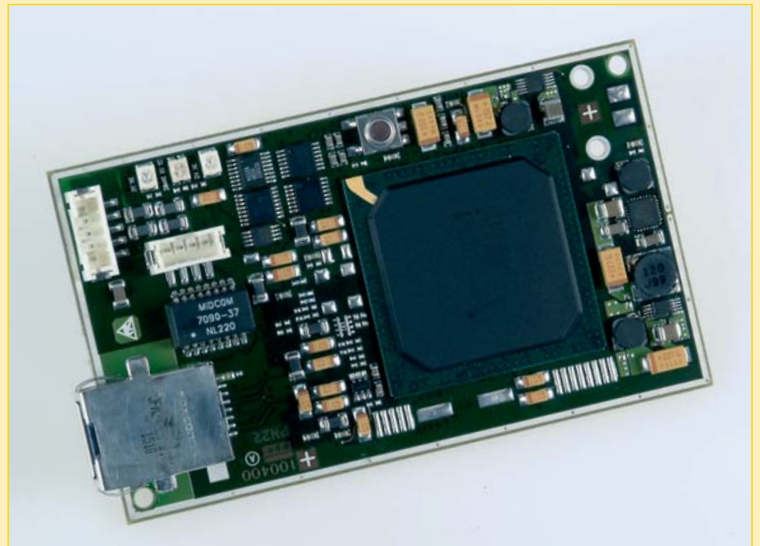
In jüngerer Zeit macht aber das Innovationstempo in der Informationstechnologie die offenen Standards Ethernet und TCP/IP so erfolgreich, dass diese zunehmend für alle Bereiche der industriellen Kommunikation relevant werden. Die erheblich geringeren Kosten für Standardkomponenten tragen zum weiteren Siegeszug von Ethernet und TCP/IP in der

Automatisierung bei. Der Einsatz von Ethernet als „Industrial Ethernet“ mit seinen nicht immer hundertprozentig kompatiblen Spielarten wie Profinet und Ethernet IP wird sich in den nächsten Jahren auch für harte Echtzeitanwendungen empfehlen.

Eine weiterer Trend: Die Nutzung offener Kommunikationsprotokolle in der Automatisierungstechnik befördert den Einsatz von Standard-Betriebssystemen wie Windows Embedded und Embedded Linux, die über die nächsten Jahre viele kleinere Embedded- und Real-Time-Betriebssysteme aus dem Markt drängen werden. Umgekehrt erlauben diese Betriebssysteme die Realisierung immer komplexerer, stärker vernetzter und interaktiverer Lösungen. Dadurch wiederum erhöht sich der Druck zur Einführung von Standard-Kommunikationsprotokollen. Der heute schon für viele Geräte in



Der mGuard ist als externes Modul und als PC-Karte verfügbar



der Automatisierung weit verbreitete Bedienzugang über Internet-Browser und HTTP wird beispielsweise erst durch eine durchgängige Nutzung von TCP/IP machbar. Dies führt zunehmend zur örtlich weit verteilten Automation. Beispiele sind die örtliche Trennung von Überwachung und Steuerung insbesondere kleiner technologischer Anlagen, das heißt: eine zentrale Steuerung dezentraler Anlagen. Weiterhin wird der Trend zur Einführung von Agententechnologien in weit verzweigten Unternehmen eine stark verteilte Infrastruktur erfordern, zum Beispiel Tele-Interaktion oder Tele-Service.

In der Diskussion um die Vorteile der Bürostandards in der Automatisierung und beim Ringen um die neuen Ethernet-Standards für die Feldebene ist das Thema IT- und Netzwerksicherheit bisher erstaunlicherweise wenig diskutiert worden. Dabei ist abzusehen, dass die

stärkere Standardisierung und Vernetzung in der Automatisierung auch zu einer höheren Anfälligkeit dieser Netze führt. Die Bedrohung kommt dabei durch die Gefahren, denen die Nutzer im Büro schon lange ausgesetzt sind und gegen die sie sich mit dem Einsatz gängiger Sicherheitslösungen mehr oder weniger erfolgreich zu wehren versuchen.

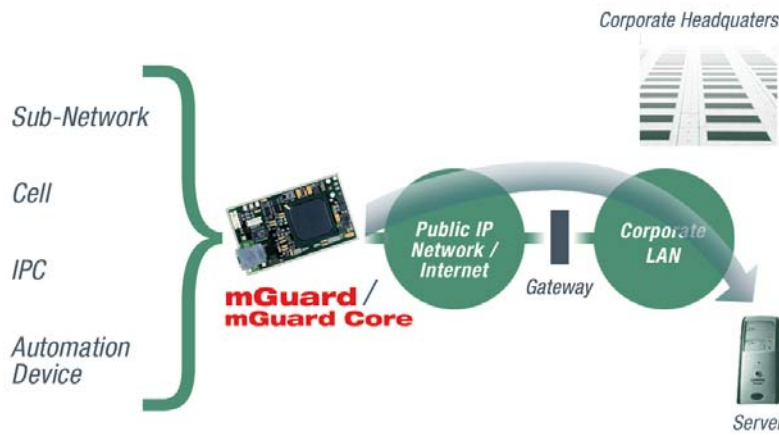
Würmer und Viren rüsten zum Angriff

Würmer und Viren, die das eine oder andere Büronetz schon für Tage lahm gelegt und so manchem IT-Verantwortlichen den Job gekostet haben, drohen in Zukunft auch verstärkt Automatisierungsnetze zu befallen. Die Tatsache, dass Windows sich in der Automatisierung im-

mer weiter verbreitet, erhöht die Notwendigkeit für grundlegende Lösungen zur Sicherstellung der Funktionsfähigkeit Ethernet- und TCP/IP-basierender Netzwerke. So werden hier und da hinter vorgehaltener Hand auch schon Berichte darüber erzählt, wie Viren oder Würmer, die sozusagen die „Artengrenze“ überschritten haben, Produktionsabläufe empfindlich gestört haben. Auch Servicetechniker mit Zugang zu durchgängig vernetzten Steuerungen und Maschinen stellen ein Risiko für die Netzwerksicherheit dar.

Damit heißt das Gebot der Stunde: Bei der Planung und Implementierung neuer Netzwerkinfrastrukturen das Thema Sicherheit von Anfang an berücksichtigen. Allerdings: Die derzeit verfügbaren Lösungen, die in der Regel aus der Bürokommunikation stammen, sind nur begrenzt für die Automatisierung tauglich. Zum

Remote Access

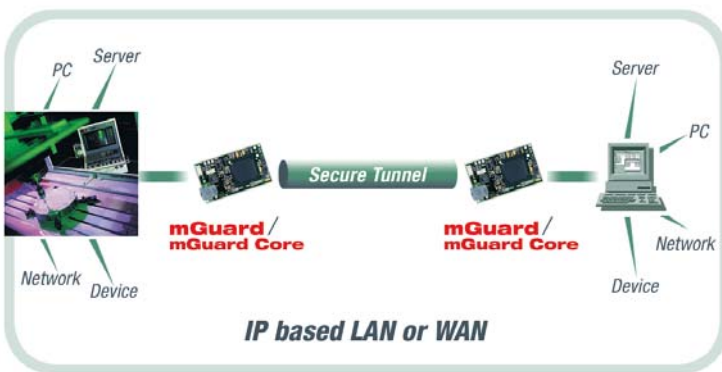


Gesicherte Zugänge ermöglichen auch die gefahrlose Steuerung räumlich getrennter Systeme per Internet

Beispiel ist für Fernwartungszugänge eine durchgängige Kommunikation notwendig. Hier ist es nicht damit getan, eine zentrale Firewall zum Schutz des Übergangs zwischen Büro- und Automatisierungsnetz zu betreiben, da Sicherheit bis zum Endgerät gewährleistet werden muss. Für den Einsatz zum Beispiel an einer Fertigungszelle sind existierende Hardware-Firewalls jedoch in der Regel zu teuer, zu groß und nicht auf die Erfordernisse industrieller Umgebungen angepasst.

Sich alleine auf den Schutz durch das Embedded-Betriebssystem zu verlassen, verbietet sich von selbst. Reine Softwarelösungen für Security, die zusätzlich zum Betriebssystem installiert werden können, scheiden oft aus, weil die Performance für die Ausführung von Sicherheitsfunktionen – gerade bei Verschlüsselung – nicht gegeben ist. Darüber hinaus müssten immer noch sehr viele verschiedene Embedded-Systeme auf den zu schützenden Geräten unterstützt werden. Weiterhin lässt sich nicht aus-

Secure Intranet Communications



Über einen VPN-Tunnel lassen sich Daten im Intranet „abhörer“ austauschen

schließen, dass eine zusätzliche Softwarekomponente das Verhalten des zu schützenden Geräts störend beeinflusst.

Passende Sicherheitslösungen

Die Innominate Security Technologies AG aus Berlin hat die Miniatur-Security-Appliance „Innominate mGuard“ als Lösung für den Schutz vor Gefahren, Angriffen und Fehlbedienungen aus Internet und Intranet entwickelt, um damit effizient vor Schaden durch Viren und Würmer zu schützen. Die mGuard-Technologie wurde jetzt von Hirschmann Electronics als Basis der eigenen Produktfamilie für industriegerechte Netzwerksicherheit „EAGLE“ implementiert. Das mit 20 x 56 x 95 Millimetern hoch miniaturisierte Sicherheitsmodul mGuard lässt sich zentral oder dezentral einsetzen. Die Security Appliance basiert auf der Kommunikationsprozessorfamilie IXP42x von Intel. Diese ist mit ihren Eigenschaften für Embedded Security und Kommunikationsaufgaben dafür bestens geeignet. Die Sicherheitslösung kommt ohne Lüfter oder andere bewegliche Teile aus, woraus eine sehr geringe Fehleranfälligkeit der Hardware resultiert. Außer Firewall- und VPN-Funktionalität mit hardwareunterstützter Verschlüsselung bietet die Appliance auch optionalen Virenschutz sowie Serverdienste wie DHCP und DNS. Dazu hat man eine bei Innominate besonders für Sicherheitsanwendungen „gehärtete“ Variante von Linux eingesetzt. Durch diese offenen Standards sind Anpassungen an verschiedene Projekt- und branchenspezifische Anforderungen leicht durchführbar. Eine der größten Gefahren für den Betrieb eines IP-basierenden Produktionsnetzes stellen Viren und Würmer dar. Diese Bedrohung besteht neben den bekannten Schadenswirkungen auf vorhandenen Daten und Programme vor allem auch darin, dass zusätzliche Verkehrslasten erzeugt werden. Diese müssen durch das Automatisierungssystem verarbeitet werden und verändern im ungünstigsten Fall das Echtzeitverhalten eines Systems. Die Security Appliance von Innominate arbeitet mit Stateful Inspection, das heißt: Eingehende und ausgehende Datenpakete werden an Hand vordefinierter Regeln überwacht. Damit ist gewährleistet, dass nur autorisierte Verbindungen entgegengenommen werden. So entsteht ein Schutz vor schädlichem Netzwerkverkehr.

Darüber hinaus ist die Sicherheitslösung mit der neuesten Stealth-Technologie ausgestattet. Diese eignet sich für den Schutz einzelner Maschinen oder Produktionszellen, lässt sich aber auch in Industrieprodukte und Geräte der Automatisierungstechnik integrieren. Die Konfiguration ist einfach gehalten: Absender- und Empfängeradressen, Netze und IP-Adressen lassen sich ohne großen Aufwand erfassen. Durch Network Address Translation (NAT) können verschiedenste Maschinen hinter einer einzigen IP-Adresse angebunden werden.

Die Firewall kann in den zwei Betriebsmodi Stealth- und Router-Modus arbeiten: Der „Stealth-Modus“ ermöglicht die Integration in bestehende Netzwerkstrukturen ohne Konfigurationsänderungen an dahinter liegenden Maschinen. Die Security Appliance wird einfach in den bestehenden Datenstrom der zu schützenden Maschine „eingeschleift“. Eingehende Verbindungen können gesperrt werden, nur autorisierte ausgehende Verbindungen sind erlaubt.

Mit Tarnkappe durch den VPN-Tunnel

Der patentierte „Stealth-Modus“ erlaubt es, einen VPN-Tunnel transparent für das zu schützende Gerät aufzubauen. Ein VPN (Virtual Private Network) ist eine verschlüsselte Verbindung zwischen zwei Rechnern oder Netzwerken, die an das Internet oder Intranet angebunden sind. Diese Verbindung ist nur von den Teilnehmern nutzbar, für die sie auch eingerichtet wurde. Somit agiert ein VPN wie ein Tunnel, durch den Datenpakete nur durch einen ganz speziellen Ausgang zum Empfänger gelangen. Darüber hinaus verleiht der „Stealth-Modus“ dem Innominate mGuard – und auf seiner Technologie basierenden Produkten wie Hirschmanns EAGLE – eine Art Tarnkappe, die es für potenzielle Angreifer fast unmöglich macht, das Gerät zu attackieren. Im Router-Modus stellt sich die Sicherheitslösung als Standard-Gateway zum unsicheren Netzwerk dar und erlaubt den Anschluss einzelner Maschinen oder großer Produktionszellen.

Konfiguriert wird die Security Appliance durch den Secure Socket Layer (SSL), der die Verbindung zwischen Server und Browser kontinuierlich verschlüsselt und somit die Daten vor dem Zugriff Dritter schützt. Dadurch lässt sich unter anderem die Versionsnummer von jedem einzelnen Softwareprogrammpaket abfragen. Dies vereinfacht das Identifizieren von Sicherheitslücken im Softwarebestand.

Fazit

Hirschmann Electronics hat den Stellenwert von Netzwerksicherheit in der Automatisierung erkannt. Daher hat der Anbieter von Netzwerkkomponenten für die industrielle Automatisierung im Herbst vergangenen Jahres eine strategische Partnerschaft mit dem Berliner Security-Spezialisten Innominate geschlossen. Das Ergebnis: Hirschmann-Kunden erhalten mit der neuen industriegerechten Produktfamilie EAGLE bereits heute „State-of-the-Art“-Sicherheit für den Einsatz in ihrer Automatisierungslösung.

Beitrag als PDF auf www.aud24.net

more @ click AD024753 >

How to use

more @ click

1. www.aud24.net
2. „more@click“-Code in eingeben
3. Beitrag aufrufen und weiterführende Informationen (ähnliche Beiträge, technische Daten, Direktlinks zum Hersteller etc.) auf www.aud24.net recherchieren.