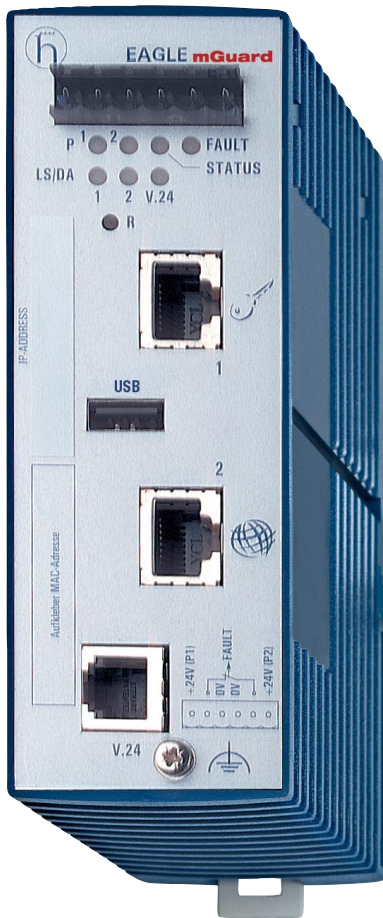


Secure Automation mit Industrie-Firewall



Die ARC Advisory Group prognostiziert: im Jahr 2006 werden weltweit 6,7 Mio. Industrial-Ethernet-Komponenten ausgeliefert – 2004 lag die Menge noch bei deutlich unter 1 Mio. vernetzten Komponenten. Im Zuge der stetigen Prozessoptimierung treiben immer mehr produzierende Unternehmen die vertikale Integration ihrer Netzwerke voran. Wachstumsraten von jährlich über 50 % spiegeln den Wunsch nach nahtlosen Zugriffsmöglichkeiten auf Produktionsdaten und einer effizienten zentralen Produktionssteuerung wider.

Die vernetzte Welt hat aber auch ihre Schattenseiten: Nicht nur geplante und erlaubte Zu- und Eingriffe auf und in Produktionsprozesse werden über das gemeinsame Ethernet-Protokoll vereinfacht, auch die Gefahr von Fehlbedienungen und Störungen über die Netzwerkzugänge steigt. An den Stellen, an denen früher die Inkompatibilität der Protokolle Produktionsnetze wie Inseln in der Unternehmens-IT geschützt haben, sind nun neue Kont-

Konvergenz und Standardisierung sind derzeit die prägenden Trends in der Netzwerkwelt. Kommunikationsbarrieren werden beseitigt, einst klar getrennte Teilnetzwerke wachsen zusammen und sprechen nun dieselbe Sprache. TCP/IP und Ethernet sind auf dem Vormarsch und haben nun auch die bisher von Bus-systemen dominierten Produktionshallen erreicht. Synergien und verbesserte Zugriffsmöglichkeiten auf Produktionssysteme sind die gewünschten Effekte, eine durchgängige Sicherheitspolitik die daraus folgende Notwendigkeit.

rollinstanzen notwendig, die Zugriffe regeln und überwachen.

Dedizierte Sicherheitslösungen gefragt

Nicht von außen – hier schützt in den meisten Fällen die zentrale Unternehmens-Firewall –, sondern von innerhalb des Unternehmensnetzwerks stammen die meisten Schadprogramme, die Automationsanlagen lahmlegen. Der durchschnittliche Schaden, den ein Sicherheitsvorfall durch Viren oder Würmer anrichtet, liegt bei etwa 1,5 Mio. € pro Vorfall. Das sind die Zahlen aus einem aktuellen Report der Management-, System- und Technologieberater der PA Consulting Group. Ihrer Ansicht nach zieht die Prozessautomatisierung außerdem zunehmend die Aufmerksamkeit von Hackern auf sich. Bereits 13 % der Sicherheitsvorfälle in diesem Umfeld von 2002 bis 2005 können als Sabotage klassifiziert werden.

Die Industrie-Firewall

Die Hardware-Firewall Eagle mGuard wurde in Kooperation mit dem „Industrial Security Alliance“-Partner Hirschmann Automation and Control GmbH speziell für den Einsatz im industriellen Umfeld entwickelt. Sie kombiniert die Eigenschaften einer Stateful Inspection Firewall, die eingehende und ausgehende Datenpakete an Hand vordefinierter Regeln überwacht, mit der Möglichkeit einer sicheren und vertraulichen Kommunikation über Virtual-Private-Network-Verbindungen (VPN) und Virenschutz. Ihre Tauglichkeit für industrielle Anwendungen wird unter anderem in der Erfüllung relevanter Industriestandards, der Hutschienenmontage und dem Bedienkonzept deutlich.

Eagle mGuard kann als eigenständiges System in das Netzwerk integriert werden und schützt ein Teilnetz, die Produktionszelle oder das einzelne Automatisierungsgerät. Eine wesentliche Komponente des

Konzepts ist die Rückwirkungsfreiheit der Firewall auf das System selbst. Im sogenannten Stealth Mode bemerkt die Maschine nicht, dass ihr im Netzwerk eine Security Appliance vorgeschaltet ist und ihre IP-Adresse nutzt; auch für mögliche Angreifer ist die Firewall dadurch unsichtbar. Dabei kann die Stealth-Firewall ihren Schutz entfalten, ohne dass sie das zu schützende System berührt. Eingriffe in das Betriebssystem oder Konfigurationen an der Maschine sind auch bei Si-

Eagle mGuard

- Robuste Security Appliance für die Hutschienenmontage,
- Security Appliance mit direkter Zuordnung zu dem zu schützenden System,
- schützt ein System oder ein Segment in der Produktion,
- verhindert wirkungsvoll Angriffe oder Fehlbedienungen von innen,
- verschlüsselt Zugänge für die sichere Fernwartung und
- ist leicht installierbar und wartungsfreundlich.

cherheits-Updates nicht notwendig; das kommt auch der Nachrüstung bestehender Systeme zugute.

Fernwartung über das Internet

Die Fernwartung von Produktionsanlagen gestaltet sich sicherlich effizienter als die mehrmalige Ausendung von Techniker-Teams in die Fertigungshallen. Um von den Möglichkeiten der Fernwartung jedoch ausgiebig profitieren zu können, bedarf es einer zuverlässigen, störungsfreien Wartungsverbindung. Eine Lösung ist der Fernzugriff durch VPN-Tunnel und bei Bedarf auch über ein Service-Web-Portal.

Eine Alternative zum Modem stellt das Breitband-Internet dar. Highspeed-Verbindungen auf Breitbandbasis gewährleisten, dass Techniker auch umfangreiche Software- und Daten-Uploads bis zu einer Größe von mehreren Hundert Megabyte schnell und sicher durchführen können. Zudem sind webbasierte Dienste installierbar.



Mit dem mGuard bladePack kann jedem unternehmenskritischen Server-System seine eigene Sicherheitskomponente zugewiesen werden: mit individuellem Sicherheits-Level, mit speziell konfigurierter Zugriffsberechtigung, ...

Ein Beispiel einer internetbasierten Lösung stellt der mGuard Tele Service mit dem Eagle mGuard dar. Er erlaubt die gesicherte Ferndiagnose und -wartung – von der einzelnen Maschine bis hin zu Produktionsanlagen. Der Datentransfer zwischen dem zu wartenden Produktionssystem und dem zentralen Techniker-Gateway wird sicher auf Grundlage der VPN-Technologie realisiert. Auf diesem Weg

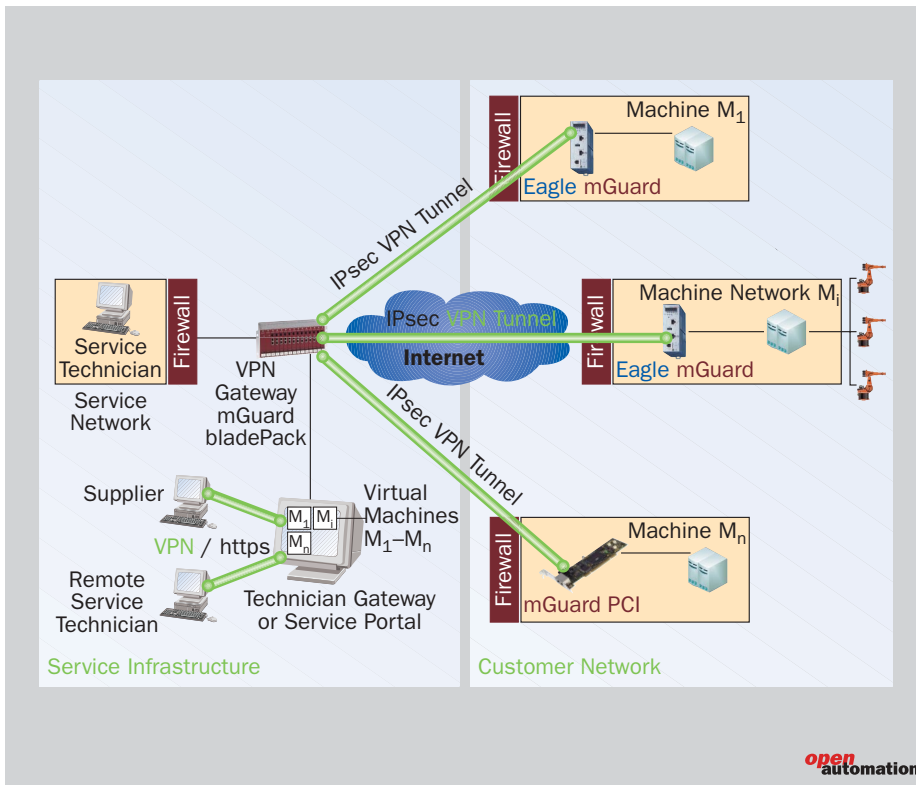
ist es möglich, Standard-IPsec-Verbindungen zu nutzen oder wahlweise über HTTP(S) und einen Proxy-Server zu tunneln.

Techniker können über ein zentrales VPN-Gateway oder ein Service-Portal auf den Eagle mGuard an der Maschine zugreifen und über eine gesicherte VPN-Verbindungen mit den zu wartenden Maschinen oder



Andreas Beierer übernahm Mitte 2005 die Leitung des Marketingressorts sowie die Betreuung der Partner-Alliances bei der Innominate Technologies AG in Berlin.

Anlagen kommunizieren. Um Verbindungen nicht auf der Basis teils unsicherer Anfragen von außen aufbauen zu müssen, stellt die



mGuard Tele Service: Der Eagle mGuard erlaubt die sichere Ferndiagnose und -wartung von der einzelnen Maschine bis hin zu kompletten Produktionsanlagen

Firewall eine eigene, von der Maschine ausgehende Verbindung mit dem VPN-Gateway her.

Konfigurationsmanagement

Über das zentrale Management Tool „Innominate Device Manager“ kann die Inbetriebnahme tausender dezentraler Fernwartungseinheiten abgewickelt werden. Außerdem ist für die Fernwartung von Produktionsstraßen keine speziellen Security-Aus-/Weiterbildung für das Personal erforderlich. Die vereinfachte Installation und Handhabung reduziert außerdem die Ausgaben für die IT-Infrastruktur und die Betriebskosten.

Fazit

Die internetbasierte Fernwartung zeichnet sich durch ihre Verfügbarkeit sowie schnelle Verbindungen aus und bezieht dabei hohe Sicherheitsstandards ein. Dadurch ebnet sich auch der Weg für eine effiziente Kombination von aktuellen Breitband-Technologien, wie Voice-over-IP oder Bild- und Video-Streaming, mit den Möglichkeiten der Teleservices. **Andreas Beierer**