



SPS/IPC/DRIVES

Halle 9

Stand 125

Sicheres Ethernet auf Feldebene

Trend in Produktionsnetzen

Ethernet hat sich in Office-Umgebungen zum unumstößlichen Standard entwickelt. Im Zuge der Vereinheitlichung von IT-Infrastrukturen und der unternehmensweiten Vernetzung ist die Ausdehnung des Standards auf weitere Unternehmensbereiche nur logisch. Ethernet-Standardkomponenten sind kostengünstiger als proprietäre Lösungen und bieten Zukunftssicherheit. Doch Kosten- und Nutzenversprechen dürfen nicht darüber hinwegtäuschen, dass der Standard Schwächen in die neuen Netzbereiche mitbringt.



Vor allem Sicherheit spielt in diesem Zusammenhang eine entscheidende Rolle, denn durch die Standardisierung steigt die Zahl der Nutzer, die auf kritische und ehemals relativ isolierte Bereiche Zugriff hat. Im Gegensatz zum Ethernet-Standard lassen sich etablierte Sicherheitskonzepte wie Office-Firewalls nicht so einfach in die Produktionsnetze übertragen. Dort gelten eigene Spielregeln, die wiederum spezialisierter Lösungen bedürfen. Die europäische Automatisierungsmesse SPS/IPC/Drives hat in diesem Jahr unter anderem „Offenes Ethernet in der Automatisierung“ und „Safety und Security in der Automatisierung“ als Schwerpunkte gewählt. Das hohe Interesse an diesen Themen ist Ausdruck der gegenwärtigen Entwicklung in Produktionsnetzen: der Trend zu unternehmensweit durchgängigen Ethernet-Infrastrukturen ist immer deutlicher zu spüren. Anbieter industrieller Anlagen und Bauteile spüren die aufkommende Nachfrage und integrieren Ethernet-Schnittstellen in Produkte wie speicherprogrammierbare Steuerungen (SPS). Bis zum Jahr 2009 soll sich die Zahl der verkauften Industrial Ethernet-Geräte laut den Analysten der ARC Advisory Group im Vergleich zu 2004 etwa versiebenfachen. Produzierende Unternehmen weltweit erwarten sich Kosteneinsparungen durch Synergien und verbesserte Zugriffsmöglichkeiten auf Produktionssysteme, beispielsweise für erweiterte Fernwartungskonzepte. Mit dem Vormarsch von „Industrial Ethernet“ rückt der Sicherheitsaspekt der zunehmend vernetzten Infrastruktur stärker ins Bewusstsein der Anwender. Die ins Gesamtnetzwerk integrierten Produktions-Systeme verein-

fachen den Zugriff auf Fertigungsstraßen und Maschinen von zentralen Steuerungspunkten oder Fernwartungs-PCs aus. So gewährleisten sie einen schnelleren Informationsrückfluss aus den Hallen in die Planungs- und Managementsysteme. Da durch den einheitlichen Standard nun aber auch die Barrieren für Schadprogramme sinken und die erweiterten Zugriffsmöglichkeiten die Wahrscheinlichkeit von Fehlbedienungen erhöhen, müssen Maßnahmen getroffen werden, die Störungsfreiheit und Ausfallsicherheit der teuren Produktionsanlagen sicherstellen.

Sichere und robuste Lösungen

Im Produktionsumfeld unterscheiden sich Anforderungen an effiziente Schutzlösungen von denen im Office-Umfeld. Während im Büro gelegentliche Fehler zwar möglichst auszuschließen sind, aber oftmals tolerierbar, haben Produktionsausfälle meist gravierende finanzielle Konsequenzen. Für den Schutz der in der Regel homogenen Betriebssystemlandschaft in Office-Netzen eignen sich zentrale Software-Firewalls. In vielen Fällen ist es unmöglich, dieselben Firewalls für die Produktionsanlagen einzusetzen, weil auf Fertigungsebene ältere Prozessortechnologien oder Betriebssysteme laufen, die kostengünstiger sind und für ihre Zwecke verlässlich die benötigte Performance bieten. Für den Betrieb mit den aktuellsten Security-Patches reichen ihre Systemeigenschaften und -leistungen jedoch meist nicht aus. Hardware-Appliances vom Server-Raum in die Produktionshallen zu bringen, ist auf Grund der dort vor-

Das Eagle mGuard-Konzept...

... wurde für den Einsatz im industriellen Umfeld entwickelt. Es 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. Netzwerk-Integration als eigenständiges System ist ebenso möglich wie der Schutz von Teilnetzen, Produktionszellen oder einzelnen Automatisierungsgeräten. Durch den patentierten „Stealth Mode“ schützt die Firewall ein System, ohne es zu berühren. Eingriffe in das Betriebssystem oder Konfigurationen an der Maschine sind auch bei Sicherheitsupdates nicht notwendig. Mit dem Innominate Device Manager (IDM) steht ein zentrales Management-System für den effizienten Roll-out der mGuard Firewall Appliances und für die Rechtevergabe zur Verfügung.

herrschenden äußeren Bedingungen nicht ohne Weiteres möglich. Eine mechanische Stabilität gegen Schocks oder Vibration, die Funktionsfähigkeit in Temperaturbereichen von mindestens -40°C bis $+60^{\circ}\text{C}$, elektromagnetische Verträglichkeit, die besonderen Anforderungen an die Spannungsversorgung oder ganz einfach die Möglichkeit der Montage auf den in den Hallen verwendeten Hutschienen sind Voraussetzungen, die Office-Hardware nicht mitbringt. Inzwischen haben Anbieter auf die neuen Anforderungen reagiert und kombinieren Sicherheit mit der notwendigen Robustheit. Innominat Security Technologies ist ein Pionier am Markt für Industrial Security. Eine Kooperation mit dem etablierten Anbieter von Automatisierungs- und Netzwerktechnik Hirschmann Automation and Control schafft unter dem Namen „Industrial Security Alliance“ Bewusstsein für die Sicherheitsrisiken im Industrial Ethernet. Die Partner bieten Security-Lösungen für die Fernwartung über Ethernet/IP (Internet-Protokoll) an, die auf der gemeinsam entwickelten Industrie-Firewall Eagle mGuard basieren.

Standard-technologie für Zulieferer

Ethernet verbreitet sich als Standard nicht nur unternehmensweit, sondern über ganze Lieferketten hinweg. Hochintegrierte Lieferketten setzen zunehmend auf die Vernetzung unternehmensübergreifender IT-Systeme. Automatische Bestellvorgänge eines Automobilherstellers bei seinen Zulieferern in zeitkritischen Just in Time-Konzepten sind nur ein Beispiel. Die Einführung von Industrial

Ethernet in den Produktionshallen der Hersteller zieht teilweise schon fast zwangsläufig die Einführung der Standardtechnologien bei den Zulieferern nach sich. Haben diese in Bezug auf die Sicherheit der neuen Infrastrukturen bereits effektive Maßnahmen installiert, so stärkt dies neben dem Schutz der eigenen Systeme auch das Vertrauen der Kunden und Partner in die Zusammenarbeit. Investitionen in die netzüber-

greifende Sicherheit sind so auch immer Investitionen in eine erfolgreiche Geschäftsentwicklung. ■

Info

Autor Andreas Beierer ist Marketingleiter bei der Innominat Security Technologies AG in Berlin.

www.innominat.de