

Industrial Ethernet – Aber sicher!

In einer Studie von 2005 sagen die Marktforscher der ARC Advisory Group dem Markt für Industrial Ethernet ein jährliches Wachstum von 51,4 Prozent über die nächsten fünf Jahre voraus [1]. In Deutschland sollen es sogar 59 Prozent werden. In 2004 wurden weltweit lediglich um die 840.000 Industrial Ethernet-Komponenten ausgeliefert, für 2009 prognostizieren die ARC-Berater ein Marktvolumen von 6,7 Millionen Geräten. Diese Zahlen sprechen für sich. Unternehmen mit eigener Produktion versprechen sich einiges von Investitionen auf diesem Gebiet: ein einfacheres Management durch den verbreiteten Ethernet-Standard, simples „Plug-and-Produce“ beim Hinzufügen neuer Maschinen, die direkte Vernetzung mit zentralen Managementsystemen oder Updates der Produktionssysteme über TCP/IP vom Planungsbüro aus – all das soll zu Kostensenkungen und Effizienzsteigerungen beitragen.

Damit diese Rechnung aufgehen kann, muss die reibungslose Funktionsfähigkeit der bereichsübergreifenden Netzwerke sichergestellt sein. Eine der wichtigsten Infrastruktur-entscheidungen in diesem Zusammenhang betrifft die Auswahl der richtigen Sicherheitsstrategie. Hier gilt: Lösungen aus den Office-Netzen sind nicht ohne weiteres auf die Produktion übertragbar. Die spezifischen Anforderungen im Fertigungsumfeld erfordern angepasste Konzepte. Ein grundlegendes Verständnis der Rahmenbedingungen in der

Automatisierung ist die Voraussetzung für die richtige Wahl und erfolgreiche Einführung einer effizienten, unternehmensweiten Sicherheitslösung.

Fertigung vs. Büro – Zwei Welten, eine Lösung?

Für die IT in der Fertigung gelten Rahmenbedingungen und Anforderungen, die sich von jenen im Büro grundlegend unterscheiden. In der Automatisierung ist vor allem die Stabilität der Systeme, beziehungsweise deren ständige Verfügbarkeit, essenziell. Der

Ausruf „Nein! Word ist gerade abgestürzt!“ hat zur Folge, dass ein Dokument im schlimmsten Fall noch einmal erstellt werden muss. Der Ausruf „Nein! Die Biegemaschine ist mitten im Prozess ausgefallen!“ kann bedeuten, dass auf einen Schlag tausende Euro vernichtet wurden. Eine Betrachtung der Anforderungen im Produktionsumfeld hilft, eine geeignete Lösung einzugrenzen:

- Zum Teil werden in der Produktion – aus Kostengründen und weil sie verlässlich die benötigte Performance bieten – ganz bewusst ältere

Prozessortechologien oder Betriebssysteme eingesetzt. Allein dieser Umstand schließt bereits einige Software-Sicherheitslösungen aus, weil für sie die vorhandenen Systemeigenschaften und -leistungen nicht ausreichen oder sie vom älteren Betriebssystem nicht unterstützt werden.

- Eine rein softwarebasierte Sicherheitslösung, die von zentraler Stelle auf alle IT-Systeme aufgespielt wird, eignet sich für manche Branchen ohnehin nicht. Im Chemie- oder Pharma-Sektor müssen bestimmte Maschinen validiert werden, bevor sie überhaupt den Betrieb aufnehmen dürfen. Jede Veränderung – beispielsweise durch regelmäßig notwendige Sicherheits-Patches – zieht erneut den Zertifizierungsprozess nach sich, der die Maschine um

	Büro	Produktion
Zuverlässigkeit	<ul style="list-style-type: none"> • Gelegentliche Fehler tolerierbar • „Beta Test“ im Feld üblich 	<ul style="list-style-type: none"> • Unterbrechungen nicht hinnehmbar • Ausgiebige Qualitätssicherung vorausgesetzt
Risiko	<ul style="list-style-type: none"> • Verlust von Daten 	<ul style="list-style-type: none"> • Verluste bei Produktion, Anlagen oder möglicherweise Gesundheit und Leben
Performanz	<ul style="list-style-type: none"> • Hoher Durchsatz • Lange Laufzeiten im Netz akzeptabel 	<ul style="list-style-type: none"> • Geringerer Durchsatz hinnehmbar • Lange Laufzeiten kritisch
Wiederanlauf	<ul style="list-style-type: none"> • Lange Zeiten für Wiederherstellung/-anlauf akzeptabel 	<ul style="list-style-type: none"> • Schneller Wiederanlauf/Austausch essentiell
Risiko Management	<ul style="list-style-type: none"> • Wiederanlauf durch Reboot • Safety spielt keine Rolle 	<ul style="list-style-type: none"> • Hohe Fehlertoleranz erforderlich
Homogenität	<ul style="list-style-type: none"> • In der Regel homogenes Umfeld (Betriebssystem etc.) 	<ul style="list-style-type: none"> • Sehr heterogen
Security	<ul style="list-style-type: none"> • Zentrale Firewall • Gateway – Ansatz 	<ul style="list-style-type: none"> • Dezentrale Sicherung von Systemen

Diagramm: Anforderungen an IT-Sicherheit in Büro und Produktion.

bis zu zwei Wochen, in manchen Fällen sogar noch länger, lahm legt und hohe Kosten verursacht.

- In der Produktion ist es aufgrund von Wartungsarbeiten regelmäßig der Fall, dass externe Geräte wie das Laptop des Servicedienstleisters Zugriff auf einzelne Bereiche des Netzwerks erhalten. Es genügt deshalb nicht, eine zentrale Firewall wie eine Mauer rund um das gesamte Unternehmensnetzwerk zu legen. 70 bis 80 Prozent aller Störfälle werden nicht durch Angriffe von außen, sondern durch unerlaubte, fahrlässige oder einfach nur unachtsame Zugriffe und Handlungen an Systemen von innerhalb des Netzwerks

verursacht. Besser ist die Absicherung hochsensibler und teurer Produktionsanlagen in Gruppen oder einzeln. Da eine Sicherheitssoftware, die direkt auf dem System der Maschine



läuft, problematisch ist, empfehlen sich sogenannte Hardware-Security-Appliances, die vor die Maschine geschaltet werden können.

- Um ihre Funktion erfüllen zu können, müssen Hardware-Lösungen die not-

wendige Robustheit und Ausstattung mitbringen, um mit den Bedingungen im Fabrik-Umfeld zurecht zu kommen. Vibration, Hitze, Staub und Maschinenlärm, eine Versorgungsspannung von meist 24 Volt anstatt von 220 Volt im Büro, 35-Millimeter-DIN-Hutschienen, die als Tragschiene dienen anstatt Racks – diese Bedingungen machen den Einsatz von Lösungen aus der Bürowelt unmöglich.

Aus den sehr unterschiedlichen Voraussetzungen in Produktion und Büro wird deutlich, warum bewährte Lösungen nicht ohne weiteres übertragen werden können. Um den vielfältigen Anforderungen an die Netzwerksicherheit im Bereich der Automatisierungstechnik gerecht zu werden, kommen im zunehmenden Maße Firewall-Systeme zum Einsatz, die für den Einsatz im industriellen Umfeld konzipiert wurden. Stateful Inspection Firewalls, wie sie sich auch im Büroumfeld durchgesetzt haben, stellen dabei den Stand der Technik dar. 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. Die Industrie-Firewall wird als eigenständiges System in das Netzwerk integriert und schützt ein Teilnetz, die Produktionszelle oder das einzelne Automatisierungsgerät. Dieses Konzept wird auch als „device attached security“ bezeichnet.

Mit „device attached security“ näher an die Maschine

„device attached security“ bezeichnet die Absicherung von Maschinengruppen oder einzelnen Anlagen direkt am Gerät:

„device attached security“

- Direkte Zuordnung der Firewall zu dem zu schützenden System
- Schützt ein System oder ein Segment in der Produktion
- Verhindert wirkungsvoll Angriffe oder Fehlbedienungen von innen
- Migration ermöglicht passgenaue Security
- Verschlüsselt Zugänge für die sichere Fernwartung

die Security-Appliance wird zwischen Netzwerkanschluss und Ethernet-Schnittstelle in den Datenstrom „eingeschleift“. Eine entscheidende Komponente des Konzepts ist die völlige Rückwirkungsfreiheit der Firewall auf das System selbst. Im patentierten „Stealth Mode“ des Berliner Sicherheitsspezialisten Innominat ist dies der

Fall: die Maschine bemerkt nicht, dass ihr im Netzwerk eine Security-Appliance vorgeschaltet ist und ihre IP-Adresse nutzt – und auch für mögliche Angreifer ist die Firewall dadurch unsichtbar. Die Stealth-Firewall kann ihren Schutz entfalten, ohne dass sie das zu schützende System berührt. Eingriffe in das Betriebssystem oder Konfigurationen an der Maschine sind auch bei Sicherheitsupdates nicht notwendig. Deshalb ist auch eine Nachrüstung bestehender Systeme problemlos möglich.

„device attached security“ unterstützt eine einfache Migration der Security-Maßnahmen und erlaubt das kostenoptimierte Sichern von Fertigungssegmenten (Maschinengruppen) bis hin zum Schutz der einzelnen Maschine. Mit dieser Vorgehensweise kann eine passgenaue Absicherung von Produktionsanlagen geplant und realisiert werden.

Systemverfügbarkeit maximieren

Haben sich die Verantwortlichen für eine Sicherheitslösung entschieden, wünschen sie sich vor allem drei Dinge: das Sicherheitssystem soll möglichst sofort und dann ohne Unterbrechung verfügbar sein. Fällt eine Komponente aus, darf die Funktionsfähigkeit nicht beeinträchtigt werden und die Komponente muss mit minimalem Zeitaufwand ersetzt werden können. Schließlich muss auch das System sehr einfach zu konfigurieren und zu verwalten sein, sodass beispielsweise im Krisenfall auch Mitarbeiter, die keine IT-Experten sind, auf unvorhersehbare Ereignisse reagieren können.

- Die Konfiguration von Regeln oder Policies für ein Automatisierungsnetz hat einen gravierenden Einfluss auf die Betriebssicherheit (Safety). Oft ist aber nicht einmal dokumentiert, welche Ports benutzt werden. Innominat's mGuard-Firewall-Reihe, zu der auch die Hutschienen Security-Appliance mGuard industrial gehört, sieht deshalb die Unterstützung des Anwenders bei der Erstellung von Security Policies vor. Der sogenannte „Learning Mode“ ist mit dem Teach-in eines Roboters vergleichbar und erlaubt es, aus dem Beobachten des Netzwerkverkehrs Regeln abzuleiten.
- Innominat bietet außerdem die Möglichkeit, einzelne mGuard-Firewalls im laufenden Betrieb auszutauschen. Eine redundante Firewall übernimmt bei einem Ausfall des Primärgeräts in der Zwischenzeit die Absicherung.

Ergänzend zur Firewall-Redundanz wird mit der Auto-konfigurations-Funktion das Austausch-Device im Fehlerfall automatisch konfiguriert und so über ein einfaches „Plug-and-Produce“ wieder in Betrieb genommen.

Fazit

Produktionssysteme werden immer intelligenter und der Bedarf Daten auszutauschen nimmt entsprechend stark zu. Der schnelle und ungehinderte Informationsfluss zwischen den Systemen und hin zur übergeordneten Steuerungsebene ist Voraussetzung für eine effiziente Produktionssteuerung. Das rasante Wachstum von vernetzten Produktionssystemen gebietet es, dem Thema Industrial Security schon bei der Planung neuer Systeme eine gewichtige Rolle einzuräumen.



Andreas Beierer
Director
Marketing & Alliances der
Innominat Security
Technologies AG, Berlin

[1] ARC Advisory Group, „Industrial Ethernet Market Outlook Study“, April 2005, vgl. www.computerwoche.de/produkte_technik/netzwerke/564742/.

Innominat Security Technologies AG, Albert-Einstein-Strasse 14, 12489 Berlin, Tel. +49 30 639 23-688, Fax -307, E-Mail: contact@innominate.com, www.innominate.com.