

Firewall-Security in der Automation

Aktueller Entwicklungsstand und Tendenzen

IP-basierte Ethernet-LANs sind heute aus Produktionsnetzen nicht mehr wegzudenken. Die Verschmelzung der ehemals abgeschotteten Produktionswelt mit den restlichen Unternehmensbereichen und dem Internet bringt einerseits ein enormes Einsparpotenzial mit sich. Andererseits birgt die Vernetzung ohne entsprechende Sicherungsmaßnahmen auch hohe Risiken.



Nur durch eine effiziente und für Produktionsnetze angepasste Sicherheitsstrategie können Unternehmen die Systemverfügbarkeit sicherstellen

Andreas Beierer

Werden diese Risiken nicht erkannt und neutralisiert, können Schadprogramme zu Produktionsverlusten oder sogar zum Ausfall des Produktionsprozesses führen. Nur durch eine effiziente und für Produktionsnetze angepasste Sicherheitsstrategie können Unternehmen die Systemverfügbarkeit sicher stellen.

Zu den Alpträumen jedes Systemverantwortlichen gehört sicherlich folgendes Szenario: Bei regulären Servicearbeiten stellt ein Wartungstechniker einer externen Firma eine Verbindung zwischen seinem Notebook und der Steuerung eines Industriesystems her. Der Wartungstechniker hat an diesem Tag schon mehrere Systeme untersucht. Zwischenzeitlich blieb keine Zeit, das

Notebook gründlich zu überprüfen und ein verstecktes Schadprogramm blieb unbemerkt.

Dieses gelangt nun auf das ungeschützte Industriesystem. Hat es sich dort erst eingenistet, lässt es seine Präsenz sehr schnell spüren: Plötzlich steht eine Maschine still, eine Produktionslinie liegt lahm oder ein Roboter spielt verrückt. Der Schaden ist entsprechend groß.

70 bis 80 Prozent aller Störfälle werden durch unerlaubte, fahrlässige oder einfach auch unachtsame Zugriffe und Handlungen an Systemen innerhalb des Netzwerks verursacht. Die zentrale Firewall wird dabei umgangen und ist als Schutzschild gegen diese Angriffe von innen völlig nutzlos. Die Sicherung hochsensibler und teurer Produktionssysteme erfordert tiefergehende Maßnahmen.

Sicherheitsplanung von Anfang an

Bei der Planung und Budgetierung einer neuen Netzwerkinfrastruktur – oder bei der Migration bestehender Systeme auf neue Standards wie Ethernet – muss das The-

ma Sicherheit von Anfang an berücksichtigt werden. Anstatt die Absicherung der Produktionsnetze ausschließlich in die Hände der zentralen IT-Abteilung zu legen, sollte die Planung einer geeigneten Security-Lösung in enger Abstimmung mit allen Unternehmensbereichen erfolgen.

Sicherheitslösungen aus dem Büro eignen sich nicht automatisch auch für den Produktionsbereich. Die – auch aus dem Office-Bereich bekannte – *Stateful Inspection Firewall* stellt den neuesten Stand der Technik dar. Diese Art von Firewall überwacht sowohl eingehende als auch ausgehende Datenpakete nach vordefinierten Regeln. Ausschließlich autorisierte Verbindungen werden zugelassen.

Eine Alternative zu Software-Firewall/Virenschutz-Lösungen können beispielsweise verteilte und systemunabhängige hardwarebasierte Firewall-Lösungen sein. Eine hardwarebasierte Firewall wird direkt vor das zu schützende System geschaltet und berührt und beeinflusst die darauf laufende Software nicht. Diese „*device attached security*“ ist vor al-

lem im Produktionsumfeld von Vorteil.

Zentrale Software-Firewalls haben den Vorteil, dass sie oft günstiger sind als eine Einzelabsicherung von Systemen. Doch dies ist nur so lange der Fall, bis es ein Virus oder ein Wurm schafft, die relativ unspezifische Sicherung zu knacken. Fällt



Produktion ist durch unternehmensweite Vernetzung nun den selben Gefahren wie Büroumgebungen ausgesetzt



Andreas Beierer,
Director Marketing &
Alliances, Innominate
Security Technologies
AG, Berlin

www.innominate.com

eine Produktionsstraße für Stunden aus, so kostet dies in den meisten Fällen mehr, als ein PC-Absturz im Büro verursachen könnte. Fertigungsnetze benötigen spezialisierte Sicherheitslösungen.

Checkliste – Basisplanung eines Sicherheitssystems

- ▶ Welche zentralen Firewalls/Router existieren bereits?
- ▶ Auflistung aller kritischen Produktionssysteme, die einzeln abzusichern sind
- ▶ Auflistung aller weniger kritischen Systeme, die segmentweise gesichert werden können
- ▶ Festlegung der Security-Levels: Sind gesicherte Verbindungen nach außen erforderlich? Sind interne Serviceschnittstellen vorhanden?
- ▶ Festlegung der Security-Policies: Gibt es bereits vorhandene Regeln, welche die Zugriffsrechte festlegen? Falls nicht, schrittweise Freischaltung der Rechte

Industrie-Firewalls für die Produktion

Die Voraussetzungen in der Fertigung in Bezug auf IT und Sicherheit unterscheiden sich von denen im Büro, weshalb auch die Anforderungen an Sicherheitslösungen deutlich andere sind. Die Systemverfügbarkeit beispielsweise spielt eine ungleich größere Rolle, Ausfallzeiten sind unakzeptabel.

In der Produktion findet man oft ältere Betriebssysteme in unterschiedlichen Versionen vor. Eine zentrale Sicherheits-Software ist schon deshalb ein Problem. Hardware-Lösungen für die Industrie müssen robust und einfach zu bedienen sein. Dass Firewall-Appliances Sicherheit und Systemverfügbarkeit bereit stellen, versteht sich von selbst.



Zur Absicherung einer großen Zahl verschlüsselter Übertragungskanäle: Innominate mGuard bladePack

Stealthmode – Firewall mit Tarnkappe

Modernste Firewall-Funktionalitäten und Virenschutz sind die Basis einer Sicherheitslösung. Sehr effektiv ist ein Schutzschild, wenn Angreifer von außen nicht wissen, dass es da ist. Die mGuard-Firewalls von Innominate beispielsweise arbeiten im *Stealth Mode* und übernehmen die IP-Adresse ihrer zu schützenden Systeme. Sie haben folglich keine nach außen hin sichtbare Identität. Auch für das System selbst sind die Firewalls so *unsichtbar*.

Die steigende Komplexität industrieller Systeme macht es unerlässlich, dass Zugriffe von außen möglich sind – beispielsweise um eine Fernüberwachung oder Fernwartung durchzuführen. Damit Systeme durch diese Zugriffe nicht gefährdet werden, sollte die Firewall sichere *Virtual Private Networks (VPN)* unterstützen, abgesicherte Einzelverbindungen zwischen den einzelnen Systemen und Netzbereichen.

Zusätzlich zu den Hardware-Firewalls muss ein intuitives und einfach zu verwaltendes Security-Policy-Management verfügbar sein, welches Administratoren über graphische Benutzeroberflächen Zugriffsrechte verwalten lässt. Erst so kann eine nachvollziehbare und lückenlose Sicherheitsstruktur gewährleistet werden.

Wofür steht „device attached security“?

- ▶ Direkte 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

Unabhängige Systemverfügbarkeit

Maschinen die stehen, kosten Geld. Sicherheitssysteme müssen ihre Schutzfunktion erfüllen, ohne dass sie die laufenden Systeme gefährden. Doch auch dies ist schon vorgekommen: Ein namhaftes Unternehmen der Prozessautomatisierung in den USA hatte in der Leittechnik eines Industrie-PCs Anti-Virus-Software installiert. Durch ein Fehlverhalten der Software wurde die Notabschaltung eines wichtigen Kesselsystems verhindert.

Dieses Beispiel zeigt, dass es sinnvoll ist, die Software der Einzelsysteme und die Software der zugeordneten Firewall voneinander unabhängig zu halten. Dies bietet außerdem den Vorteil, dass zertifizierungspflichtige Systeme, beispielsweise in der Pharma-Branche, nach Sicherheits-Updates nicht jedes Mal neu validiert werden müssen. Läuft die Sicherheits-Software hingegen auf dem Industrie-System, müsste es nach dem Aufspielen eines neuen Sicherheitspatches aus dem Betrieb genommen werden, bis es die neue Zertifizierung erhalten hat.

Die hier vorgestellten mGuard bladePacks bieten seit November 2005 außerdem die Möglichkeit, einzelne Firewallblades, die zur Absicherung des Backoffice-Bereichs zwischen Büro und Produktion verwendet werden, im laufenden Betrieb auszutauschen. Diese Eigenschaft bietet auch der speziell für den Einsatz auf DIN-Hutschienen entwickelte mGuard industrial. In beiden Fällen übernimmt eine redundante Firewall bei einem Ausfall des Primärgeräts in der Zwischenzeit die Absicherung und überspielt die vorgesehenen Konfigurationen innerhalb kürzester Zeit auf ein Ersatzgerät.

Systemverfügbarkeit bedeutet auch, dass eine neue Sicherheitsinfrastruktur schnell einsatzfähig ist. In diesem Zusammenhang hat Innominate kürzlich den *Learning Mode* vorgestellt. Damit werden im Einrichtungsprozess alle Datenverbindungen mitprotokolliert, das System kann dem Administrator selbständig und automatisch Sicherheitsregeln vorschlagen. So können aus dem laufenden Netzwerkverkehr die sinnvollsten *Security Policies* abgeleitet und nach der Freigabe durch den Si-



Industrielle Security Appliance für die Hutschiene: Innominate mGuard industrial

cherheitsverantwortlichen oder das Management scharf geschaltet werden.

Fazit

Die Produktion sieht sich durch die unternehmensweite Vernetzung nun den selben Gefahren ausgesetzt, die in Büroumgebungen schon lange bekannt und gefürchtet sind. Dennoch sind die dort etablierten Sicherheitsmechanismen nicht ohne weiteres übertragbar. In der Industrie gelten eigene Gesetze. Einige wenige Sicherheitsanbieter haben dies verstanden und bieten spezialisierte Lösungen an.

WIR ÜBER UNS

Die Innominate Security Technologies AG ist Spezialist für Security Appliances im Umfeld industrieller Kommunikation (M2M) und zur Absicherung einzelner IT-Systeme. Das 2001 gegründete Unternehmen bietet mit der mGuard Produktfamilie Firewall-, VPN- und Virenschutz-Funktionalitäten. Die mGuard Appliances werden in verschiedenen Bauformen als Dongle, PCI-Karte, Blade-Server oder Hutschienengerät vertrieben.