

# Mehr Sicherheit durch Security Policy Management

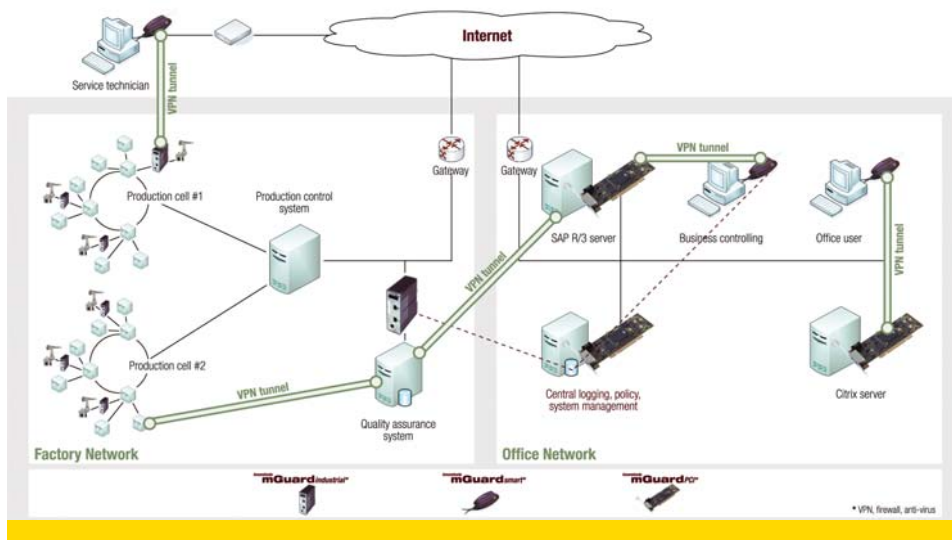


Bild 1: Zugriff des Security Policy Managements ISCM auf verteilte Firewalls

Durch die steigenden Anforderungen an die Netzwerksicherheit in der Automatisierung halten immer mehr Firewall- und Virtual Private Network-Geräte (VPN) Einzug in die Produktion oder produktionsnahe Bereiche. Solche industriellen Security Appliances müssen in ein Management-Konzept eingebunden werden. Dabei spielt neben der Überwachung auch die einfache und nachvollziehbare Definition von Security Policies eine wichtige Rolle für die Wirksamkeit solcher Sicherheitssysteme.

Durch den Einsatz von Security Policy Management Systemen wird die Wahrscheinlichkeit versehentlicher Falschkonfiguration oder widersprüchlicher Sicherheitsregeln nahezu ausgeräumt. Außerdem lässt sich festlegen, welche Personen Policies definieren und welche Personen diese dann für den Wirkbetrieb freigeben dürfen. Damit wird die Verwaltung von Firewallregeln und die Einrichtung komplexer VPN-Konfigurationen vereinfacht. Viel wichtiger ist jedoch, dass sich durch die Übersichtlichkeit und Nachvollziehbarkeit auch die Sicherheit erhöht. Die primäre Aufgabe eines Netzwerkes ist es, Daten schnell und zuverlässig zu transportieren. Diesem traditionellen Verständnis eines Netzwerkes wurde in den letzten Jahren eine weitere wichtige Aufgabe hinzugefügt: Im Netz-

werk muss es möglich sein, erwünschten von unerwünschtem Datenverkehr zu trennen. Die zunehmende Gefahr für die Sicherheit, die von einer Vernetzung von Automatisierungs- und Büronetzwerken und einer fortschreitenden Adaption von Standards wie TCP/IP und Ethernet ausgeht, macht Maßnahmen für einen sicheren Datenverkehr erforderlich. Zum Schutz vor Fehlbedienung oder vor Angriffen auf Automatisierungssysteme aus dem Inneren und der Unterbindung der Verbreitung von Würmern ist es geboten, Industrial Ethernet Netzwerke mit industriellen Firewall- und VPN-Systemen sicherer zu gestalten. Mehr Firewalls bedeuten dabei aber nicht automatisch auch mehr Sicherheit. Wie so oft macht der richtige Einsatz dieser Technologien den Unterschied: Das effiziente

und nachvollziehbare Management von Komponenten für die Netzwerksicherheit spielt die entscheidende Rolle bei der Erhöhung der Sicherheit eines Automatisierungsnetzwerkes. Laut den Ergebnissen einer MetaGroup-Studie von 2004 ignorieren immer noch 30% aller Unternehmen weitgehend alle Gefahren, die IT-Systemen drohen. Immerhin 50% sind

sich der Sicherheitsprobleme bewusst. Diese haben mit der Definition von Regelwerken für die Sicherheit begonnen und so die größten Löcher bereits gestopft. Aber erst 20% aller untersuchten Unternehmen sind auch dabei, umfassende Sicherheitsarchitekturen umzusetzen. Würde eine solche Untersuchung im Bereich der Automatisierung durchgeführt, würden

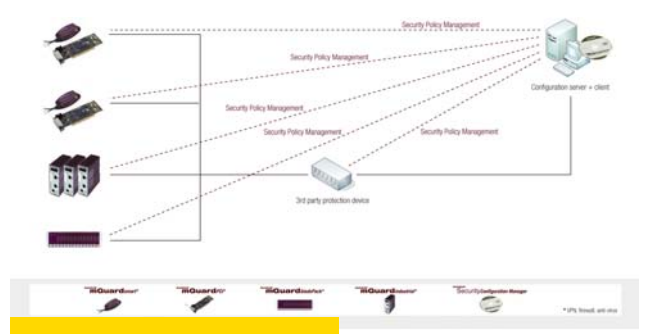


Bild 2: Management von Sicherheitsregeln in komplexen Netzwerken

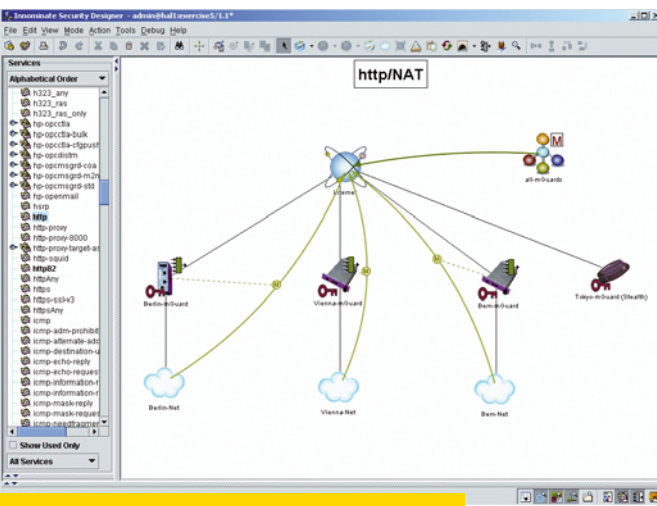


Bild 3: Grafische Oberfläche des Security Policy Management Systems ISCM

diese Zahlen noch schlechter ausfallen. Dabei ist anzumerken, dass das Sicherheitsbewusstsein vieler Automatisierungsanwender in den letzten 12 bis 18 Monaten deutlich gestiegen ist – leider oft durch entsprechende Sicherheitsvorfälle. Von den Unternehmen, die heute schon industrielle Firewallsysteme einsetzen, werden die wenigsten einen guten Überblick über die in ihrem Produktionsnetz angewandten Regelwerke haben. Oft werden nach dem Prinzip „ein wenig Sicherheit hier und ein wenig dort“ lokale Lösungen implementiert. In den seltensten Fällen wird es möglich sein, sicher zu stellen, dass ein einheitlicher Satz an Regeln auf alle zu schützenden Geräte, Zellen oder Teilnetze angewandt wird. Ein kritische Frage zur Beurteilung der Effizienz der implementierten Netzwerksicherheitslösungen ist: „Wie lange dauert es, alle Schutzmaßnahmen bei einer akuten Bedrohung neu zu konfigurieren?“

## Was sind Security Policies?

Firewall-Regeln legen fest, welche Datenverbindungen eine Firewall erlaubt und welche nicht. Dabei wird das Quell- und Zielnetzwerk und der benutzte Port definiert. Das Management einer Firewall setzt tiefgehende Netzwerkkenntnisse voraus und bezieht sich jeweils auf eine einzelne Firewall. Anders eine „Security Policy“: Hierunter versteht man eine allgemein gehaltene Vorschrift, die Zugriffe auf Netzwerkressourcen regelt und festlegt wie diese Regeln durchzusetzen sind. Damit beschreibt sie die grundlegende Sicherheitsarchitektur in einem Netz. Eine Security Policy legt auf einer übergeordneten Ebene fest, welche Zugriffe erlaubt sein

sollen. Anders als in detaillierten, technischen Firewallregeln oder so genannten Access Control Lists (ACLs), wird z.B. definiert: „Der Zugriff über das File-Transfer-Protokoll FTP ist vom Büronetz auf alle Produktionszellen in Linie 1 erlaubt.“ Eine solche Policy beschreibt auf eine einfach nachzu-

vollziehende Weise, was ohne Policy Management in vielleicht vielen Hundert einzelnen Regeln auf einer Vielzahl von Geräten mit schwer lesbaren Zahlenkolonnen hätte programmiert werden müssen. Die Summe aller Policies sollte den gewollten und erlaubten Netzwerkverkehr beschreiben und implizit alle anderen – unerwünschten – Zugriffe ausschließen. Eine wesentliche Abgrenzung zu anderen Managementsystemen liegt darin, dass Security Policy Systeme übergreifend die Sicherheitsregeln, beispielsweise für ein ganzes Werk, definieren und sich nicht darauf beschränken, die Firewallregeln auf Ebene eines einzelnen Firewallgerätes zu verwalten. Dadurch können z.B. logische Fehler, Widersprüche in Regelwerk und Zahlendreher

## Goldene Regeln für mehr Sicherheit in Automatisierungsnetzen

1. Die Ausgangsbasis aller Firewallregeln sollte lauten: „Alles verboten, nichts erlaubt“.
2. Ports und Dienste zwischen dem Automatisierungsnetz und externen Netzwerken sollten nur für einzelne Anwendungen und nur nach einer Sicherheitsbetrachtung im Einzelfall geöffnet beziehungsweise erlaubt werden.
3. Alle „erlaube“ Regeln sollten so einschränkend wie möglich sein und möglichst immer einzelne IP-Adressen und Ports beinhalten. Wann immer möglich, sollten Regeln „stateful“ sein, also den zu einer ausgehenden Verbindung gehörigen Rückkanal beachten.
4. Alle nicht IP-basierten Protokolle sollten auf Leit- und Fabrikebene vermieden/unterbunden werden. Nur dadurch lassen sich Security Policies wirklich umfassend durchsetzen.
5. Der Netzwerkverkehr zwischen Automatisierungsnetzwerk und dem Büronetz sollte immer über eine so genannte DMZ (demilitarized zone = entmilitarisierte Zone) geführt werden.
6. Jede Produktionszelle sollte durch eine separate Firewall geschützt werden, die nicht nur den eingehenden sondern auch den ausgehenden Verkehr reguliert. Dadurch lässt sich die Ausbreitung von Sicherheitsproblemen (Viren, Würmer) eindämmen.
7. Der ausgehende Verkehr vom Automatisierungsnetz sollte immer Quelle und Ziel über statische Regeln an Ports bzw. Dienste binden.
8. Automatisierungsgeräte sollten niemals direkten Zugang zum Internet haben. Durch vorgeschaltete Sicherheitslösungen lässt sich ein kontrollierter Fernwartungszugang einrichten.
9. Das Management von verteilten Firewall-Systemen sollte nur über verschlüsselte Verbindungen mit starker Authentifizierung erfolgen und auf einzelne IP-Adressen und Ports beschränkt sein.

vermieden werden. Mit der Hilfe von Security Policies können sich Produktions- und Automatisierungsexperten darüber hinaus besser mit den Verantwortlichen für die Netzwerksicherheit über Anforderungen verständigen.

## Anforderungen an Netzwerksicherheitskomponenten

Das Management von Netzwerksicherheitskomponenten in Automatisierungsnetzen stellt besondere Anforderungen. So hat die Konfiguration von Regeln oder Policies für ein Automatisierungsnetz einen gravierenden Einfluss auf die Produktion und die Betriebssicherheit (Safety). Alle Änderungen an den Security Policies sollten deshalb denselben Mechanismen unterliegen, wie es Änderungen an SPS-Systemen auch tun. Alle Regeln sollten klar dokumentiert sein und es Dritten ermöglichen, die Konsistenz und Fehlerfreiheit zu überprüfen. Dies erleichtert auch die Arbeit in der Praxis: Das Schließen aller unbenutzten Ports ist beispielsweise eine erste und

sehr wichtige Maßnahme zur Erhöhung der Sicherheit. Dies setzt aber voraus, dass bekannt und hoffentlich dokumentiert ist, welche Ports benutzt werden. Des Weiteren existieren eine Reihe funktionaler Anforderungen: Es sollte beispielsweise keine direkte Verbindung zwischen Internet und Automatisierungsnetzwerk erlaubt sein, gleichzeitig aber ein eingeschränkter Zugriff vom Büro- auf das Automatisierungsnetzwerk ermöglicht werden. Darüber hinaus sind in vielen Fällen ein autorisierter Zugriff aus dem Büronetz auf einzelne Automatisierungsgeräte und ein autorisierter Fernwartungszugang zu einzelnen Maschinen erforderlich. Um diese Anforderungen umzusetzen ist oftmals eine Vielzahl industrieller Security Appliances im Einsatz, die einheitlich verwaltet werden sollten. Die oben genannten Anforderungen lassen sich mit Hilfe eines Security Policy Management Systems wie dem Innominate Security Configuration Manager leicht umsetzen. Damit lassen sich nicht nur

mGuard Systeme von Innominate, sondern auch Systeme anderer Hersteller managen.

## Security Policy Management Systemen

Ein wichtiges Ziel des Security Policy Management ist es, die Übereinstimmung der auf die Firewallgeräte geladenen Regeln mit den vorgegebenen Policies sicher zustellen. Dazu werden im Falle des Innominate Security Configuration Managers bei Änderungen von Security Policies alle davon abhängigen Firewallregeln ebenfalls geändert und auf den Firewalls aktualisiert. Dabei werden Transparenz und Nachvollziehbarkeit der Regelwerke gewährleistet. Denn nur eine transparente Verwaltung der Sicherheitseinstellungen ist für Dritte einfach nachzuvollziehen und zu überprüfen. Ein Policy Management System folgt in der Regel einem vier-Augen-Prinzip: Die Verantwortlichkeiten für das Erstellen von Policies, für die Freigabe in den operativen Betrieb und für die Überprüfung (Audit) werden meistens durch verschiedene Personen oder Organisationen vorgenommen. Durch die Trennung dieser Rollen erhöht sich die Sicherheit, weil nie nur eine Person über neue Firewallregeln entscheidet. Weitere Unterstützung bieten Policy Management Systeme beim Austesten neuer Regeln, bei der grafischen Aufbereitung und bei der Gestaltung des Workflows. Sehr hilfreich erweist sich auch die Unterstützung bei der Einrichtung so genannter VPNs – also verschlüsselter Verbindungen zwischen zwei Systemen oder Teilnetzen. Obwohl die meisten VPN-Systeme den Standard IPsec implementiert haben, steckt hier der Teufel häufig im Detail. Anwender, die keine IT-Security Experten sind, stehen oft vor größeren Herausforderungen, wenn zwei VPN-Geräte verschiedener Hersteller verbunden werden sollen. Hier kann das Policy Management System aushelfen: Der Innominate Security Configuration Manager hat eine umfangreiche Datenbank der

gebräuchlichsten Produkte und kennt alle Eigenschaften und Eigenarten dieser VPN-Gateways. Der Administrator kann sich darauf beschränken zu definieren, wie hoch die Anforderung an die Sicherheit und Performance einer verschlüsselten Verbindung sein soll – den Rest übernimmt das Managementssystem. Security Policy Systeme ersetzen klassische Netzwerkmanagementsysteme, die in der Regel auf SNMP basieren nicht, sondern ergänzen diese. Mit Hilfe des Policy Managements Systems lässt sich die Einhaltung der Security Policy überwachen und der Prozess des Erarbeitens und Freigebens neuer Regeln gestalten. Mit Hilfe eines Netzwerkmanagementsystems kann auf den Ausfall einzelner Firewallgeräte reagiert werden.

## Fazit

Das umfassende Management von Security Policies kann für die Erhöhung der Sicherheit von Automatisierungsnetzwerken von entscheidender Bedeutung sein. Durch die Definition von Security Policies wird die Transparenz und Nachvollziehbarkeit erhöht und die Kommunikation zwischen Produktion und IT befördert. Viele Fehlerquellen werden ausgeschlossen und das Management verschiedener Geräte über Hersteller Grenzen hinweg erleichtert. ■



Autor: Olaf Siemens ist Vorstand der Innominate Security Technologies AG, Berlin.

Glossar	
<b>ACL</b>	Access Control List = Regel zur Definition erlaubten oder nicht erlaubten Netzverkehrs
<b>TCP/IP</b>	Transfer Control Protocol/Internet Protocol = gebräuchlichstes Kommunikationsprotokoll in der Datenübertragung
<b>VPN</b>	Virtual Private Network = Methode zur Verschlüsselung und eindeutiger Identifizierung bei Datenübertragungen
<b>FTP</b>	File Transfer Protocol = Das gebräuchlichste Protokoll für den Dateitransfer im Internet
<b>Firewall</b>	Geräte oder Software zur Kontrolle erlaubter Datenverbindungen
<b>Wurm</b>	Ein dem Computervirus ähnliches Schadprogramm, das im Gegensatz zum Virus aber nicht auf die Weiterverbreitung durch einen Anwender wartet, sondern sich selbst weiterverbreitet (Beispiele: Sasser, MyDoom)
<b>Appliance</b>	Kombination aus Hardware und Software, die eine einzige Aufgabe (hier: IT-Sicherheit) erfüllt
<b>Stateful</b>	Eigenschaft einer Firewall, bei der Datenpakete der Hin- und Rückrichtung einem logischen Datenstrom zugeordnet werden
<b>SNMP</b>	Simple Network Management Protocol = gebräuchlichstes Protokoll für die Überwachung von Netzwerkkomponenten

[www.innominate.de](http://www.innominate.de)