

Quarantäne für Endgeräte ergänzt die Netzsegmentierung – Erste Produkte sind bereits erhältlich

# Zonenmodell sichert gegen Angriffe vom Hintereingang

Segmentierung und Quarantäne schützen gegen aktuelle Bedrohungen besser als der klassische Firewall-Ansatz, der Datenpakete nur an der Netzgrenze kontrolliert.

Denn die Grundannahmen, auf denen das Konzept der Perimeter-Defense basiert, entsprechen nicht mehr der Realität:

- Sind alle internen Systeme vertrauenswürdig? In Unternehmensnetzen sind verstärkt Geräte im Einsatz, die sich oft außerhalb des Firmengeländes befinden, beispielsweise Laptops und PDAs. Zudem hängt der Vertrauensgrad der Endgeräte von ihrer Konfiguration ab, etwa Patch-Level oder Aktualität der Virensignaturen.

- Gibt es eine klare Grenze zwischen innen und außen? Neben der Aufweichung durch mobile Endgeräte werden Firmennetze zunehmend durch Partneranbindungen oder Wartungsschnittstellen sowie Wireless-Technologien und Virtual Private Networks (VPNs) erweitert.
- Kommen Gefahren in erster Linie von außen? Alle Systeme werden von Menschen bedient, die Fehler machen oder gegen Richtlinien verstoßen. Und dass Würmer wie Blaster oder SQL-Slammer Firmennetze befielen, obwohl die Firewall deren Ports 135 oder 1434 abblockte, zeigt,



**Viele Endgeräte werden heute nicht nur im geborgenen Firmenetz, sondern auch außerhalb benutzt. Dadurch wird die Firewall unterwandert.**

Foto: Pointsec

dass interne Mechanismen wie VPN-Zugänge oder Laptops für die Wurmverbreitung sorgen.

- Kann die Firewall Gefahren erkennen und abwehren? Die meisten Firewalls hinken der Entwicklung von Übertragungsmechanismen hinterher und können mit Instant Messaging, Voice-over-IP oder Webservices nur rudimentär umgehen. Zudem wird der Datenverkehr verstärkt über HTTP abgewickelt oder verschlüsselt, was die Kontrolle erschwert.

Viele solcher Probleme lassen sich durch eine Segmentierung

des Netzes lösen. Die einzelnen Zonen sind dabei physisch voneinander getrennt und pro Zone gelten bestimmte Richtlinien zu Konfiguration und Betrieb der Systeme. Zudem sind die Kommunikationsbeziehungen zwischen den Zonen geregelt; so dass Würmer auf einzelne Segmente beschränkt bleiben.

Der Quarantäne-Ansatz ergänzt die Segmentierung. Dabei wird für jeden Teilnehmer ein Security Level ermittelt. Parameter dafür können installierte Softwareversionen und Patches sowie vorhandene Schutz-Tools

sein. Auf Basis dieser Security Levels segmentieren Router und Switches dann mithilfe von Technologien wie 802.1x das gesamte Netz. Dieses dynamische Modell ist besser als statische Segmentierung zur Abwehr aktueller Bedrohungen geeignet.

Eine Reihe von Herstellern haben den Ansatz bereits aufgegriffen. Einer der Protagonisten ist Cisco mit seiner Network Admission Control (NAC).

Auch Microsoft, die für seine Network Access Protection (NAP) mit Enterasys oder Juniper kooperiert, will seine Strategie mit Ciscos Initiative harmonisieren. Microsoft unterstützt aber derzeit nur Remote-Access- und keine lokalen Clients. Bei Checkpoint wiederum sorgen die Interspect Appliance für die LAN-Segmentierung. Diese werden durch die Integrity Clients ergänzt, die auf Stationen im lokalen Netz wie auch VPN-Clients installiert sein können.

Enno Rey  
Geschäftsführer ERNWlab