



Wien, 21. Februar 2005

Cisco erweitert Self-Defending-Network-Strategie

Neue Produkte und Erweiterungen minimieren Sicherheitsrisiken

Die "Adaptive Threat Defense" (ATD) läutet die nächste Phase von Cisco Systems "Self-Defending Network" ein. Mit den neuen Produkten ist eine bessere Kontrolle des Netzwerkverkehrs, der Endgeräte, der Anwender und Anwendungen möglich. Somit werden die Sicherheitsrisiken in Netzwerken weiter entschärft.

Die Produkte und Lösungen der ATD-Phase minimieren die Sicherheitsrisiken für Netzwerke, indem Bedrohungen auf allen Layern dynamisch adressiert werden. Darüber hinaus senkt ATD die Betriebskosten und vereinfacht die Architektur-Designs. Der innovative Ansatz verbindet Sicherheitsfunktionen, Multilayer-Intelligenz, Anwendungsschutz, netzwerkweite Kontrolle und Reduzierung von Bedrohungen durch Hochleistungslösungen. Adaptive Threat Defense bringt Neuerungen in den Bereichen Anti-X Defenses, Anwendungssicherheit sowie Netzwerk-Kontrolle und –Eindämmung.

Anti-X Defenses

Dabei geht es um die Reaktion und Verhinderung von Bedrohungen für das Netzwerk durch eine Kombination innovativer verkehrs- und inhaltsorientierter Sicherheitsservices. Dazu gehören Firewall, Intrusion-Prevention-Systeme (IPS), Anomaly Detection und Entschärfung von Distributed-Denial-of-Service-Angriffen (DDoS) gekoppelt mit Anwendungsinspektion wie Netzwerk-Anti-Virus, Anti-Spyware und URL Filtering. Diese Konvergenz bringt die Möglichkeit der granularen Untersuchung und Kontrolle des Datenverkehrs an die zentralen Punkte zur Durchsetzung der Netzwerksicherheit, sodass bösartiger Verkehr gestoppt wird, bevor er sich im Netzwerk ausbreiten kann. Die Neuerungen in diesem Bereich sind:

- Cisco Intrusion-Prevention-System (IPS) Version 5.0

Die Lösung bietet hoch genaue und intelligente Inline-IPS-Funktionen, die durch Anti-Virus-, Anti-Spyware- und Wurm-Entschärfungsfunktionen, insbesondere durch Peer-to-Peer- oder Instant-Messaging-Traffic, ergänzt wurden. Daraus resultiert eine verbesserte Bedrohungsabwehr für viele Form-Faktoren wie Appliances, integrierte Switch-/Router-Module und Cisco IOS Software-basierte Lösungen, mit einer Performance von bis zu sieben Gigabit pro Sekunde.

- Cisco Anomaly Guard Module und Cisco Traffic Anomaly Detector Module für die Cisco Catalyst Switches der 6500er und 7600er Serien

Version 4.0 dieser Verhaltens-basierten Lösung zur Eindämmung von Distributed-Denial-of-Services-Angriffen bietet Multi-Gigabit-Schutz kritischer Netzwerkressourcen gegen Day-Zero-DDoS-Attacken als integriertes Switch-Modul.

- Cisco Security Agent (CSA) Version 4.5

Die Software bietet Verhaltens-basierten Schutz vor Malware und Spyware, umfassendes Tracking des Sicherheitsstatus von Objekten und ortsabhängige Durchsetzung von Sicherheitsrichtlinien. Der neue Client ist für alle internationalen Windows-Versionen, Solaris, sowie für Redhat Linux verfügbar und bietet jetzt die vollständige NAC-Unterstützung.

Anwendungssicherheit

Diese Technologien schützen Geschäftsanwendungen durch den Einsatz von Zugangskontrolle auf der Anwendungsebene und die Durchsetzung von Richtlinien für die Anwendungsnutzung, sowie die Kontrolle von Webanwendungen und Transaktionschutz. Zu den Neuerungen in diesem Bereich gehören:

- Secure-Socket-Layer-/Virtual-Private-Network-Services (SSL-VPN) in der Cisco VPN Concentrator Version 4.7

Diese Lösung bietet erweiterten Zugang zu nahezu jeder Anwendung mit zusätzlichem Endgeräte- und Malware-Schutz inklusive Funktionen zur Anwendungsoptimierung mit dem neuen Cisco Security-Desktop. Neu ist ebenfalls die vollständige Unterstützung von Citrix-Umgebungen ohne zusätzlichen SSL-Client.

- Cisco PIX Security Appliance Software Version 7.0

Die neue Version ist die umfangreichste Funktionsergänzung seit der Einführung der PIX Firewall-Lösung. Sie ermöglicht Inspektion und Kontrolle einer Vielzahl von HTTP-, Sprach- und IP-basierten Anwendungen. Darüber hinaus wird mit der neuen Version ein sehr flexibles Framework für Sicherheitsrichtlinien vorgestellt, das eine genaue Kontrolle individueller User-to-Application-Flows bietet.

- Cisco IPS Version 5.0 und Cisco IOS Software Release 12.3(14)T

Die beiden Lösungen bieten Funktionen gegen neue Klassen von Bedrohungen wie Spyware oder Malware im Instant-Messaging und in Voice-over-IP-Umgebungen. Sie verbessern so die Möglichkeit Schäden durch Viren-/Wurm-Angriffe zu reduzieren oder ganz auszuschliessen. Durch benutzerdefinierbare Custom-Signatures lässt sich das neue IPS leicht an neue Bedrohungen anpassen und bietet so umfassenden Schutz.

Netzwerk-Kontrolle und -Eindämmung

Netzwerk-Intelligenz und die Virtualisierung von Sicherheitstechnologien eröffnen die Möglichkeit, hoch entwickelte Auditing- und Korrelationsfunktionen einzusetzen, um jedes vernetzte Element beziehungsweise jeden vernetzten Service wie VoIP durch aktive Management- und Entschärfungsfunktionen zu kontrollieren und zu schützen. Zu den Neuerungen in diesem Bereich zählen:

- Cisco Security Monitoring, Analysis und Response System (CS-MARS) und Security Auditor

Die Lösungen korrelieren netzwerkweit Sicherheitsereignisse und überwachen die Richtlinien für aktiven Umgang mit nicht autorisierten Netzwerk-Zugriffen.

- Virtuelle Firewall-Funktionen für Cisco PIX Software Version 7.0 und Cisco IOS Release 12.3(14)T

Firewall-Virtualisierung erweitert die Kontrolle vernetzter Geschäftsressourcen zu geringeren Betriebskosten.

Das IOS Release 12.3(14)T umfasst zusätzlich eine neue virtuelle IPSecurity-Schnittstelle (IPSec), die einfaches und skalierbares IPSec-VPN-Management ermöglicht, und erweiterte Unterstützung für Sprach- und Video-Anwendungen über VPN (V3PN).

- Unterstützung von Network Admission Control (NAC) im Cisco VPN 3000 Concentrator Version 4.7

Der NAC-Support im Cisco VPN 3000 ermöglicht ab sofort die Kontrolle der Einhaltung von unternehmensweiten Sicherheitsrichtlinien in Remote-Access-Szenarien direkt am VPN-Gateway.

Das Netzwerk verteidigt sich selbst

Die Self-Defending-Network-Strategie von Cisco besteht aus drei Säulen: Secure Connectivity (sichere Konnektivität), Threat Defense System (Bedrohungsabwehr) und Trust and Identity Management (Identitätsmanagement). Die erste Phase der Self-Defending-Network-Einführung konzentrierte sich auf integrierte Sicherheit, indem sie IP- und Sicherheits-Technologien eng miteinander verband. In der nächsten Phase stellte Cisco die Initiative Network Admission Control (NAC) vor. Sie ist der erste branchenweite Ansatz, um die Einhaltung von Sicherheitsrichtlinien unternehmensweit zu prüfen und durchzusetzen. Über 20 Partner nehmen bereits an dem Programm teil, eine aktuelle Liste gibt es im Internet unter www.cisco.com/en/US/partners/pr46/nac/partners.html

Cisco Systems, Inc. (NASDAQ: CSCO), weltweit führender Anbieter von Networking-Lösungen für das Internet, feiert 20 Jahre Engagement bei Technologieinnovationen, Marktführerschaft und sozialer Verantwortung. Weitere Informationen zu Cisco finden Sie unter <http://www.cisco.at>.

Weitere Informationen:

Cisco Systems Austria GmbH, Millennium Tower, Handelskai 94-96, A-1200 Wien, www.cisco.at

Gabriele Kluger, Tel. 01/240 30-6219, Mobile: +43/664/1023376, Fax 01/240 30-6300, gkluger@cisco.com

HOCHEGGER|COM, Angelina Merz, 01/505 47 01-52, Fax 01/505 47 01-9, a.mercz@hochegger.com