Cisco Self-Defending Network noch wirkungsvoller

Integrierte Sicherheit: Neue Releases verbessern adaptive Abwehrfähigkeiten intelligenter Netze; effizienter Schutz durch netzwerkübergreifende Zusammenarbeit

WIEN, 07. Februar – Cisco kündigt heute signifikante neue Funktionen für die Verbesserung der Zusammenarbeit zwischen unterschiedlichen Produkten und Diensten seines Sicherheitsportfolios an. Damit vereinfacht sich für Unternehmen die Kontrolle von Informationssicherheit und die Eingrenzung von Sicherheitsbedrohungen über alle Netzwerke hinweg. Parallel wird der Aufwand für das Sicherheitsmanagement signifikant reduziert und der Schutz der Kommunikation für mobile Nutzer ausgebaut.

Die neuen Sicherheitsfunktionen betreffen: das Cisco Intrusion Prevention System (IPS), den Cisco Security Agent (CSA), das Cisco Security Monitoring Analysis and Response System (CS-MARS), den Cisco Security Manager (CSM) sowie Lösungen für Secure Sockets Layer Virtual Private Network (SSL VPN). In ihrer Summe bilden diese Neuerungen den jüngsten Entwicklungsschritt des Cisco Self-Defending Network (SDN). Cisco SDN integriert unterschiedlichste Lösungen für Endgeräte- und Netzwerksicherheit in eine adaptive und kollaborative Sicherheitsarchitektur, die sich für Unternehmen jeder Größenordnung eignet.

Effektive Bedrohungskontrolle und -eindämmung

Laut Mick Scully, Vice President Produktmanagement Sicherheitsprodukte bei Cisco, verschärft sich die Bedrohungslage immer weiter, insbesondere durch die wirtschaftlichen Motive der Angreifer und die Auswirkungen auf die Produktivität netzwerkbasierter Geschäftsprozesse. 'Threat Control and Containment' (Bedrohungskontrolle und -eindämmung) werde vor diesem Hintergrund mehr und mehr zu einer geschäftlichen Notwendigkeit.

"Je stärker sich Organisationen verzweigen", führt Scully weiter aus, "desto unwirksamer werden traditionelle Netzwerksicherheitskonzepte. Daher sind neue, progressive Ansätze gefragt. Unternehmen dürfen sich nicht länger auf eindimensionale Standalone-Produkte verlassen. Sie müssen stattdessen sämtliche Einzelkomponenten zu einem integrierten Sicherheitssystem zusammenführen. Das schließt alle Netzwerk- und Endgeräte ebenso ein wie zentrale Auswertungs- und Analysetools. Nur ein integriertes System ist in der Lage, seine Schutz- und Abwehrmechanismen jederzeit proaktiv zu justieren, wann und wo immer neue Bedrohungen auftauchen. Kollaborative Sicherheit verbessert die Verfügbarkeit von Netzwerken; der Informationsaustausch wird zuverlässiger und gewinnt an Effizienz."

Netzwerkweit abgestimmter Schutz

Im kombinierten Einsatz bieten die neuen Versionen Cisco IPS 6.0, CSA 5.2, CS-MARS 4.3 und CSM 3.1 jetzt netzwerkweiten Überblick, umfassende Schutzmechanismen, vereinfachtes Sicherheitsrichtlinien-Management und dynamische Reaktion auf Bedrohungen zur Verbesserung der Businesskontinuität. Die aktuellen Releases untermauern Ciscos Ansatz, die Gefahrenabwehr über die gesamte Infrastruktur durchgängig zu koordinieren: Sie stellen erstmals eine vitale Beziehung zwischen dem Netzwerk und all seinen Endpunkten her. Die "Standalone-Natur" individueller Sicherheitsprodukte ist somit überwunden. Alle potenziellen Angriffspunkte lassen sich nun in eng abgestimmter Weise schützen.

Perfektes Zusammenspiel

Ein Beispiel dafür liefert der Informationsaustausch zwischen IPS 6.0 und CSA 5.2, durch den sich die Anzahl von Fehlalarmen reduziert und IPS Appliances in die Lage versetzt werden, Angriffe frühzeitiger zu stoppen und deren Ausbreitung besser zu verhindern. Außerdem erkennt die 6.0-Version von IPS jetzt adaptiv Day-Zero-Anomalien. Durch verhaltensbasierte Analyse werden Wurm- und andere Schädlingsaktivitäten anhand ungewöhnlicher Verkehrsmuster identifiziert. Scanner anderer Hersteller lassen sich nahtlos integrieren, um die Analyse- und Abwehrfähigkeit weiter zu verbessern. Ein anderes Beispiel für adaptiven Netzwerkschutz ist die dynamische Anpassung des "Risk Ratings": Je nach Angriffsrelevanz werden automatisch die zum Betriebssystem des Angriffsziels passenden Ereignis- und Aktionsfilter verwendet.

Der Ansatz der kollaborativen Sicherheit äußert sich überdies in den Erweiterungen des neuen CSA 5.2, zum Beispiel in der verbesserten Unterstützung für Quality of Service (QoS) und drahtlosen Infrastrukturen. So vereinfacht CSA 5.2 die Anwendung von Richtlinien für mobile Endgeräte wie Notebooks. Auf diese Weise lassen sich Ad hoc SSIDs (Service Set Identifiers) limitieren oder bestimmte Verschlüsselungsmethoden durchsetzen sowie sichere VPN-Verbindungen bei Fernzugriffen erzwingen.

Durch die enge Koordination von IPS 6.0 und CSA 5.2 wird CS-MARS 4.3 umfassend über alle Bedrohungen informiert. Alle diesbezüglichen Daten fließen in der CS-MARS Appliance zusammen, um das Netzwerkverhalten zu analysieren und ein präzises Bild der aktuellen Bedrohungssituation zu liefern. Mit CSM 3.1 können auf dieser Basis dann unternehmensweite Sicherheitsrichtlinien sofort angepasst werden. In der Summe ergibt sich eine übergreifende Verteidigungsintelligenz: "Weil alle Systeme und Geräte miteinander "reden", lassen sich Abwehrmaßnahmen Ende zu Ende koordinieren. Risiken und Bedrohungen jeder Art werden somit schneller erkannt - Angriffsversuche von außen ebenso wie anomales Netzverhalten, Schwachstellen oder Richtlinienverletzungen. Kollaborative Intelligenz ermöglicht ein stark vereinfachtes, kosteneffizienteres Sicherheitsmanagement und die Umsetzung von Gegenmaßnahmen auf Echtzeit-Bedrohungen", erläutert Alexis Kahr, Business Development Manager Cisco Austria.

SSL VPN - Cisco ASA macht Fernzugriffe sicherer

Cisco kündigt heute außerdem Erweiterungen der SSL VPN-Software für die Cisco Adaptive Security Appliances (ASA) an. Die Cisco ASA Serie integriert Firewall, IPS, Anti-Malware und VPN in einer kompakten Hardwarelösung. Die neue Version 8.0 der Cisco ASA-Software erweitert die hochskalierbaren VPN-Funktionen um folgende SSL-VPN-Features:

- Clientless VPN mit erweiterten Portalfunktionen um individuelle Nutzeransprüchen gerecht zu werden, zum Beispiel durch personalisierte Bookmarks, Lokalisierungssupport sowie RSS Feeds (Really Simple Syndication - eine Technik zur Integration abonnierter Webinhalte in eigene Seiten).
- Cisco Next-Generation "AnyConnect" VPN Client mit breiter Betriebssystemunterstützung, unter anderem für Microsoft Vista und Windows, Mac OS X sowie Linux.
- Cisco AnyConnect Mobile VPN Client unterstützt Microsoft Windows Mobile 5.0 Pocket PC Edition.
- Optimierter Netzwerkzugang für Voice-over-IP und anderen latenzempfindlichen Verkehr.
- "Smart Tunnels" ermöglichen richtlinienbasierten, applikationsspezifischen Zugriff ohne Administratorenrechte.
- Eingebettete "Certificate Authority" (CA) und andere User-Credential Optionen vereinfachen die Authentifizierung.
- Der Windows-Verzeichnisdienst Active Directory lässt sich jetzt direkt für VPN-Zugriffe nutzen. Der Managementaufwand sinkt, weil VPN-Rechte automatisch aus der Windows-Nutzerverwaltung heraus gewährt werden können.
- Erweiterungen für sogenanntes Posture Assessment (Sicherheitschecks vor Verbindungsaufbau) sorgen für eine effizientere Zuordnung von Nutzerrechten.
- Intuitives Management mit dem Cisco ASA Adaptive Security Device Manager (ASDM) und CSM 3.1

Cisco Lifecycle Security Services

Cisco hat sein Security Service-Portfolio erweitert, um Unternehmen die Nutzung der neuen kollaborativen Sicherheitsfeatures zu erleichtern und deren effizienten Betrieb über den gesamten Lebenszyklus hinweg zu garantieren. Zu den wichtigsten Neuerungen zählen: das Cisco Security Center Portal, der Cisco Security IntelliShield Alert Manager Service und der Cisco IPS Signature Management Service.

Das Cisco Security Center Portal dient als eine zentrale Informationsquelle für alle aktuellen Sicherheitsaktivitäten sowie laufenden Cisco Lösungen und Services. Cisco IPS Signature Subskriptionen bieten hierbei Zugang zur Datenbank des Cisco Security IntelliShield Alert Manager Service, um intelligenter auf IPS-Meldungen zu reagieren. Zusammen mit einem bald verfügbaren Feature, das eine Korrelation herstellt zwischen IPS-Signaturen und IntelliShield Alert-Informationen, verkürzt sich die

Wiederherstellungszeit nach einem möglichen Angriff. Zusätzlich vereinfacht der Cisco IPS Signature Management Service die alltägliche Administration von IPS- Geräten durch beschleunigte Signatur-Updates.

Weitere Informationen:
Cisco Systems Austria GmbH, Millennium Tower, Handelskai 94-96, A-1200 Wien, www.cisco.at
Wolfgang Fasching, Tel. 01/240 30- 6247, Mobile: +43-664-3337631, Fax 01-24030/ 6300, wfaschin@cisco.com
HOCHEGGER|COM, Katrin Scharl, Tel. 01/505 47 01-37, Fax 01/505 47 01-4037, k.scharl@hochegger.com

---

Über Cisco
Cisco (NASDAQ: CSCO), weltweit führender Anbieter von Networking-Lösungen, verändert die Art und Weise wie Menschen miteinander in Kontakt treten, kommunizieren und zusammenarbeiten. Weitere Informationen zu Cisco finden Sie unter http://www.cisco.at. Cisco-Produkte werden in Europa von der Cisco Systems International BV geliefert, eine Tochtergesellschaft im vollständigen Besitz der Cisco Systems, Inc.