Bietet die Cisco Web Security Appliance (WSA) Schutz vor Malware/Spyware?

Inhalt

Frage

Bietet die Cisco Web Security Appliance (WSA) Schutz vor Malware/Spyware?

Die Cisco Web Security Appliance (WSA) bietet branchenweit den umfassendsten Schutz vor Spyware und webbasierter Malware. Dazu gehört alles von Adware (die die meisten Support-Probleme verursacht und erhebliche Netzwerkressourcen beansprucht) bis hin zu schädlichen Bedrohungen wie Trojaner, Browser-Hijacker, Browser-Hilfsobjekte, Phishing, Pharming, System Monitor, Keyloggers, Würmer usw.

Die Cisco Web Security-Lösung zeichnet sich durch folgende Hauptmerkmale aus:

1. Eine integrierte Layer 4 (L4)-Datenverkehrsüberwachung scannt alle Ports mit Leitungsgeschwindigkeit, erkennt und blockiert Malware und Phone-Home-Aktivitäten. Durch die Verfolgung aller 65.535 Netzwerk-Ports stoppt die L4 Traffic Monitor effektiv Malware, die versucht, Port 80 zu umgehen, und verhindert auch nicht autorisierte P2P- und IRC-bezogene Aktivitäten.
2. Proxy-Layer-Verarbeitung: Die Cisco Web Security Appliance umfasst außerdem einen extrem leistungsfähigen Web-Proxy sowie integrierte Funktionen für Zwischenspeicherung und Inhaltsbeschleunigung. Die auf dem proprietären Betriebssystem AsyncOS von Cisco basierende Cisco Web-Proxy-Appliance kann bis zu 100.000 gleichzeitige Verbindungen bis zu 10 Mal mehr unterstützen als herkömmliche UNIX-basierte Proxy-Server. Als Web-Proxy ist eine umfassende Content-Inspektion auf Anwendungsebene möglich - eine wichtige Anforderung, um Genauigkeit bei der Bekämpfung webbasierter Malware sicherzustellen.
3. Die ersten Webreputations-Filter der Branche bieten eine leistungsstarke äußere Verteidigungsschicht. Mit SenderBase® analysieren Cisco Webreputations-Filter über 50 verschiedene Webdatenverkehr- und netzwerkbezogene Parameter, um die Vertrauenswürdigkeit einer URL genau zu bewerten. Anhand fortschrittlicher Sicherheitsmodellierungstechniken werden die einzelnen Parameter einzeln gewichtet und eine Punktzahl auf einer Skala von -10 bis +10 generiert. Vom Administrator konfigurierte Richtlinien werden dynamisch angewendet, basierend auf Reputationswerten.
4. Schnelleres Scannen von Signaturen mithilfe der Dynamic Vectoring & Streaming Engine (DVS Engine). Im Gegensatz zu älteren Architekturlösungen, die auf ICAP und einer Multi-Box-Bereitstellung basieren, um Malware-Scans sicherzustellen, hat die Cisco WSA die DVS Engine für eine integrierte interne Scan-Lösung eingeführt. Diese innovative Plattform verwendet ausgefeilte Verfahren zum Parsen und Vectoring von Objekten sowie Stream-

Scannen und Verdict-Caching, wodurch der Scandurchsatz im Vergleich zu ICAP-basierten Lösungen der ersten Generation um das bis zu 10-fache erhöht wird.

5. Das branchenführende Cisco Anti-Malware-System nutzt die DVS-Engine und mehrere Signaturtypen von Webroot, um erstklassigen Schutz vor einer Vielzahl von webbasierten Bedrohungen zu bieten. Diese Bedrohungen reichen von Adware-, Browser-Hijacker-, Phishing- und Pharming-Angriffen bis hin zu schädlichen Bedrohungen wie Trojanern, Systemmonitoren und Keyloggern. Die WSA bietet die branchenweit größte Malware-Signaturdatenbank am Gateway.