Sichere Web-Appliance - Schutz vor Malware und Spyware

Inhalt

Einleitung

In diesem Dokument werden die umfassenden Malware- und Spyware-Schutzfunktionen der Cisco Secure Web Appliance (SWA) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- SWA-Verwaltung.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Die Cisco SWA bieten einen robusten und umfassenden Gateway-Schutz gegen ein breites Spektrum an Spyware und webbasierter Malware. Sie können damit Bedrohungen wirksam begegnen, die von Adware reichen, die berüchtigt dafür ist, dass sie erhebliche Probleme mit Netzwerkressourcen und Unterstützung verursacht, bis hin zu schwerwiegenderen Bedrohungen wie Trojanern, Browser-Hijackern, Browser-Helper-Objekten, Phishing, Pharming, Systemmonitoren, Keyloggern und Würmern.

Wichtigste Alleinstellungsmerkmale der SWA

Integrierte Layer-4-Datenverkehrsüberwachung (L4TM)

Die L4-Datenverkehrsüberwachung ist in der Lage, alle Netzwerk-Ports (insgesamt 65.535) mit Leitungsgeschwindigkeit zu scannen, um eine umfassende Erkennung und Blockierung von Malware und nicht autorisierten Kommunikationsversuchen sicherzustellen. Diese Funktion vereitelt Malware, die versucht, gängige Ports wie die Ports 80 und 443 zu umgehen, und unterdrückt außerdem unautorisierte Peer-to-Peer (P2P)- und Internet Relay Chat (IRC)-Aktivitäten.

Proxy-Layer-Verarbeitung

Die SWA umfassen einen leistungsstarken Web-Proxy mit integrierten Funktionen für Caching und Content-Beschleunigung. Der Webproxy basiert auf dem proprietären AsyncOS von Cisco und kann bis zu zehnmal mehr Verbindungen verwalten als herkömmliche UNIX-basierte Proxyserver. Als Web-Proxy ermöglicht er eine umfassende Content-Inspektion auf Anwendungsebene, die für einen präzisen Schutz vor webbasierter Malware unerlässlich ist.

Webreputations-Filter

Als branchenführende Web-Reputationsfilter bieten diese eine zusätzliche Verteidigungsebene. Diese Filter verwenden SenderBase®, um über 50 Web-Traffic- und netzwerkbezogene Parameter auszuwerten und die Vertrauenswürdigkeit einer URL zu bestimmen. Anhand fortschrittlicher Sicherheitsmodellierungstechniken werden jedem Parameter individuelle Gewichtungen zugewiesen, die in einem Reputationswert von -10 bis +10 gipfeln. Vom Administrator konfigurierte Richtlinien werden auf Basis dieser Bewertungen dynamisch angepasst.

Dynamische Vectoring- und Streaming-Engine (DVS)

Die DVS-Engine ermöglicht ein schnelles Scannen von Signaturen innerhalb der SWA und unterscheidet sich so von älteren Architekturen, die für das Scannen von Malware auf das Internet Content Adaptation Protocol (ICAP) und mehrere Geräte angewiesen sind. Diese hochmoderne Plattform nutzt ausgefeiltes Objektparsing, Vectoring-Techniken, Stream-Scanning und Verdict-

Caching, wodurch der Scan-Durchsatz im Vergleich zu ICAP-basierten Lösungen der ersten Generation um das Zehnfache gesteigert wird.

Cisco Anti-Malware-System

Dieses System nutzt die DVS-Engine zusammen mit verschiedenen Signaturtypen, die von Webroot stammen, und bietet so unübertroffenen Schutz vor einer Vielzahl von webbasierten Bedrohungen. Das Spektrum der Bedrohungen umfasst Adware, Browser-Hijacker, Phishing, Pharming-Angriffe und bösartigere Systeme wie Trojaner, Systemmonitore und Keylogger. SWA verfügt über die branchenweit größte Datenbank mit Malware-Signaturen am Gateway und bietet so umfassenden Schutz.

Die Cisco Web Security Appliance ist somit führend beim Schutz von Netzwerk-Gateways vor einer Vielzahl von webbasierten Bedrohungen und bietet sowohl zuverlässigen Schutz als auch einen hohen Netzwerkdurchsatz.

Zugehörige Informationen

- Bedienungsanleitung für AsyncOS 15.2 für Cisco Secure Web Appliance

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.