

PRESSEMELDUNG

ZUR SOFORTIGEN VERÖFFENTLICHUNG

Neue Features für mehr Sicherheit im Webverkehr

IronPort S-Serie jetzt mit Multi-Vendor-Signaturerkennung, verbessertem Richtlinien-Management und selektiver HTTPS-Analyse

München, 26. November 2007 – IronPort – Cisco-Geschäftseinheit und ein führender Anbieter von Anti-Spam-, Anti-Viren- und Anti-Spyware-Lösungen – stellt heute neue Features für mehr Sicherheit im Webverkehr vor. Die Appliances der S-Serie schützen Unternehmen vor böartigen Webseiten und Malware – auch wenn es sich um verschlüsselte HTTPS-Verbindungen handelt. Durch das verbesserte Management lassen sich komplexe Sicherheitsrichtlinien nun besonders einfach am Gateway erstellen und umsetzen. Zudem verhindert der Einsatz dieser Lösung, dass sensible Daten unkontrolliert das Unternehmen verlassen. Die S-Serie ist ein wichtiger Teil des Self Defending Networks von Cisco: Sie gewährleistet sowohl auf inhaltlicher als auch auf Netzwerk-Ebene einen sicheren Interneteinsatz.

Reputationsbasiertes Filtern von Webinhalten

Die IronPort Web Security Appliances analysieren zuerst die Reputation eines Webservers, bevor Verbindungen zu den aufgerufenen Webseiten aufgebaut werden. Dazu liefert die weltweite Datenbank SenderBase stets aktuelle Reputationswerte in Echtzeit. Gefährliche Webseiten mit einer schlechten Reputation werden so bereits vor dem Verbindungsaufbau abgewiesen. Diese Technologie bietet einen entscheidenden Sicherheitsaspekt, da Malware im Web äußerst schnell und mannigfaltig variiert und dadurch meist von herkömmlichen, Signatur-basierten Filtern unentdeckt bleibt. Durch reputationsbasierte Verfahren lassen sich hingegen auch polymorphe – also sich ständig verändernde – Malware-Attacken abwehren.

Der Einsatz von Reputation beschränkt sich aber nicht nur auf das Blockieren von Verbindungen. Vielmehr ist die Reputationsanalyse in alle Funktionen der Appliance integriert. Anhand der Reputationsdaten entscheidet das System beispielsweise, ob Inhalte in der Dynamic Vectoring and Streaming (DVS)-Engine einer Multi-Vendor-Signaturerkennung unterzogen werden. Die S-Serie von IronPort bietet ein integriertes Anti-Malware-System mit Signaturen von Webroot und McAfee. Darüber hinaus ist die Appliance auch in der Lage, HTTPS-Datenströme zu untersuchen. Diese umfassende Methodik sorgt für eine deutlich effizientere und intelligentere Analyse der Webinhalte.

"Die Reputationsfilter haben sich als ein mächtiges Werkzeug erwiesen. Wir setzen dieses Verfahren schon seit Jahren für unsere E-Mail-Appliances ein. Mit Erfolg, denn mehr als 90 Prozent des eingehenden Spams werden bereits auf Grund der schlechten Reputation des sendenden Mailserver erkannt. Das gleiche Prinzip nutzen unsere Web-Reputationsfilter", begründet Reiner Baumann, Regional Director für Zentral- und Osteuropa bei IronPort den Einsatz.

URL-Filter zur Durchsetzung der Sicherheitsrichtlinien

Um die Produktivität zu erhöhen und die Haftung zu begrenzen, haben viele Unternehmen inzwischen Richtlinien für den Internet Einsatz am Arbeitsplatz entwickelt. Viele dieser Richtlinien sind mittels eines URL-Filtersystems implementiert. Die S-Serie von IronPort beinhaltet eine URL-Filterlösung mit detaillierten Berichten über typisches Anwenderverhalten beim Websurfen und mehr als 50 unterschiedlichen Webseiten-Kategorien. Der Einsatz des webbasierten Richtlinien-Management-Tools erleichtert die Erstellung und die Umsetzung der LDAP-basierten Benutzerrichtlinien. Der integrierte URL-Filter ist eine effektive Ergänzung zu den IronPort Web-Reputationsfiltern.

Zuverlässiges Erkennen von Botnet-Aktivitäten

"Unsere Analysten stellen derzeit einen verstärkten Trend von E-Mail in Richtung Web als die bevorzugte Methode zur Verbreitung von Malware fest. Dies hat zur Folge, dass Unternehmen mit sehr ausgeklügelten Botnet-Infektionen konfrontiert sind, die an unterschiedlichen Punkten eindringen", erklärt Baumann. Ein spezieller Layer 4 (L4) Traffic Monitor in der S-Serie analysiert den Datenaustausch an allen Ports, um Botnet-Aktivitäten im Netzwerk aufzuspüren und zu blocken.

Gezielte HTTPS-Analyse

Eine Lücke in zahlreichen Web-Security-Lösungen ist die zunehmende Fälschung von HTTPS-Zertifikaten. Der Einsatz von HTTPS im Internet wächst jedoch – dank Online-Banking und Handel – kontinuierlich um über 60 Prozent im Jahr. "Es ist sehr einfach, eine neue Webseite zu erstellen, die der einer lokalen Bank oder eines Unternehmens sehr ähnlich sieht, eine HTTPS-Verbindung aufzubauen und dann dem Anwender Malware zu senden. Da HTTPS eine verschlüsselte Verbindung zwischen dem Client und dem adressierten Server ist, haben Sicherheitslösungen typischerweise keinen Einblick in oder Kontrolle über HTTPS-Traffic", so Baumann.

Die Web Security Appliances von IronPort sind in der Lage, diese Bedrohung zu adressieren. Das DVS-System leitet verdächtige HTTPS-Daten zur integrierten Verschlüsselungslösung. Diese entschlüsselt die Verbindung, prüft die Daten auf Malware und Richtlinienkriterien und sendet sie – falls unbedenklich – wieder verschlüsselt an den Anwender. Private Inhalte mit finanziellen, gesundheitlichen oder Kreditkarten-Informationen sollten besser verschlüsselt bleiben, um Haftungen für das Unternehmen auszuschließen und die Privatsphäre der Anwender zu schützen. Der Einsatz der Reputationsanalyse an dieser Stelle kann jedoch den entscheidenden Schutz vor Sicherheitslücken liefern: Bei Verbindungsaufbau zu verdächtigen und unbekanntem Seiten mit schlechter Reputation empfiehlt es sich, den HTTPS-Verkehr zu entschlüsseln und zu scannen.

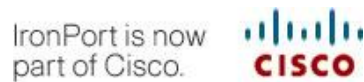
Dieser intelligente Einsatz von Reputation und URL-Kategorisierung erhöht die Sicherheit, Effizienz sowie den Schutz der Privatsphäre jedes Anwenders.

Über IronPort Systems

IronPort Systems ist eine Geschäftseinheit von Cisco und ein führender Anbieter von Lösungen zum Schutz vor Spam, Viren und Spyware. Die Appliances von IronPort wurden für kleine Firmen bis hin zu Global 2000 Unternehmen entwickelt und spielen in der Netzinfrastruktur eines Unternehmens eine geschäftsentscheidende Rolle. Die innovativen Systeme sind einfach zu bedienen und bieten höchste Leistungsfähigkeit. Sie verwenden SenderBase™, die weltweit größte Datenbank zur Beobachtung und Bewertung von E-Mail- und Web-Bedrohungen.

Mehr Informationen über Produkte, Lösungen und Services von IronPort finden Sie unter

<http://www.ironport.de>.



###

Ansprechpartner für die Presse:

Angelika Felsch
Marketing Manager
Central & Eastern Europe
IronPort Systems GmbH

Paul-Wassermann-Str. 3, 81829 München
Tel: +49 89 45 22 27-14
Fax: +49 89 45 22 27-10
E-Mail: afelsch@ironport.com