

PRESSEMELDUNG

ZUR SOFORTIGEN VERÖFFENTLICHUNG

Neue Erweiterung der IronPort Web-Reputationsfilter bietet Schutz vor Botsites und URL-Angriffswellen

München, 1. April 2008 – IronPort Systems, Cisco-Geschäftseinheit und führender Anbieter von Unternehmenslösungen zum Schutz vor Spam, Viren und Spyware, hat seine Web-Reputationsfilter um zwei wesentliche Sicherheitsfeatures erweitert. Zum einen ist die Abwehr von so genannten Botsites – also zur Verbreitung von Malware genutzten Webseiten – verbessert worden. Zum anderen erkennen die Filter nun sehr schnell jene URLs, die zwar zu eigentlich seriösen Anbietern gehören, aber durch Hackerangriffe missbraucht werden (URL-Outbreaks). Beide Neuheiten sind ab sofort in den Lösungen der IronPort S-Serie sowie über das SenderBase®-Netzwerk des Sicherheitsanbieters enthalten.

WWW: Wild Wild Web?

Von den derzeit mehr als zehn Milliarden aktiven Webseiten sind Expertenschätzungen zufolge mittlerweile zwischen zwei und zehn Prozent verseucht. Vor allem die vielfältigen Einfallstore und koordinierten Attacken auf mehreren Kommunikationsprotokollen stellen aktuell die größte Herausforderung dar. Zu den Konsequenzen gehören nicht nur der Verlust von vertraulichen Daten durch Spyware, sondern auch Systemausfälle, verminderte Arbeitsproduktivität und höhere Support-Kosten.

Ein aktuelles Beispiel für die neue Generation von web-basierten Angriffen zeigte sich Anfang März dieses Jahres: Web-User wurden beim Besuch von mehreren hundert legitimen Webseiten automatisch zu Botnetzen weitergeleitet, die Malware verbreiten. Herkömmliche URL-Filter waren in diesem Fall wirkungslos, da die URLs seriösen Anbietern gehörten. Die Web-Reputationsfilter von IronPort untersuchen hingegen, wo die Umleitung hinführt und stoppen die Verbindung zu der verseuchten Seite noch bevor die Malware ins Netzwerk gelangen kann.

Täuschungsmanöver Botsites

Einer der schnellsten Überträger von Malware sind Botsites, also gehackte oder verseuchte Webserver, die Anweisungen von Command-and-control-Netzwerken, so genannten Botnetzen, folgen. Jeder Computer in den Botnetzen erzeugt automatisch weiteren Spam, der einen Link zu der verseuchten Zielseite enthält. Damit verbreitet sich die malware-infizierte Website quasi eigenständig und baut das Netzwerk so immer weiter aus. Schätzungsweise sind heutzutage

sieben Prozent aller Computer mit Internetzugang (etwa 75 bis 100 Millionen PCs) Teil eines solchen Botnetzes.

“Die Intelligenz dieser Botnetze ist erstaunlich”, so Reiner Baumann, Regional Director Central and Eastern Europe bei IronPort Systems. “Ein einziges Botnetz kann Tausende malware-beladener Botsites hervorbringen, die einige Minuten bis zu ein paar Stunden aktiv sein können. Die einzig wirksame Abwehr dagegen liefert ein Web-Reputationsdienst, der die versteckte Gefahr in Echtzeit erkennt und die Seite ausfiltert.”

URL-Ausbrüche ohne Signatur

Verbunden mit der Zunahme an Botsites beobachtete das Threat Operations Center von IronPort in den letzten zwölf Monaten zudem ein 300-prozentiges Wachstum an URLs mit neuer Malware, für die es noch keine Signatur gibt. Diese URLs werden vorrangig über Botsites, URL-Spam, unsichere Web 2.0-Seiten oder bösartige Werbenetzwerke verbreitet. Angesichts der Vielfalt der Angriffsszenarien steigt die Bedeutung der schnellen Erkennung von Botsites und URL-Outbreaks


Lösungen mit herkömmlichen URL-Filtern sind aufgrund ihrer oft manuellen Klassifikationstechniken gegen diese neuen URL-Angriffswellen unwirksam, denn die infizierten Seiten verstecken sich meist hinter unkritischen Kategorien wie Finanzen, Unterhaltung oder News. Die URL Outbreak Detection von IronPort hingegen ist speziell dazu entwickelt worden, um neue URLs ohne Reputation oder Signatur zu erkennen und abzuwehren. Das SenderBase-Netzwerk von IronPort nutzt dafür den Überblick über einen Großteil des weltweiten E-Mail- und Webverkehrs. Analysen in Echtzeit ermöglichen es dem Threat Operations Center von IronPort, frühzeitig Reputationswerte für solche URLs zu veröffentlichen – noch vor den ersten Signaturen der Anti-Malware-Anbieter.

Diese technologischen Neuerungen bieten einen dynamischen Schutz gegen ständig neue Bedrohungen, die auf legitime Webseiten abzielen. Zudem bleibt die Infrastruktur hinter den Malware-Attacken dadurch ständig unter Beobachtung, so dass sich die Schutzfilter jeder Änderung der Angreifer umgehend anpassen können.

Mehr Informationen unter: www.ironport.com/de/products/web_security_appliances.html.

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>.

IronPort is now
part of Cisco. 

###

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