Blue Coat Systems

SSL-Datenverkehr kontrollieren

[10.11.2005] Ein neuer SSL-Proxy der Firma Blue Coat Systems untersucht verschlüsselte Datenströme auf Viren, Spyware, Phishing-Angriffe und gefährliche Anwendungsdaten. Er soll Angriffe unter Verwendung des HTTPS-Protokolls verhindern.

Die Firma Blue Coat Systems präsentiert einen neuen SSL-Proxy für die Security Appliances der Serie ProxySG. Er soll Transparenz schaffen im Datenverkehr zwischen Mitarbeitern und externen IT-Anwendungen, auch wenn dieser per HTTPS verschlüsselt ist. Damit schützen Unternehmen und Behörden ihre Netzwerke vor IT-Gefahren wie Viren, Spyware oder gefährlichen, aktiven Elementen in verschlüsselten Inhalten. Das Aufkommen an verschlüsseltem Datenverkehr steigt mit der zunehmenden Nutzung von Web-Anwendungen. Herkömmliche Sicherheitsprodukte können diesen Web-Datenverkehr meist nicht kontrollieren und lassen so eine Hintertür für Hacker und Cyber-Kriminelle offen. SSL-Datenströme können - weil verschlüsselt - mit gängigen Sicherheitslösungen wie Virenfiltern oder Firewalls nicht auf IT-Gefahren kontrolliert werden; SSL-Daten gelangen über den offenen Port 443 der Firewall also ungefiltert ins Firmennetz. Unternehmen können HTTPS-Datenverkehr nur in Echtzeit überwachen, wenn sie den SSL-verschlüsselten Datenverkehr von und zur genutzten Anwendung terminieren können. Das ist jedoch nur bei firmeneigenen Applikationen und Programmen möglich. Zwar bieten Proxy Appliances von Blue Coat Systems schon länger die Möglichkeit, zumindest eingehende SSL-Verbindungen am Proxy zu terminieren. Mit der neuen Proxy-Option funktioniert das ab sofort auch mit ausgehendem SSL-Datenverkehr. Ab Januar 2006 soll die neue Software lieferbar sein.

(hi)

Stichwörter: IT-Sicherheit, Blue Coat Systems, SSL, IT-Sicherheit, IT-Security,