

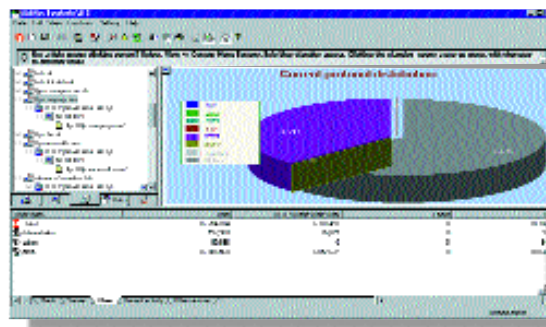
Big Brother im Netzwerk

Der Netzwerkanalysator Session Wall-3 bietet Unternehmen den sicheren Internetzugang und verhindert gleichzeitig die missbräuchliche Nutzung des Mediums.

Von Dirk Pelzer

Für Unternehmen, die ihren Anwendern den Zugriff auf das Internet gestatten, wird es immer wichtiger, nicht nur den Schutz vor externen Angreifern zu gewährleisten. Sie sehen sich inzwischen auch mit dem Problem konfrontiert, dafür sorgen zu müssen, dass die Mitarbeiter nicht dazu verleitet werden, sich Webinhalte anzusehen, die mit ihrer Tätigkeit nichts zu tun haben. Einschlägige Internetseiten mit nackten Tatsachen können dazu ebenso gehören wie die zahllosen Seiten mit Börsenkursen oder anderen Inhalten, die nicht notwendigerweise zum Arbeitsgebiet eines Mitarbeiters zählen.

Session Wall-3 ist ein Produkt, das nicht nur die beiden genannten Aspekte abdeckt, sondern darüber hinaus noch zahlreiche für die Analyse nützliche Netzwerkinformationen sammelt und übersichtlich darstellt. Es wurde von Abirnet entwickelt und gehört inzwischen zu Computer Associates.



Session Wall-3 ermittelt zahlreiche statistische Daten über die Nutzung des Netzwerks und stellt die Informationen übersichtlich dar.

Arbeitsweise von Session Wall-3

Session Wall ist von seiner grundsätzlichen Arbeitsweise her mit einem Netzwerkanalysator vergleichbar, der alle Pakete der Netzwerksegmente analysiert, an welche das System angeschlossen ist. Vereinfacht ausgedrückt könnte man das Tool als passive Firewall bezeichnen, denn Pakete, die zwischen dem Internet und dem Unternehmensnetz ausgetauscht werden, müssen Session Wall nicht passieren.

Um seine Funktion zu erfüllen, benötigt Session Wall lediglich einen Anschluss an ein Netzsegment. Idealerweise ist dies mit dem internen Anschluss der Firewall oder des Routers identisch, über den die Internetverbindung realisiert ist. Falls die Session Wall-Anbindung über einen Switch erfolgt, muss der entsprechende Port im Promiscuous-Mode arbeiten, wie das beispielsweise bei einem Diagnose-Port der Fall ist. Ansonsten kann Session Wall nicht alle Pakete untersuchen, womit die Funktionalität hinfällig wäre.

Zahlreiche Funktionen integriert

Die Aufgabengebiete, die der Netzwerkverwalter mit Session Wall-3 abdecken kann, gliedern sich in die fünf Bereiche Überwachung, Alarmierung, Blockieren von Sessions, Aufspüren von Eindringlingen und Reporting. Session Wall analysiert alle Pakete, die in den angeschlossenen Netzsegmenten ausgetauscht werden und erstellt für jeden Client, Server und Benutzer Statistiken über Art und Anzahl der ausgetauschten Pakete auf der Ebene von HTTP, Telnet, FTP, POP und weiterer gängiger Internetprotokolle. Die gesammelten Daten stehen

in Form von Diagrammen oder als Tabelle zur Verfügung (siehe Abbildung 1).

Für die weitere Auswertung fertigt Session Wall darüber hinaus anhand frei definierbarer Regeln Aufzeichnungen über die ausgetauschten Informationen zwischen internen und externen Rechnern an. So ist der Netzwerkverwalter nicht nur in der Lage zu sehen, wer mit wem kommuniziert hat, sondern kann auch am Bildschirm lesen,

welche Inhalte dabei ausgetauscht wurden, was allerdings datenschutzrechtlich nicht ganz unbedenklich sein dürfte (siehe Abbildung 2).

Regeln entscheiden

Die gesammelten Informationen erlauben nicht nur die Analyse, wer mit wem welche Daten austauscht, sondern ermöglichen die Definition von Regeln und Alarmen, die festlegen, was beim Auftreten einer bestimmten Konstellation geschehen soll. So kann der Administrator beispielsweise eine Regel definieren, die allen internen Systemen den Zugriff auf eine bestimmte Website verbietet. Session Wall-3 verfügt in der Basiskonfiguration bereits über zahlreiche vorkonfigurierte Regeln, die den Start erleichtern.

Das Tool kategorisiert die Regeln in verschiedene Themenbereiche, etwa solche zum Entdecken von Angreifern. Ebenso sind Regeln zum Aufspüren von E-Mail-Viren, gefährlichen Applets und ActiveX-Controls sowie verdächtigen Netzwerkaktivitäten wie Port-Scanning oder IP-Spoofing integriert. Da sich die Zahl der bekannten Viren und Angriffsarten permanent vergrößert, bietet Computer Associates seinen Kunden einen regelmäßig aktualisierten Abonnement-Service.

Unerwünschtes blockieren

Ist einmal festgelegt, auf welche Ereignisse reagiert werden soll, muss der Administrator nur noch über die von Session Wall durchzuführenden Aktionen entscheiden. Auch hier bietet das Produkt wieder umfangreiche Möglichkeiten. So steht es dem Administrator frei, eine Session zu blockieren, Nachrichten per Mail,

Shortcut

Executive Summary

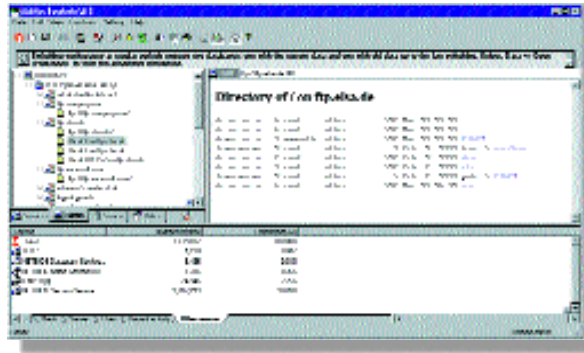
Session Wall-3 ist ein komplementäres Produkt zu herkömmlichen Firewall-Systemen. Es erlaubt dem Netzwerkverwalter, ein- und ausgehenden Netzwerkverkehr zu überwachen, Informationen zu sammeln, Verbindungen zu blockieren und Alarme beim Entdecken von bestimmten Ereignissen wie etwa einem Ping-Flooding-Angriff auszulösen.

Resources

Produkt: Session Wall-3
Preis: ab ca. 3000 Mark (1534 Euro)
Hersteller: Computer Associates
Anbieter: Help GmbH
Tel: +49 (0) 60 51/97 49-0
www.cai.com

Der Autor

Dipl.-Ing. Dirk Pelzer ist freiberuflicher Consultant und Journalist. Er beschäftigt sich unter anderem mit Hochverfügbarkeitslösungen für Windows NT, Storage Area Networks und dem Thin-Client/Server-Computing.



Session Wall-3 kann nicht nur feststellen, wer mit wem kommuniziert, sondern sogar die übermittelten Inhalte aufzeichnen und dem Administrator anzeigen.

Fax oder SNMP zu senden oder einen Eintrag in das NT Eventlog zu schreiben oder ein Programm zu starten. Um eine Session zu blockieren, sendet das Tool einfach ein TCP RST-Signal und beendet damit eine Verbindung.

Um auch Schutz vor internen Störfrieden zu gewährleisten, die ihre Rechner als Spielkonsolen missbrauchen und das Unternehmensnetz als Spielwiese betrachten, kann der Netzwerkverwalter darüber hinaus Netzwerkspiele wie zum Beispiel Doom oder Quake blockieren.

Reporting schafft Überblick

Für eine angemessene Darstellung der von Session Wall-3 gesammelten Daten sorgen die umfangreichen in das Tool integrierten Reportingmechanismen. Auch hier gibt es zahlreiche vordefinierte und -konfigurierte Berichte. Sie reichen von den zehn aktivsten Rechnern über die am häufigsten besuchten Websites bis hin zum Auflisten aller möglichen Ereignisse, aufgeschlüsselt nach Client, Benutzer oder Server.

Wünscht der Administrator eine regelmäßige Dokumentation bestimmter Ereignisse, kann er zudem die Reporterstellung zeitgesteuert ausführen und die Ergebnisse in unterschiedlichen Formaten, etwa als kommaseparierte Text-, Excel- oder HTML-Datei abspeichern.

Session Wall im Test

Um Session Wall auf den Zahn zu fühlen, wurde das Produkt in einem Testnetzwerk auf einem NT 4.0-Server installiert. Der Internetzugriff erfolgte über einen Proxy-Server, der sich im selben LAN-Segment wie der Session Wall-Rechner befand. Ohne dass überhaupt eine Konfiguration stattfinden musste, machte sich Session Wall sofort nach einem Neustart des NT-Servers daran, alle möglichen Informationen über das Netzwerk sowie die darin befindlichen Arbeitssta-

tionen zu sammeln und übersichtlich darzustellen.

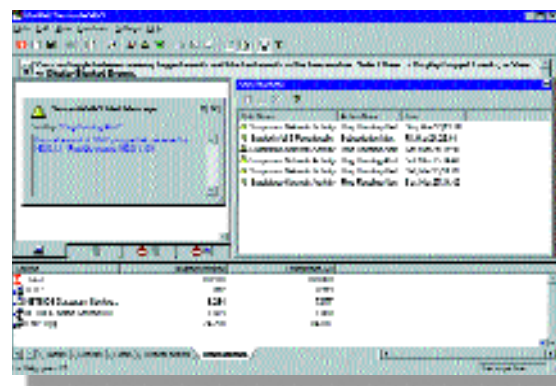
Einen Ping-Flooding-Angriff, der durch das Kommando `ping servername -t` simuliert wurde, erkannte Session Wall ebenso auf Anhieb, wie einen nachgestellten Denial-of-Service-Angriff auf den RAS-Dienst des Proxy-Servers (siehe Abbildung 3). Auch die Protokollierung des Netzwerkverkehrs zwischen internen Clients und Internet-Web-

Servern funktionierte problemlos.

Mit nur wenigen Handgriffen war es möglich, Regeln aufzustellen, die den Zugriff eines bestimmten Clients auf einen angegebenen Web-Server unterbanden, während andere Clients weiterhin ohne Schwierigkeiten darauf zugreifen konnten. Die Reporting-Qualitäten von Session Wall waren ebenfalls einwandfrei.

Fazit

Session Wall-3 kann hinsichtlich Funktionalität und Bedienbarkeit voll überzeugen. Durch zahlreiche vorkonfigurierte Regeln und Alarme erhält der Netzwerkverwalter ein System, mit dem er sofort loslegen kann. Aufbauend auf den Erkenntnissen und Resultaten, die ihm das Tool liefert, lassen sich eigene Richtlinien und Aktivitäten implementieren, um so das Unternehmensnetz effektiv zu schützen. Beinahe beängstigend ist schon die Vielfalt und der Detaillierungsgrad der Informationen, die Session Wall-3 zum Vorschein bringt. So wäre es beispielsweise problemlos möglich, den gesamten E-Mail-Verkehr auf dem Netzwerk zu filtern und herauszufinden, ob ein Mitarbeiter vielleicht Kontakt zu einem Konkurrenzunternehmen hat. Das geht sogar so weit, dass beim Auffinden bestimmter Schlüsselwörter ein Alarm ausgelöst wird. Big Brother lässt grüßen. ■



Session Wall-3 erkennt verdächtige Ereignisse und alarmiert automatisch den Administrator, etwa beim Auftreten einer ungewöhnlich großen Anzahl von Ping-Kommandos, die an ein System geschickt werden.