PROTECTSTAR

AWARD 2004

Computer Security

CHECK POINT - SAFE@OFFICE

Firewall Appliance

PROTECTSTAR
secure your business

Einleitung

Die Safe@Office-Serie von Check Point Software Technologies bietet kleinen und mittleren Unternehmen mit bis zu 100 Arbeitsplätzen lückenlosen Schutz mit geprüfter Technologie, die 100% der Top 100 Unternehmen weltweit absichert.

Die Geräte schützen vor Hackern und reduzieren die Ausfallzeit des Netzwerks, sodass sich Unternehmen auf ihr Kerngeschäft konzentrieren können.

Mit den optionalen Services wie Web-Filtering, Anti-Virenscanner, Dynamic-DNS und Dynamic VPN sind die Safe@Office Lösungen mit der Stateful Inspection Technologie für weit mehr als nur für die sichere Anbindung von Filialen und Außenstellen an Unternehmensnetze geeignet.

Die Serie ist in vier verschiedenen Gerätetypen (Safe@Office 105, 110, 225 und 225U) erhältlich.

Sicherheit

Heutzutage sind die meisten Firewalls lediglich zur Vermeidung von Angriffen auf der Netzwerkebene geeignet. Aus diesem Grund nutzen Hacker immer häufiger Schwachstellen auf der Applikationsebene, um beispielsweise Trojaner in Unternehmensnetzwerke einzuschleusen. Die Sicherheitslösungen von Check Point sind die einzigen, die sowohl auf der Netzwerk- (Layer 3) als auch auf der Applikationsebene (Layer 7) effektiven Schutz bieten können.

In unseren Testreihen haben wir die Safe@Office Appliances mit der Software-Version 4.5.50s detailliert unter die Lupe genommen und können den Geräten eine ausgezeichnete Schutzwirkung bestätigen. Die Geräte haben an den Tagen unseres Testverfahrens alle zum Zeitpunkt bekannten 4686 verschiedenen Angriffs- und Sicherheitstest erfolgreich abgewehrt.

In diesen Testreihen wurden beispielsweise verschiedene Arten von Portscans, über zweihundert Arten von Denial of Service Angriffen, alle bekannten Schwachstellen von Firewalls und Betriebssystemen, sowie Sicherheitslücken in bestimmten Anwendungen, unter realen Bedingungen getestet.
In den drei verschiedenen Sicherheitseinstellungen der Appliances wurden keine offenen Ports gefunden, die für externe Angreifer nutzbar sein könnten. Die beiden Schutzfunktionen „IP-Spoof-Schutz“ und „TCP-Flag-Validierung“, die in der Safe@Office-Serie standardmäßig integriert sind, funktionierten in unseren Tests tadellos.

Der IP-Spoof-Schutz blockierte zuverlässig alle Nicht-Broadcast- und Multicast-Pakete, die an dem WAN-Port der Appliance eingehen und deren Quell-IP-Adresse einem internen Teilnetz entsprach. Die TCP-Flag-Validierung schützt vor ungültigen TCP-Flag-Kombinationen, die beispielsweise von Port-Zuweisung-Tools, wie NMAP benutzt werden. TCP-Flag wird benutzt, um Firewalls in Netzwerken zu erkennen oder die in einer Firewall eingerichteten Sicherheitsrichtlinie zuzuordnen.

Unseren fünfstündigen Dauer-Penetrationstest haben die Geräte ebenfalls erfolgreich absolviert. Eine weitere Schutzfunktion bietet die passwortgeschützte Web-Konfigurationskonsole, die nur autorisierten Personen Zutritt verschafft. Der Zugang zur Konsole kann wahlweise über den Port 80 (HTTP), sowie über den verschlüsselten Port 443 (HTTPS) aufgerufen werden. Die Zugangsmöglichkeit über HTTPS bietet guten Schutz vor Netzwerksniffern, die sich in einem internen Netzwerk befinden, um das Konfigurationskennwort der Safe@Office Appliance auszuspionieren. Das Standardregelwerk der Stateful Packet Inspection Firewall blockiert alle Verbindungsversuche aus dem Internet und lässt jede Verbindung von dem internen Netzwerk in das Internet zu. Mit den drei Sicherheitsstufen LOW, MEDIUM und HIGH kann das Regelwerk der Firewall vom Anwender selbst weiter eingeschränkt werden. In der Sicherheitsstufe „LOW“ wird jegliche Verbindung von dem internen Netzwerk zum Internet erlaubt. Alle aus dem Internet stammenden Verbindungen werden blockiert. Einzige Ausnahme sind ICMP Pakete - so genannte Pings.

In der „MEDIUM“ Sicherheitsstufe werden alle Verbindungen vom internen Netzwerk zum Internet erlaubt. Mit Ausnahme den Windows Datei Freigaben (NTB Ports 137, 138, 139 und 445). Es werden alle aus dem Internet stammenden Verbindungen blockiert. Die „HIGH“ Sicherheitsstufe ist die höchste und restriktivste Stufe. Bis auf einige Ausnahmen wird jede Verbindung aus dem internen Netzwerk zum Internet unterbunden. Lediglich die Verbindungen für Standard Internet Anwendungen werden zugelassen. Dazu zählen der Zugriff auf Webseiten (HTTP, HTTPS), E-Mail (IMAP, POP3, SMTP), FTP, NNTP, Telnet, DNS, IKE, Port 2746/UDP und Port 256/TCP.

Alle Verbindungen aus dem Internet auf das interne Netzwerk werden von der Firewall blockiert. Auch wenn solche „Schieberegler“ bei Firewalls unter Experten nicht beliebt sind, so muss hier eine Ausnahme gemacht werden, da die unterschiedlichen Sicherheitslevels sehr an die Bedürfnisse von Unternehmen angepasst sind. Alle Safe@Office Appliances unterstützen die Verschlüsselungsverfahren AES (Advanced Encryption Standard), 3DES (Triple Data Encryption Standard) und DES als auch die Algorithmen SHA1 und MD5. Die automatische Update-Funktion sorgt für einen lückenlosen Schutz gegen neue Bedrohungen und sich schnell verbreitende Attacken. Pünktlich alle zwei Stunden sucht eine Safe@Office automatisch

nach möglichen verfügbaren Updates. Es ist aber auch möglich, bei Bekannt werden von neuen Threads entsprechende Patches zum optimierten Schutz vom Managed Service Provider sofort eingespielt zu bekommen.

Benutzerfreundlichkeit

Die Installation einer Safe@Office ist anwenderfreundlich und der Installationswizard hilft dem Anwender das Gerät in einfachen Schritten zu konfigurieren. Das Web-Interface ist optisch ansprechend und übersichtlich gehalten, so dass alle Funktionen und Einstellungen leicht vorgenommen werden können.

Bei der Installation und Konfiguration dürfte es im Regelfall keinerlei Komplikationen geben. Sollten sich dennoch Schwierigkeiten ergeben, so helfen das mitgelieferte zweihundertfünfzigseitige Handbuch und die Schnellanleitung, die alle relevanten Schritte und Fragen sehr detailliert und anschaulich beantworten. Zusätzlich stehen dem Benutzer jederzeit auf der linken Seite des Web-Interfaces durch anklicken des „Help"-Button eine praktische Online-Hilfe zur Verfügung. Hier sollte jedoch nachgebessert werden, da sich die Hilfe zum Teil auf vergangene Software-Versionen bezieht oder keine Hilfestellungen zu vorhandenen bzw. neuen Einstellungsmöglichkeiten bieten.

Auf der Rückseite der Safe@Office 200er-Serie sind, im Gegensatz zu den 100er Baureihen, ein zusätzlicher DMZ (De-Militarized-Zone) Port angebracht, der es Unternehmen erlaubt, einen öffentlichen Server, wie beispielsweise einen Webserver, ohne zusätzlichen Switch anzuschließen und gleichzeitig durch die Stateful Packet Inspection Firewall des Gerätes schützen zu lassen. Bei der Safe@Office 110 kann manuell eine logische DMZ eingerichtet werden. Zusätzliche Hubs oder Switches können an den Safe@Office Appliances problemlos angeschlossenen werden. Hier ist zu beachten, dass bei der Serie 100 gekreuzte Netzwerkkabel verwendet werden müssen. Die 200er Serie erkennt automatisch die angeschlossenen Gerätetypen.

Die zusätzlichen Funktionen wie Gateway High Availibility, Backup ISP, Dial Backup VLAN-Unterstützung und Static NAT sind für Unternehmen nützliche Werkzeuge, die in den Safe@Office Appliances 225 und 225U standardmäßig integriert sind.

Optisch besonders hervorgehoben ist unter dem Menüpunkt „Reports" -> „Active Computers" die grafische Darstellung für die an der Safe@Office angeschlossenen Computersysteme (einschließlich Computername & MAC-Adresse). Zudem erfährt der Anwender unter diesem Menüpunkt, welche IP-Adresse die entsprechende Workstation oder Server hat und ob diese IP-Adresse statisch oder via DHCP an das jeweilige System vergeben wurde.

Die Log-Dateien sind ausreichend und können bei Abschluss eines entsprechenden Servicevertrages zusätzlich in Form eines übersichtlichen und graphisch aufbereiteten Reports bereitgestellt werden. Anwendern können unter „Reports" -> „Event Log" auf eine farbige Tabelle zurückgreifen, auf der rot untermalte Einträge einen erfolgreich abgewehrten Angriff und blau untermalte Einträge einer Änderung in der Konfiguration der

Safe@Office kennzeichnen. Aus den Einträgen kann der Benutzer erfahren, dass ein Angriff getätigt worden ist und wann der Angriff (über das Protokoll TCP oder UDP) getätigt und welcher Computer/Server auf welchem Port angegriffen wurde. Durch einen Mausklick auf die IP-Adresse des Angreifers öffnet sich ein WHOIS-Fenster, in dem der Benutzer mehr Informationen über den Angreifer bzw. dessen Provider erhalten kann. Mit einem möglichen Reporting-Servicevertrag werden den Safe@Office Benutzern jedoch über eine zentrale Service Management Plattform (SMP) ein monatliches Reporting in grafischer Auswertung zugesendet, dass keine Wünsche mehr offen lässt. Der optional erhältliche und kostenpflichtige eMail Anti-Virenscanner kommt aus dem Hause Trend Micro oder eAlladdin, je nach Betreiber des Dienstes.

Auf Anwenderwunsch kann er in ein- und/oder ausgehenden (SMTP/POP3) E-Mails nach Viren und Trojanern suchen. Der Virenscanner funktionierte hervorragend und erkannte alle Testviren und Trojaner, die wir per E-Mail verschickten oder erhalten haben. Sobald der Anwender beispielsweise eine E-Mail mit einer virenverseuchten Anlage erhält, entfernt der Anti-Virenscanner zuverlässig diese Datei und fügt in der ursprünglich eMail-Nachricht, statt der verseuchten Anlage eine Textdatei namens „InterScan_SafeStamp.txt" ein, in der die entsprechende Warnung über den Virenfund dokumentiert wird.

Ebenfalls zuverlässig verrichtete das Web-Filtering seine Arbeit. Der URL Web-Filter kommt von SurfControl und kann optional durch einen entsprechenden Servicevertrag erworben werden. Über die Konfigurationskonsole des Gerätes kann man dann den Filter wahlweise ein- oder ausschalten, sowie den Zugriff auf bestimmte Kategorien erlauben und blockieren. Der Benutzer kann zwischen den Kategorien „Violence", „Drugs & Alcohol", „Adult", „Criminal Skill", „Gambling", „Hate Speech" und „Unknown Sites" auswählen. Unter die Kategorie „Adult" fällt zum Beispiel die Webseite von Playboy und alle anderen bekannten Webseiten, die keine jugendfreien und anstößigen Inhalte besitzen. Gerade für größere Unternehmen ist die Kategorie „Unknown Sites" wertvoll. Hier wird unter anderem der Zugriff auf die Suchmaschine Google und auf das Online-Auktionshaus Ebay blockiert. Dies kann verhindern, dass Angestellte während der regulären Arbeitszeit diese Dienste verwenden.

Hier haben wir die Option vermisst, das Web-Filtering zu bestimmten Uhrzeiten ein- oder auszuschalten, so dass beispielsweise der Zugriff auf Ebay während der täglichen Mittagspause eines Unternehmens erlaubt und zu allen anderen Zeiten blockiert werden kann.

Performance

Die Safe@Office Geräte arbeiteten bei unseren Testreihen schnell und zuverlässig. Wir konnten keine Leistungseinbußen oder Mängel bei der Performance in irgendeiner Art und Weise feststellen. Selbst während unseres fünfstündigen Dauer-Penetrationstest konnte mit den Safe@Office Appliances weiterhin unter kleinen Leistungseinbußen gearbeitet werden.

Von der Safe@Office-Serie sind zwei Baureihen erhältlich. Die 100er Serie für Small- und Home Offices unterstützt dabei mit den Modellen 105 und 110 den sicheren Internetzugriff von 5/10 Usern bei gleichzeitigen Durchsatzraten von 22 MBit/s bzw. 3 MBit/s mit VPN-Unterstützung.

Auf noch mehr Performance ist die 200er Serie ausgelegt. 25 gleichzeitige Internetverbindungen managt die Safe@Office 225 Appliance bei einer Datendurchsatzrate von 80 MBit/s. Darüber hinaus können zehn VPN-Tunnel aufgebaut werden. Unternehmen, deren Anforderungen diese Werte übertreffen, bietet Check Point mit der Safe@Office 225U noch höhere Performance für eine unbegrenzte Anzahl an Benutzern (unlimited User). Die große 200er-Appliance hat keine Begrenzung der simultanen Internetzugriffe und kann darüber hinaus bei Datendurchsätzen von 150 MBit/s (30 MBit/s bei VPN) und 25 VPN-Tunnel aufbauen. Die maximale Anzahl der gleichzeitigen Verbindungen bewegt sich zwischen 2000 (Safe@Office 105 und 110) und 8000 (Safe@Office 225 und 225U).

Support

Mit dem Erwerb einer Safe@Office Appliance erhalten Anwender ein Jahr lang Garantie und Softwareupdates inklusive. Unter http://www.checkpoint.com/techsupport hat der Anwender von Produkten aus dem Hause Check Point, Zugriff auf eine umfangreiche Wissensdatenbank (Knowledgebase) und die am häufigsten gestellten Fragen (FAQ). Interessenten können die Appliances nicht direkt bei Check Point, sondern bei einem autorisierten Reseller erwerben. Dieser ist dann für den Support und die gesetzlichen Gewährleistungen zuständig und erneuert auf Wunsch hin auch den Supportvertrag.
Zusammen mit dem Kauf einer Safe@Office können dann auch optional die verschiedenen Services, wie Web-Filtering, Dynamic-DNS und eMail Anti-Virenscanner erworben werden. Einige Händler bieten individuelle Dienstleistungen oder vollständige Service-Komplettpakete an, die speziell auf die Bedürfnisse der Anwender zugeschnitten werden können.

Preis / Leistung

Die Preisspannen der Safe@Office-Serie bewegen sich zwischen 299,00 Euro und 1.799,00 Euro. Aufgrund der nahtlosen Schutzwirkung, der Vielzahl an Sicherheitsfunktionen und den nahezu unbegrenzten Einsatzmöglichkeiten, sind die Safe@Office Appliances, vor allem auch im Verhältnis zu anderen Hardware-Firewalls auf dem IT-Sicherheitsmarkt, preiswert.

Die Safe@Office 105 und 110 können wir mit einem Preis von 299,00 Euro bzw. 599,00 Euro nicht nur kleineren Unternehmen oder Zweigstellen, sondern auch Privatanwendern empfehlen, die Computersysteme im Heimnetzwerk absichern möchten. Die Preise für die verschiedenen Services, wie Antiviren-Scanner, Web-Filtering, Dynamic-DNS, Dynamic-VPN, usw. sind je nach Händler unterschiedlich. Einige rechnen nach der Anzahl der an der Safe@Office angeschlossenen Benutzer und andere bieten günstige Komplettpakete einschließlich einer Safe@Office Appliance an.

In der Regel bewegen sich die Preise (abhängig vom Safe@Office Modell) für die optionalen Services zwischen 145,00 Euro und 1.400 Euro pro Jahr, und sind im Vergleich zu separaten Softwareprodukten, günstig und zugleich empfehlenswert.

Fazit

Unser Fazit für die Safe@Office-Serie lässt sich in einem Satz zusammenfassen:
Es ist gibt für jeden, egal ob großes oder kleines Unternehmen, Zweigstelle oder Privatanwender eine passende Safe@Office Appliance, die durch die optionalen Serviceleistungen individuell an die jeweiligen Anforderungen angepasst werden kann.

Die Geräte verbinden umfassende Sicherheit mit einem zuverlässigen Internet-Gateway in einer kostengünstigen Lösung. Hier sind vor allem die minutenschnelle Installation, die leicht einzurichtenden Sicherheitsregeln mit Hilfe von Konfigurationsassistenten (One-Click-Technologie), sowie der Schutz auf der Netzwerk- (Layer 3) und auf der Applikationsebene (Layer 7), besonders erwähnenswert. Darüber hinaus eignen sich diese Appliances hervorragend als Lösung zur sicheren Anbindung von Kommunikation mit Außendienstmitarbeitern, Teleworkern und weiteren Niederlassungen des Unternehmens.

Die einzigartige Kombination aus Hardware, Software, den genannten Services, sowie dem lückenlosen Sicherheitskonzept, machen die Safe@Office Appliances aus dem Hause Check Point zu einer „State of the Art" Firewallösung auf dem IT-Sicherheitsmarkt.

Den optionalen Erwerb der Services wie Web-Filtering, eMail Anti-Virenscanner und Dynamic-DNS können wir Anwendern und zukünftigen Benutzern nur wärmstens empfehlen. Übrigens wird es noch in diesem Jahr als weiteren zusätzlichen Service einen SPAM-Filter geben, der das vorhandene Sicherheitskonzept abrunden wird.

Die gesamte Safe@Office-Serie von Check Point erhält aufgrund der ausgezeichneten Testergebnisse und der Vielzahl an individuellen Einsatzmöglichkeiten den ProtectStar-AWARD für das Jahr 2004.

ProtectStar

secure your business

www.ProtectStar.com

Impressum:

ProtectStar

secure your business

ProtectStar Inc.
Testcenter

Postfach 10 25 08
D-86015 Augusburg
Germany

www.protectstar.com
testcenter@protectstar.com

Gestaltung und Konzeption:

wo-pro werbung

wo-pro werbung -agentur für
klassische und neue medien
Wettringer Str. 32
D-74585 Kleinansbach

Fon: 07958 92 57 14
Fax: 07958 92 68 98
E-Mail: info@wo-pro.de
Web: www.wo-pro.de