PROTECTSTAR

AWARD 2004

Computer Security

SYMANTEC SGS 320
Firewall Appliance

Die Sicherheitsappliance enthält eine Stateful Inspection Firewall, sichere IPsec-kompatible VPN-Verbindungen, Intrusion Detection und Prevention, statisches Content Filtering und Funktionen zur Richtliniendurchsetzung für über Symantec verbundene Virenschutz-Clients.

Die SGS 320 Appliance von Symantec erhält aufgrund der sehr guten Testergebnisse und den vielseitigen Schutzfunktionen den ProtectStar-AWARD für das Jahr 2004.

PROTECTSTAR
secure your business

Einleitung

Netzwerke in kleineren Unternehmen stellen hohe Anforderungen an die Sicherheit. Jedoch verfügen diese Unternehmen nur selten über die erforderlichen Ressourcen, die für den Betrieb kostenintensiver Lösungen mit hohem Verwaltungsaufwand erforderlich sind.

Aus diesen Gründen bietet Symantec mit den Modellen der Symantec Gateway Security 300 Serie ideale Firewall-Appliances für kleine Unternehmen an. Die Geräte verbinden umfassende Sicherheit mit einem zuverlässigen Internet-Gateway und einer sicheren Wireless-LAN-Option in einer einzigen kostengünstigen Lösung.

Die Serie ist in drei verschiedenen Ausführungen (SGS 320, 360, 360R) erhältlich.

Die Sicherheitsappliances enthalten eine Stateful Inspection Firewall, sichere IPsec-kompatible VPN-Verbindungen, Intrusion Detection und Prevention System, statisches Content Filtering und Funktionen zur Richtliniendurchsetzung für über Symantec verbundene Virenschutz-Clients.

Sicherheit

In unseren Testreihen haben wir das kleinste Modell, den SGS 320 und zusätzlichem Wireless LAN Access Point detailliert und die Lupe genommen und können dem Security Allrounder eine ausgezeichnete Schutzwirkung bestätigen, der einen umfassenden und sicheren Schutz für kleine Unternehmen bietet.

Zunächst fanden unsere Experten eine mögliche Sicherheitslücke, da das Gerät den ICMP-Leak-Test nicht bestanden hat. Nach genauer Überprüfung stellte sich jedoch heraus, daß es sich um einen klassischen „False Positiv" handelte und keinerlei Auswirkungen auf die Sicherheitsfunktionen der Appliance hat.

Der SGS 320 hat an den Tagen unseres Testverfahrens alle zum Zeitpunkt bekannten 3719 verschiedenen Angriffs- und Sicherheitstest erfolgreich abgewehrt. Wir konnten in den verschiedenen Standardeinstellungen der Appliance auch keine offenen Ports finden, die für einen externen Angreifer nutzbar sein könnten. Unseren vierstündigen Dauer-Penetrationstest hat das Gerät ebenfalls erfolgreich absolviert.

Die beiden Schutzfunktionen „IP-Spoof-Schutz" und „TCP-Flag-Validierung", die in der SGS Appliance der 300er Serie standardmäßig integriert sind, funktionierten in unseren Testreihen 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.

Ebenfalls gut verrichtete das IDS (Intrusion Detection System) bzw. das IPS (Intrusion Protection System) seine Aufgabe. Die IDS- und IPS-Funktionen schützten unser Test-Netzwerk vor Fragmentierungsangriffen, IP-Optionsangriffen, Pufferüberlaufangriffen und Port-Scans. Die vorhandenen IDS/IDP-Signaturen (Ping of Death, Overdrop, Back Orifice, Bonk, Jolt, usw.) bieten für kleine Unternehmen ausreichenden Schutz. Dennoch könnten unserer Meinung nach diese Signaturen nachhaltig erweitert und ergänzt werden, so dass ein nahtloser Schutz garantiert werden kann. Immerhin existieren in den Enterprise Modellen Symantec Gateway Security Appliances der 5000er Serie zehnmal mehr solcher Signaturen, als in den 300er Modellen.

Einen echten, in dem Gerät integrierten, Virenscanner gibt es in diesem Sinne nicht. Die SGS 300er Serie unterstützt lediglich Mithilfe von AVpe, die AntiVirus-Konfigurationen unterstützter und verbundener Symantec Richtlinien. So ist AVpe in zwei Umgebungen einsetzbar: In einem Netzwerk mit einem internen Symantec AntiVirus Corporate Edition Server, der Virenschutzinformationen verwaltet, oder in einem Netzwerk mit nicht verwalteten Clients.

Praktisch hier ist die Möglichkeit, den Status aller Symantec-Virenschutzlösungen auf den Arbeitsplatzrechnern abzufragen und – wenn erforderlich – Aktualisierungen auszuführen sowie alle sendenden Stationen auf das Vorhandensein eines Virenschutzes überprüfen zu lassen.

Über die LiveUpdate-Funktion wird die Appliance-Software automatisch auf dem neuesten Stand gehalten. Dies sorgt für einen lückenlosen Schutz gegen neue Bedrohungen und sich schnell verbreitende Attacken. Je nach Bedarf, kann der Anwender Mithilfe eines „Planers" die Aktualisierungsfunktionen so einstellen, daß das Gerät von alleine zum Beispiel jeden Tag, einmal in der Woche, 14-tägig oder einmal im Monat zu einer bestimmten Uhrzeit auf dem entsprechenden Symantec-Server nach möglichen verfügbaren Firmware-Updates sucht.

Eine weitere Schutzfunktion bietet die passwortgeschützte Web-Konsole, die nur autorisierten Personen Zugang verschafft. Der Zugang zur Konsole kann über den Port 80 (HTTP) aufgerufen werden. Leider existiert kein Zugriff auf die Konsole über den verschlüsselten Port 443 (HTTPS). Dadurch besteht die Gefahr, daß das Passwort der Konfigurationskonsole über den http-Port durch Netzwerksniffer ausgespäht werden könnte.

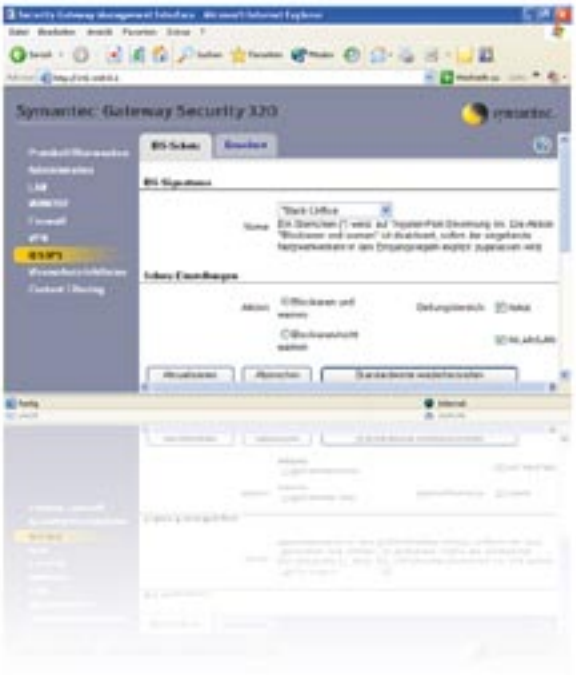
Die SGS Appliances der 300er Serie unterstützen drei Arten von VPN-Tunnels: Gateway-to-Gateway, Client-to-Gateway und Wireless- Client-to-Gateway. Allerdings ist keine VPN-Tunnel-Komprimierung möglich.

Die Log-Datei lassen etwas zu wünschen übrig, denn aus ihnen kann der Anwender lediglich erfahren, dass ein Angriff stattgefunden hat. Was für ein Angriff genau getätigt wurde, bleibt fraglich. Dem Anwender ist nur ersichtlich, wann der Angriff (über das Protokoll TCP oder UDP) getätigt wurde und welcher Computer/Server auf welchem Port angegriffen wurde.

Benutzerfreundlichkeit

Die Installation der SGS 320 ist anwenderfreundlich und der Installationsassistent hilft dem Anwender das Gerät in wenigen Schritten zu konfigurieren. Das Gerät erfordert nur geringe technische Kenntnisse bei Installation und Betrieb. Das Web-Konfigurationsinterface ist optisch ansprechend und übersichtlich gehalten, so dass alle Funktionen und Einstellungen leicht vorgenommen werden können.

Bei der Installation und Konfiguration des Gerätes dürfte es keine Schwierigkeiten oder Probleme geben. Unerfahrenen Anwendern helfen der mitgelieferte, knapp zweihundertfünfzigseitige, „AdminGuide“, der sich als PDF-Datei auf einer dem Gerät beiliegenden CD-Rom befindet und die Schnellanleitung, die alle nötigen Schritte und Fragen des Benutzers detailliert und anschaulich beantwortet.



Besonders gut hat uns der Help-Button im Konfigurationsmenü der SGS 320 gefallen. Er ist durch ein klar ersichtliches Fragezeichen gekennzeichnet und öffnet durch anklicken eine praktische und hilfreiche Online-Hilfe zu den jeweiligen Einstellungsmöglichkeiten.

Das manuelle Hinzufügen von Firewall-Regeln (Eingangs- und Ausgangsregeln) wird zum Beispiel mit Hilfe einem verständlichen Auswahlmenü vollzogen. Alle Eingaben können bequem per Mausklick vorgenommen werden.

Für alle Modelle der Symantec Gateway Security 300 Serie ist ein Zusatzmodul erhältlich, womit die Appliances auch als Wireless LAN Access Point fungieren können. Dafür sorgt eine spezielle Wireless-Firmware und ein CardBus-Steckplatz für ein optionales Add-on, das aus einem integrierten 802.11-Funkmodul (es unterstützt die WLAN-Standards 802.11g und 802.11b) samt Antenne besteht und die größtmögliche Sicherheit in WLANs mit Clients gewährleistet, auf denen die Client VPN-Software von Symantec installiert ist.

Sehr gut funktionierte auch der in der Appliance integrierte Content Filter, mit dessen Hilfe der Anwender bestimmte Webseiten manuell blockieren oder freigeben kann.
Das statische Content Filtering wird über Computer-Gruppen und VPN-Gruppen verwaltet. Computer-Gruppen sind im Firewall-Abschnitt definierte Gruppen, für die dieselben Regeln gelten.
Wenn der Benutzer eine Computer-Gruppe definiert, gibt er an, ob diese Gruppe für das Content Filtering Listen vom Typ „Ablehnen“ oder „Zulassen“ verwendet.

So können beispielsweise „Black Lists“ und „White Lists“ erstellt werden, auf die die einzelnen Clients bzw. Computer-Gruppen zugreifen bzw. nicht zugreifen dürfen.
Alle Listen vom Typ „Ablehnen“ (Black Lists) aufgeführten Webseiten werden dann zuverlässig blockiert.
Zweite Option ist eine Liste vom Typ „Zulassen“ (White Lists) zu erstellen. Nur diejenigen Seiten, die dann in dieser Liste aufgeführt sind, können aufgerufen werden. Der Zugriff auf alle anderen Sites wird dann automatisch blockiert.

Ein weiteres Plus in Sachen Benutzerfreundlichkeit sind die mitgelieferten Steckleisten-Adapter, die für alle Länder dieser Welt kompatibel sind.

Leider haben die Geräte der SGS 300er Serie keinen zusätzlichen DMZ (De-Militarized-Zone) Port angebracht, daß Unternehmen erlauben würde, öffentliche Server wie Web-, Mail- und FTP-Server, ohne zusätzlichen Switch anzuschließen und gleichzeitig durch die Stateful Packet Inspection Firewall zu schützen.

Performance

Das Gerät arbeitete bei allen unseren Testreihen schnell und zuverlässig.
Wir konnten keine Leistungseinbußen oder Mängel bei der Performance in irgendeiner Art und Weise feststellen.
Selbst bei unserem vierstündigen Dauer-Penetrationstest konnte problemlos, unter wenigen Einschränkungen, mit der SGS 320 gearbeitet werden.

Die Stateful Inspection Firewall kann Durchsatzraten von 55 MBit/s verarbeiten. Die VPN-Funktionen arbeiten im verschlüsselten Modus (3DES) mit einer Durchsatzrate von 10 MBit/s.

Zudem unterstützt die SGS 320 Appliance bis zu 10.000 gleichzeitige Verbindungen.

Support

Zusammen mit dem Gerät erhalten Kunden 90 Tage lang telefonischen Support, sowie Gerätegarantie und LiveUpdate für die Appliance-Software für zwölf Monate.

Gegen Aufpreis sind bei Symantec die Support-Pakete: „Silver Support“, „Gold Support“ und „Platinum Support“ erhältlich. Diese Supportprogramme ermöglichen beispielsweise eine unbegrenzte Anzahl

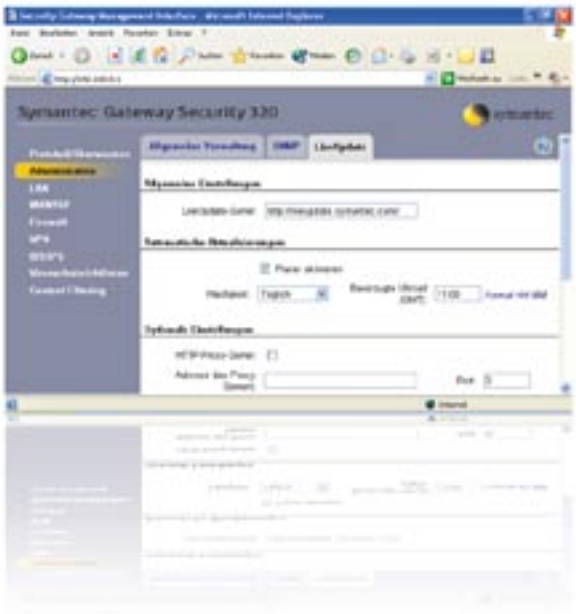
von Anrufen für Installationsunterstützung in den ersten 90 Tagen während der normalen Geschäftszeiten bzw. eine telefonische Unterstützung rund um die Uhr (24x7) und ein Jahr Verlängerung der Garantie, sowie erweiterten Austauschvereinbarung für Ersatzlieferungen.

Preis-Leistung

In Anbetracht individueller Anforderungen in Sachen Preis/Leistung bietet Symantec die Gateway Security 300 Serie in drei verschiedenen Ausführungen (320, 360 und 360R) an.

Mit einem Preis von 499,00 Euro (netto) ist die SGS 320 Appliance aufgrund ihrer Schutzwirkung, dem enthaltenen Content-Filtering, der Vielzahl an Funktionen und flexiblen Einsatzmöglichkeiten, preiswert. Die beiden größeren Appliances SGS 360 und SGS 360R sind ab 699,00 bzw. 899,00 Euro erhältlich. Sie besitzen aufgrund der zwei vorhandenen WAN-Ports die Möglichkeit, jederzeit auf eine Einwahlverbindung zurückzugreifen, auch wenn eine Breitbandverbindung gestört ist. Zudem kann die Bandbreite der vorhandenen WAN-Ports gebündelt werden, so daß effektiv die doppelte Bandbreite für ein- und ausgehende Verbindungen zur Verfügung steht.

Nicht günstig ist unserer Meinung nach das Zusatzmodul für die Nutzung des WLAN Access Point. Es ist mit einem Preis von 199,00 Euro relativ hoch, auch wenn es die WLAN-Standards 802.11g und 802.11b unterstützt



Fazit

Die Symantec Gateway Security Appliances der 300er Serie sind ausgezeichnete Lösungen für kleine Unternehmen, die neben hohem Internet-Verkehr einen sicheren und anwenderfreundlichen Datentransfer zwischen externen Niederlassungen und Außendienstmitarbeitern und der Firmenzentrale per VPN bewältigen müssen. Zudem sind die Geräte bestens für Einzelplatzumgebungen oder als Erweiterung zu SGS Appliances der 5400er Serie in Umgebungen mit einem Hub geeignet. Besonders erwähnenswert sind die einfache Handhabung und Bedienung, die nur geringe technische Kenntnisse bei Installation, Wartung und Betrieb erfordern.

Die schnell einzurichtenden Sicherheitsregeln und die effektiven Schutzfunktionen, wie Intrusion Detection und Prevention System, statisches Content Filtering, IPsec-basiertes VPN mit Hardware-seitiger Verschlüsselung und die Möglichkeit, den Status aller Symantec-Virenschutzlösungen auf den Arbeitsplatzrechnern abzufragen, sowie die praktische Erweiterung mit einem WLAN Access Point, machen die SGS der 300er Serie zu einem ausgezeichneten Security-Allrounder für kleine Unternehmen, die ihre Netzwerke ohne großen Verwaltungsaufwand sicher gestalten möchten.

Einen Punktabzug erhält die SGS 320 aufgrund des fehlenden verschlüsselten Zugriffs über den Port 443 (http) auf die Web-Konfigurationskonsole, da hierdurch die Möglichkeit bestehen könnte, die Zugangsdaten der Web-Konsole durch Netzwerksniffer auszuspähen.

Die SGS 320 Appliance von Symantec erhält aufgrund der sehr guten Testergebnisse und den vielseitigen Schutzfunktionen den ProtectStar-AWARD für das Jahr 2004.

„ We´re testing for your security“

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

wo-pro werbung

Gestaltung und Konzeption:
wo-pro werbung
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