

TESTBERICHT
-
INNOMINATE
MGUARD GATEWAY

ProtectStar hat die Sicherheitslösung „mGuard Gateway“ der Firma Innominate auf Herz & Nieren getestet. Das Gerät zeigte sehr gute Ergebnisse bei unseren Testreihen.



Einleitung

Die Miniatur Firewall / VPN Appliance „mGuard Gateway“ von Innominate bietet trotz ihrer kompakten Maße (20x56x95 mm) einen ausgezeichneten Schutz für kleinere und mittlere Netzwerke als auch einzelne Computer. Sie kann problemlos in ein bestehendes Netzwerk integriert werden oder dient dazu, interne Netzwerke zusätzlich zu sichern.

Neben der integrierten Stateful Inspection Firewall bietet diese Appliance die Möglichkeiten eines VPN Gateways, aufbauend auf dem IPsec Standard. Dabei kann der Benutzer mit 3DES oder mit AES verschlüsseln. Der integrierte Hardwareverschlüsselungschip garantiert eine hervorragende Performance von bis zu 35 MBit (3DES) VPN Durchsatz. Außerdem hat man durch den Stealth Modus die Möglichkeit, transparente VPN Tunnel zu legen.

mGuard Gateway ist eine zuverlässige und wirtschaftliche Sicherheitslösung, welche individuell an die Sicherheitsanforderungen kleiner sowie mittelständischer Unternehmen angepasst werden kann.

Sicherheit

Die Schutzwirkung von mGuard Gateway ist ausgezeichnet. Man kann sowohl einen einzigen Computer oder Notebook, als auch ganze SOHO Netzwerke mit einem DSL-Internetzugang vollständig abschirmen. Hier ist vor allem der so genannte „Stealth Modus“ des Gerätes zu nennen, welcher mGuard Gateway vollkommen unsichtbar macht.

Das Gerät wehrt erfolgreich alle gängigen und bekannten Angriffe aus dem Internet ab. Dabei hilft die leistungsstarke Stateful Inspection Firewall mit einer Durchsatzrate von bis zu 100 Mbps. Sie untersucht Datenpakete anhand der Ursprungs- und Zieladresse und blockiert unerwünschten Datenverkehr.

Wir konnten bei unseren Testreihen keine Sicherheitslücken oder offene Ports finden, welche für einen externen Angreifer nutzbar sein könnten.

Die Konfigurationskonsole wird zudem über das Protokoll https verschlüsselt und bietet somit einen zusätzlichen Schutz gegen eine Ausspähung des Passworts durch mögliche Sniffer im internen Netzwerk.

Eine tolle und einmalige Innovation des mGuard ist die Möglichkeit, über den Stealth Modus einen transparenten VPN Tunnel aufzubauen. Die Verschlüsselung des VPN-Tunnels bietet mit 3DES (168 Bit) oder AES (256 Bit) einen starken Schutz vor Datenschnüfflern. Da das mGuard so klein und mobil ist eignet es sich hervorragend um z.B. auch vom Hotelzimmer oder Seminarraum über VPN auf das Firmennetzwerk zuzugreifen.

Jedoch vermissten wir bei der Konfiguration die Möglichkeit, sich eine Warnung oder Informationen auf dem Bildschirm anzeigen zu lassen, sobald ein Angriff gegen den Benutzer ausgeübt wird.

„Installieren und vergessen“ ist eine feine Sache, jedoch meinen wir, dass man wenigstens optional die Möglichkeit haben sollte, sich Portscans oder andere Attacken anzeigen zu lassen.

Selbstverständlich lassen sich bei der Appliance auch Firewall-Regeln an die Bedürfnisse des Anwenders oder eines bestehenden Netzwerks anpassen. Da es sich bei mGuard Gateway um eine Stateful Packet Inspection Firewall handelt und die aktiven Verbindungsdaten in einer Datenbank erfasst (connection tracking) werden, müssen die Regeln nur in eine Richtung definiert werden, da die Daten aus der anderen Richtung dann automatisch durchgelassen werden. So kommen nur Anfragen ins Netzwerk, für die von innen her auch eine Anforderung besteht.

Mit dem jetzigen Softwarestand kann das Gerät selbst noch keine Viren in den Protokollen SMTP, POP und HTTP erkennen. Momentan wird an der Entwicklung eines Kaspersky Virenschanners für den mGUard gearbeitet, welcher die genannten drei Protokolle nach gefährlichen Viren und Trojanern durchsuchen wird. Dieser wird voraussichtlich bis zum Q3/2004 erhältlich sein.

Benutzerfreundlichkeit

Die Installation von mGuard Gateway gestaltet sich zunächst ein wenig untypisch und für einen Laien möglicherweise etwas kompliziert. Zwar sind die notwendigen Ethernetkabel schnell mit dem Gerät verbunden, jedoch haben wir in unserem Test nicht sofort eine Verbindung mit dem Gerät herstellen können.

Der Grund hierfür ist, dass sich mGuard Gateway in der Standardeinstellung im so genannten „Stealth Mode“ befindet. So mussten wir erst in der MS-DOS-Eingabeaufforderung den Befehl **„arp -s 192.168.1.1 aa-aa-aa-aa-aa-aa“** eingeben. Erst jetzt konnten wir über die Netzwerk-Schnittstelle auf den mGuard unter der Adresse **„https://1.1.1.1“** (Stealth Modus) bzw. **„https://198.168.1.1“** (in Router- oder PPPoE-Modus) zugreifen.

Anschließend sind eventuell kleine, zusätzliche Änderungen in der Netzwerkumgebung von Windows/Linux/Mac vorzunehmen, sofern das Gerät als Router, VPN- oder DHCP Server eingesetzt werden soll.

Wenn man mGuard jedoch in eine bereits bestehende Verbindung einschleifen möchte, entfällt diese genannte ARP-Eingabe, denn sie ist nur nötig, wenn keine Verbindung besteht.

Das wirklich einmalige an dem „Stealth Mode“ ist die Möglichkeit VPN Tunnel transparent aufbauen zu können.

Die Konfiguration erfolgt über eine übersichtliche und verständliche Weboberfläche, die mittels des Browser aufgerufen wird. Natürlich kann auch diese Einstellung wieder individuell an ein bereits vorhandenes Netzwerk angepasst werden.

Über diese Weboberfläche können problemlos die unterschiedlichen Einstellungen von VPN, DHCP Server, das Einstellen von Verbindungsdaten (PPPoE, statische oder dynamische IP Adresse), etc. eingegeben werden. Die Menüführung ist in deutscher Sprache.

Eine weitere Besonderheit an mGuard ist, dass der Anwender das Gerät individuell an seine Bedürfnisse anpassen kann, denn Sie können die Mini-Appliance sowohl an einen einzigen Computer anschließen oder mit einem Hub, Switch oder auch Router kombinieren. Es wird einfach zwischen xDSL Modem und Hub, Netzwerk oder Router geschaltet und kann sowohl von Windows- als auch von Linux- und Mac-Anwendern genutzt werden.

Da mGuard Gateway auch NAT-T beherrscht, kann es auch über einen separaten Router via Modem und ISDN genutzt werden. Außerdem kann man mit dem Gerät VPN Tunnel zwischen dynamischen IP Adressen aufbauen.

Sehr gut hat uns auch die USB Steckleiste gefallen, welche gerade für mobile Anwender mit Notebook praktisch ist, da mGuard Gateway dadurch keine Steckdose mehr benötigt, sondern den nötigen Strom über die USB-Schnittstelle des Computers/Notebooks erhält.

Für erfahrene Anwender dürfte es bei der Installation und Konfiguration von mGuard Gateway keinerlei Schwierigkeiten geben. Unerfahrenen Anwendern helfen der kleine zweiseitige „Quick Installation Guide“ und das mitgelieferte Handbuch, welches sich nur in digitaler Form als PDF-Datei auf einer CD-Rom befindet. Es beantwortet alle relevanten Schritte und Fragen des Anwenders anschaulich und ausreichend.

Praktisch ist auch die Möglichkeit zur Fernkonfiguration. Dabei kann mGuard Gateway über seine gesicherte webbasierte Administratorfläche von einem entfernten Rechner aus konfiguriert werden. Zusätzlich besteht die Option das Gerät nicht nur über den Browser via HTTPS, sondern auch über die Kommandozeilen-Eingabe über das Protokoll SSH zu konfigurieren.

Performance

Trotz des Miniaturformates von mGuard Gateway arbeitete das Gerät bei unseren Testreihen äußerst schnell und zuverlässig und wir konnten keine Leistungseinbußen oder Mängel feststellen. Es zeigte auch sehr gute Leistungen bezüglich der Performance, als wir mit mehreren Computern gleichzeitig und permanent Filesharing betrieben haben.

Die in mGuard Gateway integrierte CPU (Intel IXP 42x mit mind. 266MHz), die 32 MB SDRam Hauptspeicher, der 16 MB große Flash-Speicher, sowie die VPN Durchsatzrate von 35 MBits (3DES) und eine Firewall-Durchsatzrate von 100 MBits sind für diese Miniatur-Appliance hervorragend und suchen auf dem IT-Sicherheitsmarkt ihresgleichen.

Wem diese Performance immer noch nicht ausreichen sollte, so bietet Innominate eine größere 533MHz Variante des mGuard Gateway an, welche sogar VPN Durchsatzraten von 70 MBits (3DES) beherrscht.

Support

Mit dem Erwerb des Gerätes erhält der Kunde alle verfügbaren Updates und Patches für mGuard über die Webseiten von Innominate.

Besonders gut hat uns der Support via Telefon (der Servicezeitraum des Telefonsupports ist Montag bis Freitag von 09:00 bis 17:00 Uhr).

gefallen. Ein freundlicher und kompetenter Mitarbeiter kennt die speziellen Probleme der Anwender und kann deshalb sofort Hilfestellungen geben.

Im Durchschnitt bekamen wir für unsere Problemmeldung bei dem telefonischen Support innerhalb von zwei Minuten eine Lösung für unser Problem.

Außerdem besteht noch die Möglichkeit Problemmeldungen auf elektronischem Weg rund um die Uhr an den Support von Innominate zu senden. Das Unternehmen Innominate bietet eine garantierte Antwortzeit binnen 24 Stunden.

Preis / Leistung

mGuard Gateway kostet € 499,00 (netto). Wir finden den Preis angesichts des sehr kompakten Formates, der hohen Datendurchsatzraten, der vielseitigen Einsatzmöglichkeiten und der enthaltenen 10 VPN-Tunnel für absolut gerechtfertigt.

Als abgespeckte Version bietet Innominate den „mGuard professional“ auch bereits für € 399,00 (netto) an, allerdings dann mit nur 2 VPN Tunnel und ohne VPN Serverfunktionalität für L2TP (Microsoft VPN).

Fazit

Das mGuard Gateway hat den **ProtectStar-AWARD** nur ganz knapp verfehlt.

Hervorzuheben sind die sehr kleine Bauweise, die außerordentliche Schutzwirkung gegen Angriffe aus dem Internet, die Leistungsfähigkeit, die Verwendungsmöglichkeiten, der Support und auch die flinken und motivierten Mitarbeiter bei Innominate.

Ein klares Plus ist auch die optionale Stromversorgung über USB, welche gerade für mobile Anwender bestens geeignet ist.

Eine etwas benutzerfreundlichere Installation (wenn keine Verbindung besteht!) könnte unserer Ansicht nach schnell durch das Abschalten des „Stealth Mode“ in der Standardeinstellung von mGuard Gateway erreicht werden.

Was uns allerdings noch gefehlt hat waren zum einen die Option sich Angriffe zum Beispiel über Logdateien anzeigen zu lassen und zum anderen die (noch) fehlende Virenerkennung.

Laut Hersteller soll zum Sommer eine neue Softwareversion auf den Markt kommen, welches Logdateien und eine Virenerkennung für die Protokolle HTTP, SMTP und POP dann mit einschließen soll.

Des Weiteren werden in der neuen Software Version noch Neuerungen wie ein VPN Tunnel Mode im „Stealth Mode“ enthalten sein, es werden individuelle Einstellungen für jeden einzelnen VPN Tunnel möglich sein, sowie die Unterstützung von UDP syslog und SNMPv3.

Kunden mit der jetzigen Version können das neue Software-Update dann kostenlos downloaden.

Auch bietet Innominate für den mGuard ein kostenloses SDK für professionelle Anwender an, welche damit eigene mGuard Applikationen entwickeln können. Ebenfalls ist eine Änderung des Corporate Designs möglich.

Wir sind jedenfalls sehr neugierig wie die neue Software in den mGuard-Modellreihen in unseren Tests abschneiden wird.