

# Bodyguard für einen Rechner

Nach dem Konzept der „Device-attached Security“ bietet Innominate die Sicherheitsgeräte der Mguard-Reihe für den Schutz einzelner Rechner an. Durch die Anordnung direkt vor der Netzwerkschnittstelle werden auch Angriffe aus dem eigenen Netz abgewehrt, außerdem kann das Gerät in Gegenrichtung unerlaubte Zugriffe auf die benachbarten Netzkomponenten unterbinden.

Das Produkt Mguard gibt es in mehreren Bauformen, darunter Mguard Smart zum Einschleifen in das Netzkabel, Mguard industrial für die Hutschienmontage in Schaltkästen, Mguard Blade-pack für den Rack-Einbau und Mguard Delta als 4-Fach-Switch.

LANline testete die Produktversion „Mguard PCI Professional“ für den Einbau in einen PC. Das Produkt hatte den Firmwarestand 3.1.0. Als halbhohe Einsteckkarte für den PCI-Bus ist der Mguard PCI nicht viel größer als gängige Ethernet-Karten, obwohl er einen vollständigen Rechnerkern enthält. Auf der 266-MHz-CPU mit 64 MByte Speicher läuft ein komplettes Linux-System und erledigt zunächst die Aufgaben von Router und Firewall. Zu den Router-Diensten gehören DHCP (Client und Server), DNS-Caching und NAT ebenso wie die Aktualisierung eines dynamischen DNS. Dank NTP-Synchronisation ist die Uhrzeit für Meldungen und Logfiles stets präzise, und über PPPoE lässt sich zum Beispiel ein DSL-Internetzugang direkt anknüpfen.

## Volle Netzwerkgeschwindigkeit

Die Firewall arbeitet mit voller Netzwerkgeschwindigkeit und unterstützt dank Zustandsverfolgung auch FTP-Verbindungen im aktiven und passiven Modus. Eine SYN- und Ping-Begrenzung schützt bei Flood-Attacken.

In den „Enterprise“-Versionen arbeitet die Karte zudem als VPN-Router und erspart so auf dem Wirtsrechner Konfigurationsaufwand und Sicherheitsmaßnahmen. Der dafür angegebene Durchsatz von 35 MBit/s und die Maximalzahl von 10 VPN-Tunneln dürfte in vielen Fällen ausreichen. Für höhere Anforderungen gibt es noch die „Enterprise XL“-Version, die mit 533 MHz Prozessortakt einen Durchsatz von 70 MBit/s erreicht und bis zu 250 VPN-Tunnel unterstützt.

Auch als Virenschutz kann Mguard PCI tätig werden, sofern der Nutzer eine optionale Lizenz für den Kaspersky-Virenfilter erwirbt. Datenübertragungen mit den Protokollen HTTP, POP3 und SMTP werden dann zwischengespeichert und auf Viren-

signaturen geprüft, wobei gängige Archivformate wie ZIP oder RAR selbsttätig ausgepackt werden. Da das Mguard-Rechner-system keine Festplatte enthält, muss dies allerdings im Hauptspeicher geschehen. Dabei können umfangreiche Archive die Begrenzungen des Speichers überschreiten und werden dann – je nach Konfiguration – entweder ungeprüft durchgereicht oder pauschal zurückgewiesen.

Mit zwei Netzwerkanschlüssen und der Verbindung zum PCI-Bus lässt sich die Mguard-Einsteckkarte auf unterschiedliche Weise betreiben. Entweder verhält sie sich auf dem Bus wie eine normale Netzwerkkarte und wird über mitgelieferte Treiber in das Windows-2000-, Windows-XP- oder Linux-Betriebssystem des Computers eingebunden, oder sie nutzt im Power-over-PCI-Modus den PCI-Steckplatz nur zur Stromversorgung und überträgt die Daten über ein außen anzuschließendes Patch-Kabel an eine bereits vorhandene Ethernet-Buchse.

## Betrieb im Stealth-Modus oder als Router

Bei beiden Anschlussarten kann die Karte entweder im „Stealth“-Modus oder als Router konfiguriert werden. Im ersten Fall wird die IP-Adresse des PCs unverändert nach außen weitergereicht, und der Mguard nimmt unsichtbar seine Schutz-aufgaben wahr, ohne dass die anderen Netzkomponenten umkonfiguriert werden

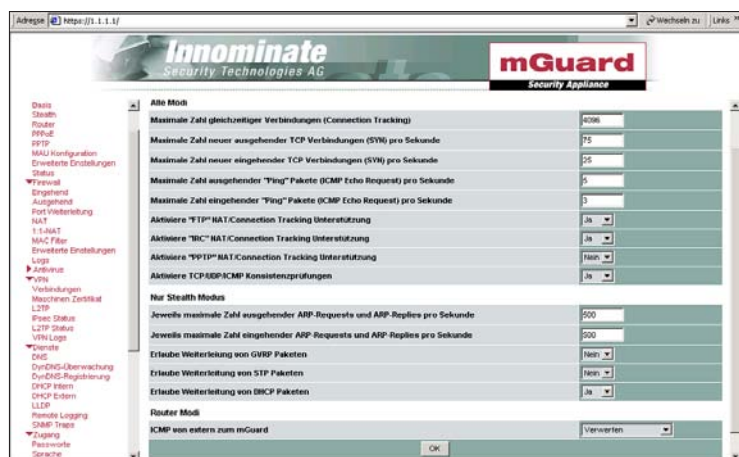


Mguard beim Start: Zugang per Webbrowser

müssen. Im Router-Betrieb bilden PC und Mguard dagegen ein separates Subnetz, in dem der Mguard als Gateway nach außen fungiert.

Für unseren Test wählten wir den „Power-over-PCI“-Modus und nutzten einen schon

laden und wiederherstellen. Sollte einmal das Administrationspasswort in Vergessenheit geraten oder durch fehlerhafte Einstellungen der Zugriff auf die Administrationsseiten verloren gehen, so lassen sich Stealth-Mode und Default-Adresse durch



Konfigurationsseite für die Firewall-Funktionen

etwas betagten Rechner als Baugruppen-träger und Stromspender. Dessen Funktion blieb nach dem Einbau der Karte erwartungsgemäß unverändert. Obwohl der Mguard PCI ab Werk im Stealth-Modus arbeitet und somit keine passende IP-Adresse hat, galt es nun, das Gerät per Browser auf der Adresse <https://1.1.1.1/> anzusprechen und zu konfigurieren. Das gelingt nur – wie in der Dokumentation ausführlich erläutert – mit einem Griff in die Trickkiste: Auf dem zur Konfiguration verwendeten Rechner wird per Eingabeaufforderung und ARP-Befehl die IP-Adresse des Gateways mit einer fiktiven MAC-Adresse verknüpft, daraufhin ist dann das Mguard-System im eigenen Subnetz erreichbar. So funktionierte es auch bei unserem Test, und nach dem Wegklicken der Warnungen zum HTTPS-Zertifikat und der Eingabe des Standardpasswords erschien die sauber gestaltete und klar gegliederte Konfigurationsseite. Hier sind die vielfältigen Einstellmöglichkeiten über zahlreiche Untermenüs erreichbar. Änderungen an den Einstellungen werden sofort umgesetzt, und selbst ein Neustart ist in 30 Sekunden erledigt, ohne dass eine erneute Anmeldung erforderlich wird.

Die aktuelle Einstellung lässt sich als Konfigurationsprofil sowohl im Gerät selbst ablegen als auch über den Browser herunter-

eine Recovery-Taste wiederherstellen. Über die Weboberfläche werden auch Versions-Updates eingespielt, die Innominat für registrierte Nutzer auf seiner Website bereithält – eine lange Versionsliste zeugt dort von der laufenden Produktpflege. Zudem wird noch die Möglichkeit geboten, die Firmware vollständig neu in das Gerät zu laden.

### Paketfilterung nach MAC-Adresse und Protokoll

Die jüngsten Updates enthalten einige Erweiterungen für den Stealth-Mode, beispielsweise ist nun die Paketfilterung nach MAC-Adresse und Protokoll möglich, mehrere Clients werden unterstützt, und auch die IP-Adresse für den Administratorzugang im Stealth-Mode ist nun änderbar. In Verbindung mit der optionalen Administrationssoftware „Innominat Security Configuration Manager“ lässt sich jetzt die Suche nach den korrekten Firewall-Einstellungen automatisieren, im „Autolearning Mode“ beobachtet das System den Datenverkehr und generiert dann selbst die dazu passenden Sicherheitsregeln.

Die Konfigurationsformulare der Web-oberfläche sind sinnvoll aufgeteilt und gut beschrieben. Angesichts der Fülle von Parametern und Einstellmöglichkeiten emp-

fehlt sich zudem das genaue Studium der PDF-Dokumentation, die viele wichtige Hinweise gibt. So wird beispielsweise bei der Verwendung als Router der Zugang zum Internet erst nach dem Einstellen der NAT-Funktion möglich.

In unseren LANline-Tests führte der Mguard PCI – richtige Einstellungen vorausgesetzt – seine vielfältigen Funktionen korrekt aus. Fehler bei den Konfigurationseinstellungen sind allerdings nicht immer leicht zu finden, eine Testfunktion für die WAN-Verbindung innerhalb der Administrationsoberfläche (zum Beispiel ein einfaches PING-Werkzeug) wäre dann manchmal durchaus hilfreich. Gut gelöst ist die automatische Sprachumschaltung – abhängig von den bereits im Browser eingestellten Präferenzen erscheint die Bedienoberfläche in Deutsch, Englisch oder auch Japanisch.

Einmal richtig konfiguriert sorgt der Mguard PCI dann unabhängig von Hardware und Betriebssystem des angeschlossenen Rechners für die sichere Netzanbindung. Durch die Ausführung als PCI-Erweiterungskarte qualifiziert er sich überall dort, wo einzelne PCs außerhalb eines Firmennetzes eine sichere Netzanbindung benötigen oder wo besonders sensible Systeme innerhalb eines Netzes speziellen Schutz brauchen. Im Systemgehäuse integriert und damit selbst vor Manipulationen gesichert schützt er dann sowohl den Rechner als auch die Netzumgebung vor Gefahren und gewährleistet, dass die vorgegebenen Firewall-Regeln und VPN-Routings auch eingehalten werden.

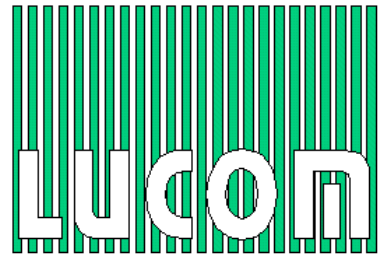
Der empfohlene Verkaufspreis für das Produkt Mguard PCI beginnt bei 259 Euro für die Version ohne VPN, die „Enterprise“-Version für bis zu 10 VPN-Verbindungen kostet 317 Euro, und der Preis für das Topmodell „Enterprise XL“ schließlich beläuft sich auf 349 Euro (jeweils zuzüglich Mehrwertsteuer). Die Lizenzgebühr für den Virenschutz beträgt zusätzlich 57 Euro pro Jahr.

Bernhard Sterzbach/wj

Info: Innominat  
Tel.: 030/63923300  
Web: [www.innominat.de](http://www.innominat.de)

# Innominate **mGuard**

## Industrial Network Security



Innominate  
**certified**  
partner



Innominate  
**mGuard**

**[WWW.LUCOM.DE](http://WWW.LUCOM.DE)**

**LUCOM** GmbH

Komponenten & Systeme  
Ansbacher Str. 2a

**D 90513 Zirndorf**

Tel. +49 (0) 9127 / 59 460-10

Fax. +49 (0) 9127 / 59 460-20

E-Mail: [info@lucom.de](mailto:info@lucom.de)