

Sicherheit im Zwölferpack bietet das in Rot gehaltene M-Guard Blade-Pack, das bei Bedarf jedem Server im Netzwerk eine eigene Firewall voranstellt.



# Einfach sicher

Angesichts des Trends zur Server-Konsolidierung, der auch vor der Hardware selber nicht Halt macht, scheint mit der Blade-Pack-Firewall von Innominate ein lang gehegter Wunsch von IT-Verantwortlichen in Erfüllung zu gehen: In Server-Farmen einfach und günstig Sicherheit gewährleisten zu können. **VON CHRISTIAN FICHTER\***

Vor knapp zwei Jahren überraschte ein junges Unternehmen aus Berlin die von Berichten über Internet-Gefahren geschüttelte IT-Branche mit einer unüblichen, aber sehr willkommenen Netzwerk-Appliance: dem M-Guard. Dabei handelt es sich um eine kleine Plastikbox, die man zwischen einen zu schützenden Rechner und seinen Netzwerkanschluss stöpselt. Der Clou des Gerätes ist sein so genannter Stealth-Mode, welcher es auch Anwendern ohne Fachwissen ermöglicht, einen beliebigen Rechner ohne jede Umkonfiguration vor Angriffen aus dem Internet zu schützen. Dieses ebenso simple wie überzeugende Konzept weitet der Hersteller jetzt in Form des M-Guard-Blade-Pack auf professionelle Serverumgebungen aus. Dieses soll einfa-

che, preiswerte Sicherheit bieten und gleichzeitig robust und flexibel genug sein für unternehmenskritische Anwendungen.

Die vom Hersteller treffend Device Attached Security genannte Idee sieht vor, jeden Server im Rack mit einer eigenen, dedizierten Sicherheitsschleuse auszustatten. Einerseits erhöht man so die Ausfallsicherheit durch Minimierung des Single Point of Failure. Andererseits maximiert man die Flexibilität, indem jeder Server seine eigene Sicherheitskonfiguration bekommt. Mit herkömmlichen Gateways ist das schwierig bis unmöglich umzusetzen.

Beim Blade-Pack handelt es sich um einen 19-Zoll-Rack-Einschub mit drei Höheneinheiten, welcher bis zu zwölf einzelne M-Guard-Appliances aufnehmen kann.

Diese stecken jetzt nicht mehr in rotem Plastik, sondern in metallenen Einschüben. Wie es sich für eine professionelle IT-Umgebung gehört, kann man die einzelnen Blades auch im laufenden Betrieb auswechseln, ohne dass die Nachbarn davon tangiert werden. In jedem Einschub steckt ein abgespecktes und auf Sicherheit getrimmtes Mini-Linux. Dieses wird von einem X-Scale-Prozessor von Intel angetrieben, wie man ihn auch in Taschencomputern findet.

Die Blades gibt es in zwei Sorten, mit 266 oder 533 MHz schnellem Prozessor. Dabei erlaubt die schnellere XL-Ausführung 250 anstatt nur zehn VPN-Verbindungen (Virtual Private Network), bei maximal 70 MBit/s

\* Christian Fichter ist freier Journalist in Zürich.

Datendurchsatz. Der zur Verfügung stehende Arbeitsspeicher ist bei beiden Ausführungen 64 MByte gross und nicht erweiterbar. Das Rack-Modul enthält zwei unabhängige, redundante Netzteile sowie einen Controller für die übergeordnete Steuerung der maximal zwölf anderen Rechner. Praktischerweise handelt es sich dabei ebenfalls um ein M-Guard-Blade. Allerdings, abgesehen von einer Statusanzeige für die Einschübe und dem Versenden von SNMP-Nachrichten (Simple Network Management Protocol) etwa beim Ausfall eines Netzteils bleibt unklar, welche Funktion der Controller hat. Denkbar wären etwa Fernsteuerung oder gemeinsame Konfiguration der Blades. Doch ist im Verwaltungswerkzeug nichts davon zu sehen. Noch dazu ist die Anzeige des Software-Status der Blades falsch. So muss man zur Kontrolle trotzdem jedes einzeln administrieren. Hier wird Innominat hoffentlich schnell nachbessern, so wie sie es beim ersten M-Guard getan hat.

## Komfortable Einrichtung

Die Inbetriebnahme des Blade-Pack gestaltet sich schon fast ungewohnt problemlos. An der Vorderseite befindet sich je ein Anschluss für WAN (Wide Area Network) und LAN, welche man am besten über eine Patchbay mit den im Rack eingebauten Servern verbindet. Es handelt sich um 100-MBit-Schnittstellen. Zukunftsträchtiges Gigabit-Ethernet wäre durchaus sinnvoll gewesen, ist aber nicht erhältlich. Einstellungen wie Betriebsmodus, Firewall-Regeln oder Passwort können nun bequem per Webbrowser über eine SSL-verschlüsselte (Secure Socket Layer) Verbindung vorgenommen werden. Eine Fernkonfiguration über die WAN-Schnittstelle ist möglich, standardmässig aber abgeschaltet.

Hat man erst eine Konfiguration erstellt, so kann man diese abspeichern und später wieder ins Gerät laden. Sehr interessant ist die Möglichkeit, Konfigurationen zeitgesteuert zu wechseln. Dazu verfügt jedes Blade über einen Scheduler, welcher eine Einstellungsdatei von einem Server im Netz holt und die Konfigurationsänderung selbstständig vornimmt.

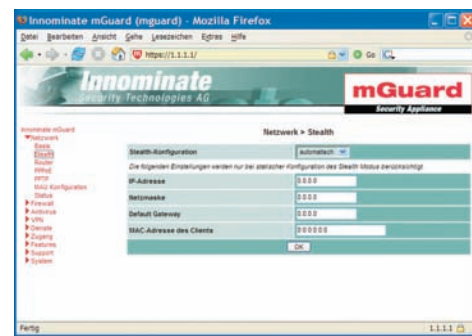
Eine herausragende Eigenschaft des M-Guard ist der erwähnte Stealth-Modus. Dieser ermöglicht eine transparente Einbindung der zu schützenden Rechner. Dabei belauscht ein Blade einen Moment lang den ein- und ausgehenden Netzwerkverkehr und konfiguriert sich dementsprechend selbst mit der IP-Adresse des Servers. Dadurch wird das M-Guard quasi unsichtbar. Für Aussenstehende ist nicht unmittelbar erkennbar, dass die Verbindung überhaupt

durch eine Firewall geschützt wird. Schon das alleine ist ein wesentliches Sicherheitsmerkmal, das potenzielle Hacker vor Schwierigkeiten stellt. Doch der Stealth-Mode ist kein Allheilmittel, denn die Transparenz endet dort, wo Windows-Rechner ins Netz eingebunden werden sollen, oder bei Verwendung weniger gebräuchlicher Dienste wie etwa Videotelefonie. Immerhin lassen sich auch im Stealth-Modus die Firewallregeln editieren, so dass mit etwas Mehraufwand diese Klippen umschiffen werden können. Hier fehlt uns noch eine UPNP-Implementierung (Universal Plug&Play), wie wir sie schon beim ursprünglichen M-Guard angedacht hatten.

## Die Blades im Betrieb

Die Anwendungsszenarien gehen über den Stealth-Mode hinaus. Es können, wie mit konventionellen Firewalls, auch ganze Netze geschützt werden. Dazu versetzt man das M-Guard in den Router-Modus und verwendet die eingebaute Network Address Translation (NAT), den DHCP-Server (Dynamic Host Control Protocol) und den DNS-Cache (Domain Name Service), welcher Adressauflösungen zwischenspeichert. Die Dokumentation verdient wie beim Original-M-Guard besonderes Lob. Ein Flyer erklärt die schnelle Inbetriebnahme, und ein ausführliches PDF-Handbuch dient der Vertiefung. Darin werden anschaulich verschiedene Anwendungsfälle illustriert, die man durch ein solches Firewall-Multipack abdecken kann. Leider gibt es auch ein paar Lücken. Die Funktion des Controller-Blades etwa wird kaum erläutert.

Einmal eingerichtet, versieht das Blade-Pack unauffällig seinen Dienst. Wenn auch noch nicht alle Möglichkeiten des Konzepts implementiert sind, so profitieren Administratoren doch von der zuverlässigen Softwarebasis der Blades. Das Innominat Se-



Der Stealth-Mode lässt sich automatisch einrichten.

cure-Linux ist nämlich identisch mit dem seit bald zwei Jahren gepflegten Betriebssystem der Einzelplatz-Appliances aus der M-Guard-Reihe. Das vereinfacht Software-Updates, erklärt aber auch selten nachgefragte Beigaben wie einen Dyn-DNS-Client. Stattdessen würden wir uns eine Möglichkeit zur Failover-Konfiguration wünschen, damit beim Ausfall eines Blades ein anderes dessen Aufgabe übernehmen kann. Diese Funktionalität ist immerhin angekündigt und soll nachgeliefert werden.

Optional kann pro Blade ein kostenpflichtiger Virenschutz von Kaspersky nachgerüstet werden. Dabei werden eingehende Dateien in die RAM-Disk kopiert und gescannt. Eine Einschränkung ergibt sich aus dem nicht ausbaubaren Arbeitsspeicher von 64 MByte: Grössere Dateien können nicht gescannt werden. Für die einfache Konfiguration der Blades in grossen und komplexen Umgebungen bietet die Herstellerin zudem mit dem Security Configuration Manager ein grafisches Tool an, in welchem man Sicherheitsumgebungen per Drag&Drop erstellen kann. Dieses lässt sich Innominat aber mit rund 10 000 Franken teuer bezahlen. Hier wäre eine kundenfreundlich abgestufte Preisgestaltung wünschenswert, zum Beispiel angepasst an die Netzwerkgrösse.

## Fazit

Das M-Guard Blade-Pack schützt umfangreiche, heterogene Serverumgebungen auf einfache und zugleich effiziente Weise vor Gefahren aus dem Internet. Das System ist einfach aufzubauen, skalierbar und flexibel, bleibt dabei aber preislich im Wohlgefühlbereich. Besonders willkommen erscheint uns die Möglichkeit, dank eines Blade-Packs auch nicht unternehmenskritische und dementsprechend vielleicht weniger aufwändig gesicherte Server ohne grosse Kosten effektiv zu schützen. Das Blade-Pack empfiehlt sich daher dort, wo es an Zeit und Geld mangelt, aber Sicherheit dennoch ernst genommen wird. ■

 [www.computerworld.ch](http://www.computerworld.ch)  
Webcode: 0532410

### INFO

## Blade-Pack im Überblick

### M-Guard Blade-Pack

**Hersteller:** Innominat

**Preis:** Blade-Base 4355 Franken, Blade Enterprise 830 Franken, Blade Enterprise XL 998 Franken.

**Vorteile** Einfache Bedienung, preiswert, sicher, flexibel.

**Nachteile** Beschränkte Controllerfunktion und -Dokumentation, nur zehn VPN-Verbindungen bei kleinerem Modell, RAM nicht aufrüstbar, keine UPNP-Unterstützung.

[www.innominat.de](http://www.innominat.de); [www.cetus.ch](http://www.cetus.ch)

