Publication: Computerworld (CH)
Publishing House: IDG Communications
Publication date: 16.05.2008
Page: 18-19

Security für den Mittelstand: Zahlbar und sicher

KMU stehen vor der grossen Herausforderung, den Schutz ihrer IT mit begrenzten finanziellen und personellen Ressourcen sicherzustellen. Gefragt sind also gleichermassen wirksame wie einfach zu verwaltende Abwehrsysteme. VON FRANZ KAISER

ILLUSTRATION: FOTOLIA

HIER LESEN SIE...

- vor welchen Security-Herausforderungen KMU heute stehen.
- warum UTM einen wirklich sicheren Rundumschutz bietet.
- wie sich UTM-Systeme weiterentwickeln werden.

Polymorphe Viren, Social Malware, modularer Schadcode oder Blended Threats, die gleich ein ganzes Bündel an bösartiger Software mitbringen: Was die Anzahl, Vielfalt und Raffinesse angeht, hat die Cyberkriminalität inzwischen neue Dimensionen erreicht. Betroffen von den diversen Internetbedrohungen sind längst nicht mehr nur die Grosskonzerne, sondern auch kleine und mittlere Unternehmen. Und Antiviren-Software und Firewalls für den Desktop bieten längst keinen ausreichenden Schutz mehr.

In der Tat ist für Mittelständler das Security-Problem noch grösser als bei Konzernen. Die Krux: Während grosse Unternehmen über die nötigen Ressourcen verfügen, in viele Einzellösungen unterschiedlicher Hersteller zu investieren, können sich KMU dies nicht leisten – der Kosten- und Managementaufwand ist zu hoch.

Genau hier setzen sogenannte UTM-Lösungen (Unified Threat Management) an. Sie integrieren das komplette Spektrum der Netzwerksicherheit in einer einzigen Appliance und machen das Netzwerk so robust, dass es gegenüber den meisten Attacken unempfindlich wird. Damit stehen KMU nicht mehr vor der schwierigen Entscheidung, welche Security-Elemente sie zwingend brauchen und auf welche sie allenfalls verzichten können.

Komponenten mit echten UTM-Fähigkeiten weisen folgende Funktionen auf:

- Die Firewall sorgt für das Ausführen verbindungsbasierter Richtlinien zusammen mit den Anforderungen für SSL und IPSec VPN.
- Intrusion Prevention Security (IPS) hilft, die Ausbreitung von Würmern einzudämmen und einige gezielte Attacken abzuwehren. Viele IT-Administratoren bemängeln an IPS jedoch, dass es im Netzwerk eine sichere und eine unsichere Seite schafft. Mit anderen Worten: Maschinen, die auf demselben LAN-Segment wie infizierte Maschinen laufen, sind einem Risiko ausgesetzt. Um das ganze Netzwerk zu sichern, müsste IPS vor jedem Gerät an Endpunkten platziert werden.
- Inline-Antivirus ist ein treibendes Moment für Security Appliances geworden, da unerwünschte oder infizierte E-Mails, Instant Messaging und P2P-Files (Peer to Peer) die Verarbeitungskapazitäten der jeweiligen Server beeinträchtigt.

Franz Kaiser, ist Country Manager Schweiz und Österreich bei bei Fortinet.

- URL Content Filtering wurde anfänglich nicht als Security-Thema behandelt. Seit immer mehr Websites mit bösartigem Inhalt infiziert sind, ist es jedoch eine kritische Komponente zur Absicherung des Endnutzers.

Den grössten Nutzen bringt eine Kombination dieser UTM-Features, da sich Angriffe, die Elemente bösartiger Software mit Netzwerkattacken über neue Protokolle verbinden, nur mit einer integrierten Appliance abwehren lassen.

Trends: Weiterentwicklung von UTM

UTM befindet sich aktuell im Wandel: Der nächste Schritt in der Evolution der kombinierten Security Appliances wird nun mit der Ergänzung um Netzwerkkapazitäten vollzogen. Routing-Protokolle wie beispielsweise OSPF (Open Shortest Path First), RIP (Routing Information Protocol) und BGP (Border Gateway Protocol) bieten die architektonische Flexibilität, die Unternehmen benötigen. Allerdings ohne die Kosten für Konzipierung, Konfiguration und Wartung separater Router und Lastverteiler zu verursachen. Oft kann dann eine UTM-Lösung eingesetzt werden, ohne dass ein Router benötigt wird – eine deutliche Steigerung des Wertbeitrags von UTM und gerade für KMU ein überzeugendes Argument.

Wie traditionelles UTM zeigte, kann die Zusammenführung und Integration von Security-Funktionen in Bezug auf Kosten und Effizienz eine wirksame und wirtschaftliche Lösung für Unternehmensnetzwerke aller Grössenordnung bieten. Security-Anbieter können darauf aufbauend Lösungen entwickeln, die das Netzwerk durch die Kombination von Netzwerk-Switch, IPS, AV, Firewall und Router schützen. Anders ausgedrückt: Switch und Router werden künftig in die traditionelle UTM Security Appliance integriert.

Für diese Entwicklung zwingend notwendig ist eine geswitchte Netzwerkarchitektur, normalerweise mit Core und Access Switches. Virtuelle LANs (VLAN) liessen sich dazu einsetzen, um bei Bedarf Granularität bis hin zu den Geräten zu schaffen. Der Switch setzt dabei Richtlinien auf Basis von Informationen der Schicht 2 und 3 um. Datenströme, die normal sind und daher zulässig, lassen sich durch zusätzliche IPS-Funktionalitäten filtern, die im Idealfall direkt im Switch ablaufen. Verbindungen ins Internet oder in fremde Netzwerke lassen sich mit Firewall-Funktionalität realisieren, die ebenfalls im Switch eingebettet sind. Eine derartige UTM Security Appliance könnte ferner zusätzliche Netzwerksegmentierungen schaffen, etwa für Transaktionszonen und Abteilungsabgrenzung.

Fazit

Dieses Konzept führt Unified Threat Management weit über seinen Ursprung als einfache Security-Plattform hinaus. Security-Lösungen werden mit Netzwerk-Features die Branche bald grundlegend verändern. Traditionelle Router- und Switch-Anbieter werden die Erfahrung machen, dass ihre auf Schnelligkeit und Einfachheit aufbauenden Produkte nicht im Stande sind, tiefgehende Paketinspektionen und granulare Absicherung einzuschliessen. Auf Firewall oder IPS spezialisierte Security-Anbieter werden bald den Druck der flexibleren Produkte zu spüren bekommen, die Security mit Networking verbinden.

Gerade in KMU kommen die Vorteile solch neuartiger UTM-Lösungen vom Typ Alleskönner besonders zum Tragen. Denn damit lassen sich unterm Strich Managementaufwand, Zeit und Kosten sparen – Argumente, die im Mittelstand besonders überzeugend sind. ■