| Publication: | Publishing House: | Publication date: | Page: |
| --- | --- | --- | --- |
| Netzwoche (CH) | Netzmedien AG | 28.10.2009 | 27-29 |

# Komplettlösungen rollen den IT-Sicherheitsmarkt auf

Unified Threat Management ist in aller Munde und wird sogar als Zeichen für den fortschreitenden Reifeprozess der IT-Sicherheit gewertet. Anstatt auf eine Vielzahl von Tools zu setzen, zieht der moderne CIO einfach sein Schweizer Taschenmesser aus der Westentasche. *Christian Walter*

Auf den Enron-Finanzskandal folgte das SOX-Reglement mit neuen Anforderungen an die Compliance; was alles auf die Finanzkrise folgt, ist noch nicht vollständig klar. Wenn SOX allerdings als Indikator anzusehen ist, dürfte so mancher CIO ins Rotieren kommen. Dies gilt aber auch dann, wenn die kommenden Massnahmen weniger anspruchsvoll ausfallen, als erwartet. Selbst kleine Veränderungen bedeuten bei der heutigen Komplexität viel Arbeit.

Es ist also nicht verwunderlich, dass Lösungen, die eine Reduktion der Komplexität versprechen, mit Wohlwollen betrachtet werden. Unified Threat Management (UTM) erhebt diesen Anspruch und wird deswegen gern von Marketingstrategen als Rundumlösung für Sicherheitsprobleme angepriesen. Nicht zuletzt auch deswegen, da es zur Senkung der Kosten beitragen soll.

## Der Markt wächst

Gemäss den Markforschern von IDC belief sich das Volumen des Weltmarkts für UTM im Jahr 2008 auf etwa 1,5 Milliarden US-Dollar und wuchs gegenüber dem Vorjahr um 14 Prozent. Zum Vergleich: der Gesamtmarkt für Security Appliances wuchs nur um 4 Prozent. Ähnlich sieht es in der Schweiz aus. 2008 belief sich das Marktvolumen für UTM auf etwa 16,1 Millionen Dollar. Dies entspricht einem Wachstum von etwa 13 Prozent gegenüber dem Vorjahr im Bereich UTM, während der Gesamtmarkt nur um 4 Prozent wuchs. Somit boomt der Markt für UTM nicht nur global, sondern auch in der Schweiz. Dabei ist er noch vergleichsweise jung. Der Begriff selbst wurde erst 2004 geprägt. Hervorgegangen ist dieser Lösungsansatz aus der klassischen Firewall. Um zahlreiche Funktionen erweitert, vereinigt UTM heute ein ganzheitliches Sicherheitskonzept in einer einzigen Lösung. Dabei deckt eine UTM-Lösung zahlreiche Bereiche ab, wie Intrusion Prevention, Antivirus, VPN, Anti-Spam, Content Filter, Load Balancing oder verschiedene On-Appliance-Reporting-Funktionen. Seit Neuestem gibt es solche Lösungen auch virtualisiert. Der Umfang einer jeden UTM-Lösung kann aber von Hersteller zu Hersteller variieren.

## UTM oder Best of Breed?

Dabei steht der einheitliche UTM-Ansatz dem Best-of-Breed-Konzept gegenüber, das auf eine Kombination verschiedener Lösungen unterschiedlicher Anbietern setzt. Oder anders formuliert: die Bequemlichkeit, die eigene Sicherheit mit nur einem Werkzeug zu managen, gegenüber der Gefahr, einen Single Point of Failure zu kreieren. Hersteller von UTM-Lösungen verwehren sich aber gegen diese Darstellung. In ihren Augen ist eine Sicherheitslücke bei beiden Ansätzen gleich schlimm, denn bei keiner der beiden Varianten existiert eine zweite Verteidigungslinie. Im Zweifelsfall soll das Risiko einer Sicherheitslücke bei UTM sogar geringer sein, da hier alle Komponenten aufeinander abgestimmt sind. Auf diese Weise sollte es keine blinden Flecken im Sicherheitskonzept geben. Ausserdem arbeiten die einzelnen Anwendungen ohne Probleme miteinander.

Vielleicht liegt der Grund für das Unbehagen aber auch woanders: Einerseits herrschen Zweifel an der universellen Qualität von UTM-Lösungen gegen alle Arten von Bedrohungen, und andererseits möchte so manch ein CIO, dass die Sicherheit nicht von nur einem einzigen Partner abhängt. Nichtsdestotrotz sprechen die Wachstumsraten für UTM.

## Die Qual der Wahl

Zurzeit gibt es aber noch ein weiteres Indiz, das für die Zukunftsfähigkeit von UTM spricht: das steigende Interesse von Seiten grosser Unternehmen. Das ist neu, da UTM bisher vor allem im KMU-Umfeld zum Einsatz kam. Im Gegensatz zu grossen Unternehmen verfügen diese nämlich häufig nicht über die nötigen Ressourcen, um in viele Einzellösungen unterschiedlicher Hersteller zu investieren – Kosten- und Managementaufwand sind einfach zu hoch. Mit steigender Skalierbarkeit von UTM scheint sich das aber zu ändern.

# Konsolidierung der Netzwerksicherheit

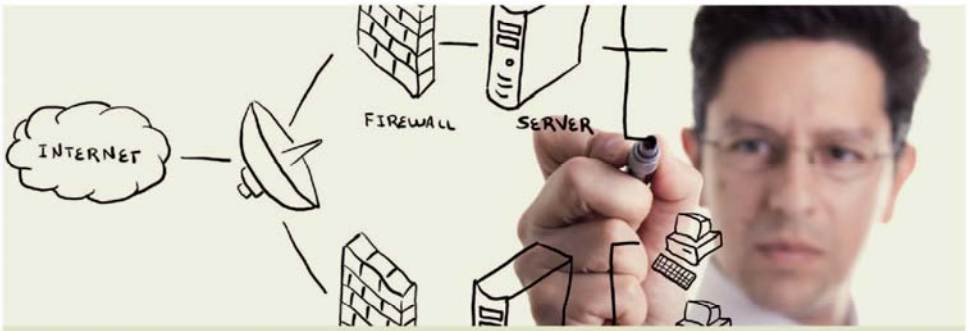
IT-Sicherheitsfachleute sind mit einer ständig wachsenden Vielfalt von Bedrohungen und Compliance-Anforderungen konfrontiert, während sie gleichzeitig steigende Kosten, Platzmangel im Rechenzentrum, zunehmend komplexes Management sowie Umweltfragen bewältigen müssen. *Franz Kaiser*

Betrüger, Phisher, Bot Herder, Spammer, Onlineerpresser, Identitätsdiebe – sie alle haben es auf eins abgesehen: kriminellen Gelderwerb. Vor zehn Jahren reichte eine Firewall mit Paketfilter, um sich vor praktisch allen Bedrohungen aus dem Internet zu schützen. Die Cyberkriminalität hat jedoch neue Dimensionen erreicht, was die Anzahl, Vielfalt und Raffinesse der Internetbedrohungen angeht. Antivirus-Software und Firewall allein bieten Enterprise-Unternehmen allenfalls einen löchrigen Schutz.

Die Entwicklung der Informationssicherheit gleicht einem Wettrüsten: Hacker, Cracker und Virenschreiber gegen Security-Anbieter. Sobald eine neue Schwachstelle auftaucht, ziehen die Security-Anbieter sofort mit Schutzmechanismen und Sicherheitsmassnahmen nach, worauf die Gegenseite neue Wege findet, um Blockaden zu umgehen und neue Schutzwälle anzugreifen. Weiter verschärft hat sich der Kampf durch die Entwicklung sogenannter Blended Threats, die ein ganzes Bündel an bösartiger Software unterschiedlicher Kategorien kombinieren wie zum Beispiel Trojaner mit integrierten Spam-Engines oder Viren mit Spyware-Payloads. Paradox ist, dass die meisten Security-Technologien den Blended Threats einiges zu verdanken haben.

Cyberkriminelle sind schnell und erfinderisch und haben die meisten Security-Technologien oft genug auf die Plätze verwiesen. Erfreulicherweise zeichnet sich bei der Netzwerksicherheit eine Wende ab. Es werden umfassende Lösungen entwickelt, die das Netzwerk selbst so robust machen, dass es gegenüber den meisten Attacken unempfindlich wird. Die lange gehegte Vorstellung, es könne ein Netzwerk ohne Schad-Traffic und Missbrauch geben, wird nun mithilfe konvergierter Sicherheitslösungen Realität. Gute Aussichten für grosse Unternehmen.

**Franz Kaiser** ist Country Manager Austria, Switzerland and CEE bei Fortinet.




**Die Entwicklung der Informationssicherheit gleicht einem Wettrüsten: Hacker, Cracker und Virenschreiber gegen Security-Anbieter.** *Bildquelle: Fotolia*

## «Frankenstein»-Lösungen sind fehl am Platz

Eine Netzwerk-Fabric lässt sich absichern, indem Netzwerk-Switch, Intrusion-Protection-System, Antivirus, Firewall und Router in einem System kombiniert werden. Mit anderen Worten: Switch und Router werden Teil der traditionellen Unified Threat Management (UTM) Appliance. Zwingend notwendig dafür ist eine integrierte, geswitchte Netzwerkarchitektur. Der Schlüssel dazu ist hoch konzentrierte, proprietäre Hardware. «Frankenstein»-Lösungen ebenso wie Bundled Threat Management auf der Basis rasch gebildeter strategischer Allianzen einiger Security-Anbieter sind hier fehl am Platz.

UTM-Lösungen vom Typ «Alleskönner» werden in drei Bereichen hoch interessante Effekte haben: Netzbetreiber und Serviceanbieter könnten damit endlich bösartigen Traffic aus ihren Backbones filtern und ihren Kunden saubere Leitungen anbieten. Die Idee, dass die weitgehende Entfernung von Viren, Trojanern, Würmern und Malware aus den Netzwerken in der Verantwortung der Betreiber liege, steht seit etlichen Jahren im Raum. Unter anderem haben Kosten, technisches Know-how und oft auch der politische Wille die praktische Umsetzung bislang verhindert. Die technologische Basis dafür liesse sich nun legen. Das zweite Szenario betrifft die internen Netzwerke in Enterprise-Unternehmen. Mit den neuartigen UTM-Lösungen liesse sich jede Abteilung und schliesslich auch jedes Gerät segmentieren und schützen. Das interne Netzwerk entspräche zum ersten Mal wirklich einem harten Sicherheitsmodell.

Das Konvergenzkonzept führt Unified Threat Management weit über seinen Ursprung als einfache Security-Plattform hinaus. Security-Lösungen werden sehr bald immer häufiger Netzwerk-Features beherbergen. Traditionelle Anbieter von Routern und Switches werden die Erfahrung machen, dass ihre auf Schnelligkeit und Einfachheit aufbauenden Produkte nicht im Stande sind, tiefgehende Paketinspektionen und granulare Absicherung einzuschliessen. Auf Firewalls und Intrusion Protection spezialisierte Security-Anbieter werden im Markt bald den Druck flexiblerer Produkte zu spüren bekommen: Produkte, die Security mit Networking verbinden.

## Security-Virtualisierung trifft auf UTM

Die Integration mehrerer Sicherheitsfunktionen in einer Appliance hat den klassischen Firewall-Markt stark verändert. Sicherheitsfunktionen wie Stateful Inspection Firewalling, Antivirus, Intrusion Prevention & Detection (IPS/IDS), Antispam, Web-Content Filtering, Traffic Shaping und dynamisches Routen wurden in einer einzigen Appliance zusammengefasst. Mit der Virtualisierung

der integrierten Sicherheitsfunktionen erhält das Security-Management mit UTM einen weiteren Freiheitsgrad.

Firewall-Virtualisierung ist kein ganz neues Thema in der Netzwerksicherheit. Schon seit Jahren virtualisieren Carrier, Internet Service Provider (ISPs), Hosting und Managed Security Provider (MSPs) klassische Netzwerk-Firewalls für ihre Kunden. Zum Einsatz kamen meist grössere redundante Cluster-Firewall-Systeme, die von mehreren Endkunden geteilt wurden. Jeder Kunde benutzte somit seine eigene virtuelle Firewall mit entsprechend getrennten Konfigurationsmöglichkeiten. Das spart Hardware- und Softwarelizenzen und ermöglichte den Providern, ihren Kunden einen kostengünstigen und hoch verfügbaren Firewall-Service anzubieten. Doch anders als damals ist die Virtualisierung heute nicht mehr auf klassisches Stateful Inspection Firewalling begrenzt. Heute können auch alle zusätzlichen UTM-Sicherheitsfunktionen virtualisiert werden. Auf Knopfdruck können diese Funktionen innerhalb einer virtuellen Firewall aufgeschaltet werden. Selbst der Betriebsmodus lässt sich beliebig kombinieren. Eine virtuelle Firewall kann beispielsweise im NAT/Route-Modus laufen und die zweite im sogenannten Transparent Mode (Layer 2). Auf der ersten Instanz könnten Funktionen wie Firewall, IPS und Antivirus laufen und auf der zweiten nur ein reiner Webfilter.

Vermehrt verwenden heute auch Endkunden Virtualisierungsfunktionen. Firmennetzwerke sind heute derart komplex, dass mit der Virtualisierung ganzer Firewall-Funktionen oder der Virtualisierung von Netzwerkschnittstellen gearbeitet wird. Auch für die Absicherung von Niederlassungen, getrennten Business Units und Abteilungen bietet sich Virtualisierung an. Die Administration kann an verschiedene Administratoren delegiert werden, die dann jeweils nur ihre virtuelle Firewall sehen und administrieren können.

### UTM für Enterprise-Unternehmen der bestmögliche Schutz

Nimmt man alle Vorteile von UTM und der Virtualisierung verschiedener Security-Funktionen zusammen, so erhält man einen umfassenden, flexiblen und einfach zu verwaltenden Rundumschutz. Besonders Enterprise-Unternehmen werden hiervon profitieren können, da hier Lösungen benötigt werden, die schnell auf Veränderungen und veränderte Anforderungen angepasst werden müssen und zudem ohne grossen Mehraufwand leicht zu erweitern sein sollten. UTM ist da der richtige Weg.