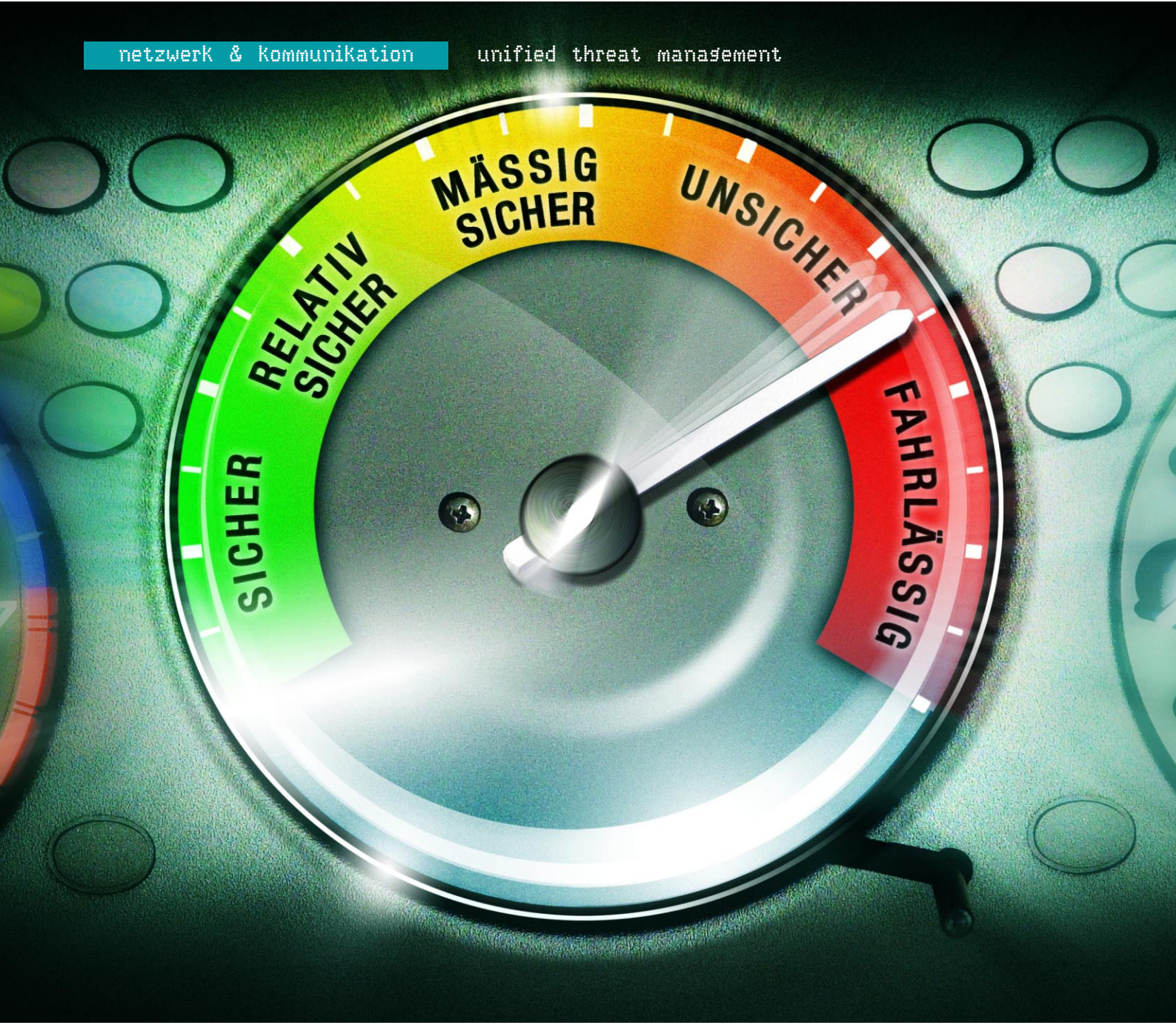


JOHANNES FRITSCHE

RUNDUM SICHER

Für kleine und mittelständische Unternehmen mit begrenzten finanziellen und personellen Ressourcen kann Unified Threat Management (UTM) eine kostengünstige Lösung sein, die Unternehmens-IT komplett abzusichern. Wer allerdings das Risiko möglicher Ausfälle der Schutzsysteme wegen seiner speziellen betrieblichen Bedingungen minimieren muss, fährt mit einer Mehr-Hersteller-Strategie sicherer.

Immer raffinierter werdende Angriffe auf die Informations- und Kommunikations-Infrastruktur der Unternehmen erfordern komplexe Schutzlösungen. Viren-, Spam- und Spyware-Schutz, Firewall und Intrusion-Detection- oder Prevention-System, Content-Filter, Authentifizierung und Verschlüsselung gehören mittlerweile zum Standard-Arsenal der Abwehr.

Für die IT-Teams ist es zu einer großen Herausforderung geworden, die meist von verschiedenen Herstellern stammenden Teilsysteme korrekt zu installieren, aufeinander abzustimmen und zu warten. Vor allem kleine und mittlere Unternehmen haben damit Schwierigkeiten, ganz zu schweigen vom Kosten- und Zeitaufwand.

„Durch eine falsche oder nicht optimierte Konfiguration verschenken die IT-Verantwortlichen einen Teil des Sicherheitspotenzials der Schutzlösungen oder heben die Schutzwirkung sogar komplett auf. Dann wiegt sich der Anwender in falscher Sicherheit", warnt Sebastian Schreiber, Geschäftsführer der Tübinger SySS GmbH, die sich in der Fachwelt mit der Durchführung anspruchsvoller Penetrationstests einen Namen gemacht hat.

Eine Möglichkeit, die Komplexität besser zu beherrschen, sind All-in-One-Lösungen. Michael Claus, Leiter EDV und Organisation bei der KHD Humboldt Wedag AG in Köln, setzt auf diese Strategie. „Leistung und Kostenansatz sind wichtig, ohne den Sicherheitsgedanken aufgeben zu müssen". Das Unternehmen entwickelt und plant mit rund 700 Mitarbeitern Zement- und Kohleaufbereitungs-Anlagen, die weltweit zum Einsatz kommen. Rund um die Uhr greifen Tochterfirmen, Ingenieur-Teams, Außendienstler, Telearbeiter und Kunden auf die betrieblichen Anwendungen zu. Die Verbindung für alle externen Anwender läuft über ein Virtual Private Network (VPN), das durch eine NetScreen 50 Firewall sowie Viren- und Spamschutz abgesichert ist. 50 VPN-Verbindungen können so gleichzeitig sicher genutzt werden.

Die gesamte Sicherheitstechnik, also Hardware, Betriebssystem und Schutz-Software, hat Michael Claus als fertige Box (als Appliance) von einem IT-Dienstleister installieren lassen. Dieser übernimmt auch das laufende Management der Anwendungen sowie die Wartung der Software und Fehler-Patches. Die IT-Abteilung kümmert sich nur noch um die Administration. „Trotz der guten Funktionalität ist die Lösung unkompliziert, sodass wir keinen Power-Administrator mehr brauchen, der nichts Anderes mehr tun kann", berichtet der IT-Leiter.

Gezielte Angriffe

Dass integrierte Schutz- und Abwehrsysteme wie bei der Kölner Firma, die sich über eine Management-Konsole verwalten lassen, immer notwendiger werden, zeigte bereits der McAfee Virtual Criminology Report von 2005. Die Studie führte der unabhängige Schweizer Internet-Sicherheits-Experte und Computerkriminologe Peter Troler vom Eidgenössischen Technologie-Institut in Zürich im Auftrag von McAfee (www.mcafee.de) durch. Unterstützung lieferten auch europäische Behörden zur Bekämpfung von High-Tech-Verbrechen in Großbritannien, Frankreich, Deutschland, den Niederlanden, Spanien und Italien.

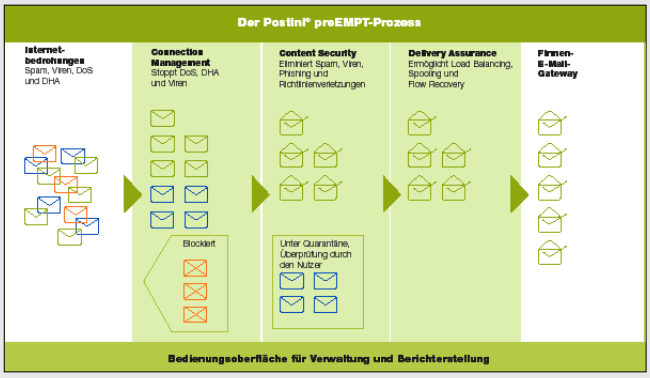
Die Untersuchung zeigt eine deutliche Weiterentwicklung der Internet-Kriminalität. Der einzelne Computerhacker, der von seiner Wohnung aus Angriffe auf einzelne Rechner unternimmt, wird von einer organisierten „Cybermafia" verdrängt, die umfangreiche unsichtbare Bot-Netzwerke mobilisiert, um Unternehmen anzugreifen und zu erpressen, oder mit Spyware Industriespionage für den Mitbewerber betreibt.

„Wie die Hacker sind Angehörige des organisierten Verbrechens immer auf der Suche nach Schwachstellen innerhalb des Systems, die sie ausnutzen können, und wie Hacker genießen sie diese neue Herausforderung. Die Strafverfolgungsbehörden müssen sich dieser Bedrohung jetzt bewusst werden und damit beginnen, sie zu bekämpfen. Sonst werden wir eine Explosion der Internet-Kriminalität erleben, die die vergangene Zeit als embryonal erscheinen lassen wird", fordert Toralv Dirro, Security Sales SE bei McAfee.

Schwachstellen als Ansatzpunkte für Angriffe gibt es genug. Ipsos Research hat für eine andere Studie im Auftrag von McAfee 600 IT-Entscheider aus europäischen Unternehmen mit mehr als 250 Mitarbeitern befragt, welchen Ansatz sie beim Patch-Management verfolgen. Heraus kam, dass 45 Prozent der Befragten nicht in der Lage waren, ihre IT-Infrastruktur hundertprozentig vor Risiken durch Software- und Netzwerk-Schwachstellen zu schützen.

Zu einer ähnlichen Einschätzung der Bedrohungslage kommt der aktuelle MessageLabs Intelligence Report (www.messagelabs.de) für das erste Quartal 2006 über die globale Viren-, Spam- und Phishing-Aktivitäten sowie abzusehende Trends. „Dass die Bedrohungslage insgesamt weitgehend stabil bleibt, ist nur die halbe Wahrheit. In Wirklichkeit werden die Cyber-Kriminellen immer besser darin, die Aufmerksamkeit von sich abzulenken und exakt gezielte Viren- und Phishing-Angriffe im kleinen Rahmen auszuführen. Es werden kleinere Botnets betrieben und neue Wege gefunden, um mit Opfern auf der ganzen Welt Geld zu machen. Der zunehmende Trend zu gezielten Angriffen zeichnete sich bereits 2005 ab. Diese Bedrohung nimmt weiter zu und wird immer trickreicher. Wir verzeichnen auch eine Bewegung in anderen Kategorien, wie etwa die Zunahme von Spear Phishing", kommentiert Mark Sunner, Chief Technology Officer von MessageLabs, die aktuelle Situation.

Beim Spear Phishing versenden die Phisher echt aussehende E-Mails an sämtliche Angehörigen oder Mitglieder eines bestimmten Unternehmens. Die Nachricht ist so



Postinis umfassender Sicherheits- und Management-Ansatz

aufgesetzt, dass sie vom Arbeitgeber oder von einem Kollegen, zum Beispiel dem IT-Administrator, zu stammen scheint, der eine E-Mail-Nachricht an alle Mitarbeiter des Unternehmens sendet und Benutzernamen bzw. Kennwörter anfragt. Während der traditionelle Phishing-Betrug es auf die Daten einzelner Personen abgesehen hat, soll Spear Phishing den Zugriff auf die gesamten Server und Daten eines Unternehmens ermöglichen.

UTM statt Bauchladen

Solche Bedrohungsszenarien und die Schwierigkeiten mit dem Einsatz komplexer Schutzlösungen erfordern eine neue Sicherheitsphilosophie. „Ein Unternehmen braucht eine Kombination aus mehreren Sicherheitskomponenten wie Virenschutz-Software oder Spam-Filter, um den reibungslosen Ablauf des Geschäftsbetriebes trotz der vielfältigen Angriffe zu gewährleisten, die von einer Firewall allein nicht abgefangen werden können, des Weiteren müssen die einzelnen Komponenten aufeinander abgestimmt sein“, empfiehlt Bernd Bilek, Network & Gateway Security Solution Specialist EMEA von Symantec (www.symantec.de). Abhilfe schaffen integrierte Appliances, die mittlerweile von etlichen Herstellern von Sicherheitslösungen angeboten werden. Appliances sind komplette Lösungen auf einer vorbereiteten Hardware-Plattform mit vorinstallierter Software. Sie können neben der Firewall weitere Komponenten wie Virenschutz, Intrusion Detection/Prevention, Spamschutz, VPN, Content Filtering, Spyware- und Adware Detection und IPSec oder SSL-VPN-Technologien enthalten. Die Platz sparenden Hardware-Boxen enthalten alle benötigten Komponenten wie CPU, Speicher und die entsprechenden Netzwerk-Schnittstellen. Unified Threat Management Appliances nennt IDC solche Lösungen.

Einer der Vorteile der Appliances ist die Vorkonfiguration durch den Anbieter. Die meisten Hersteller bieten mehrere Varianten an, die bereits bei der Auslieferung auf verschiedene Anforderungs-Szenarien zugeschnitten sind. Unterschiede gibt es zum Beispiel in der Art und Anzahl der Netzwerk-Schnittstellen, bei der CPU-Leistung oder bei der installierten Software. Die Komponenten der Appliance sind so aufeinander abgestimmt, dass sie bei der Auslieferung einsatzbereit ist. Nur das Feintuning auf die spezifischen Anforderungen des Unternehmens fehlt noch, was die hausinterne IT erledigen können sollte.

Ein weiterer Vorteil ist, dass Appliance-Lösungen mit dem Unternehmen wachsen. Daher sind sie für Unternehmen jeder Größe geeignet. „Der Einsatz einer Firewall/VPN-Lösung lohnt sich bereits für Unternehmen ab zehn Mitarbeitern“, schätzt Symantec-Sicherheits-Experte Bilek.

Eine gefragte Lösung

Wegen solcher Vorteile verwundert es nicht, dass einige Marktforscher die Nachfrage nach UTM-Appliances stark ansteigen sehen: Eine von Secure Computing (www.securecomputing.de) in Auftrag gegebene Studie kommt zu dem Ergebnis, dass mehr als 60 Prozent der befragten IT-Manager ernsthaft über eine UTM Appliance nachdenken.

Zehn Prozent der befragten IT-Chefs haben bereits ein solches Gerät im Einsatz oder planen, es innerhalb der nächsten zwölf Monate anzuschaffen. Fast die Hälfte zeigte sich im Vergleich zum letzten Jahr eher interessiert an den All-in-One-Geräten. IDC erwartet in den nächsten Jahren einen Boom des UTM-Marktes. Im Jahr 2003 lag der Gesamtumsatz der UTM Appliances noch bei 105 Millionen US-Dollar, bis zum Jahr 2008 soll dieser auf 3,5 Milliarden US-Dollar anwachsen.

Seit Jahren diskutieren die Experten darüber, ob All-in-One-Produkte oder spezialisierte Einzellösungen die bessere Alternative sind. Gemäß der Studie wollen IT-Manager beides: Best-of-Breed-Sicherheitsfunktionen verschiedener Hersteller auf einer einzigen Plattform. Über die Hälfte der Befragten bevorzugt eine Appliance, auf der Technologien von mehr als einem Hersteller gebündelt sind.

Überraschend ist, dass es den meisten IT-Managern bei der Entscheidung für eine UTM Appliance nicht vorrangig darum ging, die Zahl der Produkte verschiedener Sicherheitshersteller im Unternehmen zu verringern. Für nur 38 Prozent war dies ein entscheidendes Kriterium. Für mehr als 70 Prozent der Befragten waren das Management einer Vielzahl von Sicherheits-Funktionen mit einem einzigen Interface, integrierte Sicherheitsreports, die mehrere Sicherheitsfunktionen abdecken, und niedrige Total Costs of Ownership entscheidend.

„Die Studie zeigt, dass Unified Threat Management Security Appliances stark nachgefragt werden. Die Unternehmen suchen nach Best-of-Breed-Lösungen, die in einem Gerät eine Kombination von Hardware, Software und Netzwerk-Technologien sowie verschiedene Sicherheitsfunktionen inklusive Firewall, Intrusion Prevention System (IPS) und Anti-Viren-Lösung kombinieren“, erklärt Frank Kölmel, Sales Director Central and Eastern Europe bei Secure Computing.

Die Grenzen von UTM

Dass moderne Sicherheitslösungen zunehmend miteinander kommunizieren und si-

UTM-ANBIETER IM ÜBERBLICK

Integrierte Sicherheitslösungen als Software Suite oder komplette Appliance im Sinne von Unified Threat Management gibt es von den folgenden Anbietern:

Anbieter	Internet-Adresse
Check Point	www.checkpoint.de
McAfee	www.mcafee.de
Panda	www.panda.de
Secure Computing	www.securecomputing.de
Securepoint	www.securepoint.de
Sonicwall	www.sonicwall.de
SurfControl	www.surfcontrol.de
Symantec	www.symantec.de
Telco Tech	www.telco-tech.de
Trend Micro	www.trendmicro.de
WatchGuard	www.watchguard.de
Websense in Kooperation mit Crossbeam	www.websense.de

cherheitsrelevante Informationen miteinander korreliert werden müssen, lässt sich unter der Flagge nur eines Herstellers auf einer Plattform einfacher realisieren als bei mehreren Herstellern und Systemen. „Auf der anderen Seite sind die derzeit verfügbaren UTM-Lösungen nicht immer in allen Komponenten gleich gut ausgestattet“, weiß Matthias Rosche, Director Consulting der Integralis GmbH (www.integralis.de).

Nicht jeder Hersteller habe in allen technischen Bereichen, die eine UTM-Lösung abdecken muss, die gleiche Erfahrung. Inwieweit UTM-Lösungen einsetzbar sind und welche Lösung zu bevorzugen ist, hängt vom Sicherheitsbedarf, der Bandbreite und der Struktur des Netzwerkes eines Unternehmens ab. Klassischerweise werden solche Systeme deshalb in Unternehmen kleiner bis mittlerer Größe mit wenigen Lokationen und moderaten Sicherheits-Anforderungen eingesetzt. „Wird die Struktur komplexer oder sind spezifische Anforderungen abzubilden oder auch eine hohe Bandbreite sicherzustellen, tendieren Unternehmen heute eher zu einer integrierten Gesamtlösung aus leistungsfähigen Komponenten mehrerer verschiedener Hersteller“, hat Sicherheitsexperte Rosche beobachtet.

Das schätzt Andreas Lamm, Geschäftsführer der Kaspersky Labs GmbH (www.kaspersky.de), ähnlich ein: „UTM hat durchaus eine Berechtigung im Markt, jedoch sollte die Bedeutung auf den gesamten Sicherheitsmarkt nicht überbewertet werden“.

UTM-Lösungen können gerade für solche Unternehmen sinnvoll sein, die kaum eigene Ressourcen in Form von Personal und Finanzmittel für die Administration der Informationssicherheit bereitstellen können. Dieser Mangel ist häufig bei kleineren und mittleren Unternehmen anzutreffen. In diesen Fällen ist eine relativ einfach zu bedienende Lösung ein geeigneter Ansatz.

„Für größere Unternehmen, bei denen das Thema Informationssicherheit mittlerweile auch von der Ressourcenseite her vernünftig ausgestaltet ist, stellt die Kombination verschiedener Lösungen den eindeutig besseren Ansatz dar“, ist Lamm überzeugt.

Durch die Kombination unterschiedlicher Lösungen und Plattformen können Monostrukturen – viele Sicherheitsfunktionen auf einem System – und deren höhere Verwundbarkeiten reduziert werden. Durch die Verteilung der Sicherheit auf unterschiedliche Systeme und Hersteller führt der Ausfall eines Systems nicht zwangsläufig zum Zusammenbruch des gesamten Sicherheitssystems des Unternehmens. Weiter erlaubt der traditionelle Ansatz, dass optimal auf die Sicherheitsbedürfnisse des Unternehmens zugeschnittene Gesamtlösungen greifen, wohingegen UTM-Lösungen immer einen Kompromiss darstellen. Es seien deshalb eine Reihe von Variablen und Faktoren zu berücksichtigen, um herauszufinden, ob eine UTM- oder eine traditionelle Sicherheitslösung für ein Unternehmen der bessere Weg ist. „Dies wussten übrigens auch bereits unsere Vorfahren, sie haben je nach Schutzbedürfnis die Burgen mit mehreren Mauern, Gräben und Wällen versehen“, meint Kaspersky-Geschäftsführer Lamm.

Dass eine UTM-Strategie trotz solcher kritischen Überlegungen auch bei hohen Sicherheitsansprüchen eingesetzt werden kann, zeigt das Beispiel der ONE GmbH mit Hauptsitz in Wien. Das Unternehmen ist mit etwa 900 Mitarbeitern Österreichs drittgrößter Mobilfunk-Betreiber. ONE muss nicht nur das unternehmensinterne Datennetz, sondern auch das externe für seine Kunden vor Viren und Hackern schützen. Als 2004 die bisherige Lösung ersetzt werden musste, entschied sich das Management für die Anschaffung einer Unified Threat Management Firewall von Secure Computing.

Die Lösung basiert auf dem Konzept der Application Defenses: Sie filtert den Datenverkehr bis auf Anwendungsebene, der höchsten Schicht des OSI-Modells. Während reine Paketfilter nur den Umschlag und die Adressierung der Datenpakete überprüfen, sieht eine Firewall mit Application Defenses in das Paket hinein und durchleuchtet einzelne Anwendungen. Die Technik arbeitet mit auf einzelne Dienste (zum Beispiel WWW, E-Mail, Telnet und FTP) spezialisierten Proxy-Servern, die den Verkehr nach einer genauen Analyse an die Zielserver weiterleiten. Die Proxy-Server sind wiederum durch vor- und nachgeschaltete Paketfilter geschützt und befinden sich daher in einem Teilnetz, das auch als demilitarisierte Zone (DMZ) bezeichnet wird.

Zum Sicherungskonzept zählen auch das Sicherheitspersonal für den physischen Objekt- und Personenschutz sowie Richtlinien, die den Mitarbeitern Handlungsweisungen vorgeben und Verantwortliche bestimmen.

Nur noch eine Konsole

Für Unternehmen, die keine komplette Appliance wie bei ONE, sondern nur einen einheitlichen Software-Rundumschutz wol-

KOMMENTAR

Udo Schneider ist Product Marketing Manager bei Trend Micro.

Lösungen, die das Leben vereinfachen

Kleinere und mittlere Unternehmen stehen vor einem Dilemma: Die Gefahr von Bedrohungen steigt dort wesentlich schneller bei einer gleichzeitigen Begrenzung des Handlungsspielraums durch Zeit, Kosten und verfügbare Ressourcen. Der Mittelstand benötigt also Lösungen, die ihm das Leben durch eine weitgehende Automatisierung der Sicherheitsvorkehrungen vereinfachen.

Unified Threat Management (UTM) ist daher sicherlich eine geeignete Security-Strategie für den Mittelstand. Zentrale Verwaltung und einfache Administration sind für kleinere Unternehmen besonders wichtig. Mit eventuell geringen IT-Kenntnissen muss ein Höchstmaß an Sicherheit für die vorhandene IT-Infrastruktur geschaffen werden. In diesem Spannungsfeld ist eine Zwei-Hersteller-Strategie oft nicht die beste Lösung, die von Unternehmen mit über 1000 PC-Arbeitsplätzen häufig vorgezogen wird. Kleinere Unternehmen ohne eigene IT-Abteilung dagegen sind hoch erfreut über eine einfache, umfassende und effiziente Absicherung ihrer PC-Arbeitsplätze. Dies zeigt auch eine Studie von Trend Micro aus dem Jahr 2005.

KOMMENTAR

Igor Levin ist Sales Director bei WatchGuard Technologies.

Ein Mix ist die Regel

Vor allem mittelständische Unternehmen setzen gerne auf Unified Threat Management Appliances. Sie wollen eine Lösung aus einem Guss, die einfach zu warten ist und alle wichtigen Sicherheitsfunktionen beherrscht. Aber vor dem Einsatz sollten sich Unternehmen klarmachen, was für Anforderungen sie stellen und welche Systemvoraussetzungen sie definieren. Es gibt sowohl für UTM-Appliances als auch für Specialized Security Appliances gute Gründe. Welche Lösung besser ist, lässt sich pauschal nicht sagen. In der Praxis zeigt sich, dass in der Regel ein Mix von UTM-Appliance und Specialized Security Appliances in den Unternehmen vorzufinden ist. Der Einsatz erweiterbarer Hardware bewahrt die nötige Flexibilität. Beherrschen UTM-Appliances High-Availability-Konfigurationen, können sie auch den Ausfall eines Systems überbrücken.

len, bietet McAfee mit der *Total Protection Solution* einen neuen Ansatz für die Administration von Sicherheitslösungen an: Alle Teilkomponenten werden mit einer Konsole zusammengefasst und verwaltet. Die *Small Business*-Version lässt sich auf vorhandener Hardware installieren, während die *Enterprise*-Version auch als Appliance lieferbar ist.

Zu deren Leistungsspektrum gehören eine Anti-Viren-Lösung für alle Ebenen des Netzwerks, eine Desktop Firewall, ein Host Intrusion Prevention System sowie Lösungen zur Abwehr von Spyware und Spam. Integriert ist zudem ein vollwertiges Network Access Control System (NAC). Bei allen Versionen verwaltet eine Konsole alle Komponenten. „Die integrierte Sicherheitslösung spart Kosten, schaltet Redundanzen aus und bietet gleichzeitig einen besseren Schutz“, verspricht Kevin Weiss, President von McAfee.

Auch Computer Associates (CA, www.ca.com/de) bietet mit der Software *Integrated Threat Management r8* eine integrierte Lösung zum Schutz der Unternehmes-Netzwerke gegen Malware, Spyware, Rootkits und andere Formen bösartigen Codes an. Die Software wird durch eine zentrale Web-basierende Konsole gesteuert.

Je nach Geschäftsanforderung können Administratoren ihre IT-Umgebung automatisch mit Updates, Patches, Virensignaturen oder Dateien auf den neuesten Sicherheitsstand bringen oder sich den Status der Desktops an eine zentrale Verwaltungskonsole senden lassen und so gewährleisten, dass alle Rechner ein Update erhalten.

Die Lösung unterstützt auch die von Cisco (www.cisco.de) gesponserte Initiative NAC (Network Admission Control), die darauf abzielt, definierte Sicherheits-Richtlinien (Security Policy Compliance) im gesamten Netzwerk zu verankern. Administratoren können die Threat Management Software über Unicenter Software Delivery, Microsoft SMS oder Lösungen von Drittanbietern im Unternehmens-Netzwerk verteilen.

„Ein integrierter Sicherheitsansatz ermöglicht den Unternehmen, das Management von Sicherheitsrisiken an den Geschäftszielen auszurichten“, erklärt Gerhard Beeker, Business Unit Manager Security Management bei CA. Sie könnten damit Sicherheitsrisiken proaktiv identifizieren und beseitigen, bevor sie sich negativ auswirken. Die bloße Implementierung nicht integrierter weiterer Sicherheits-Technologien ist nach Beekers Überzeugung eine vergebliche Strategie, die nur zu mehr Komplexität und geringeren Effekten führt: „Die Lösung lautet besseres Management, nicht mehr Produkte“.

Alternativ auslagern

Für manche Unternehmen kann es interessant sein, das Unified Threat Management nicht selbst zu realisieren, sondern teilweise oder vollständig an einen Managed Security Services Provider auszulagern. Die FIBRO GmbH in Weinsberg bei Heilbronn, Spezialist für Normalien, Rundschalttische und Automation bzw. Robotik, hat diese Strategie für ihren E-Mail-Verkehr gewählt. Die über 1100 Beschäftigten arbeiten in zwei Werken und weltweiten Niederlassungen und Tochterunternehmen.

Vor der Kooperation mit einem externen Dienstleister schützten ein eigener Mail- und SMTP Mailrelay Server, der Virenschutz *Antigen* von Sybari und der Spamfilter *Mail Essentials* von GFI Mailverkehr und Instant Messaging (IM) des Unternehmens. IM ist zwar ein leistungsfähiges Tool zur Steigerung der Unternehmensproduktivität. Doch sein Einsatz ist auch ein Risiko, da es nicht in der gleichen Weise wie E-Mail, Desktop- und Geschäftsanwendungen verwaltet wird. Da IM direkt über das Internet läuft, kann es Würmer schneller als E-Mail verbreiten. Zudem können vertrauliche oder nachteilige Informationen ohne Sicherheits-Checks nach außen gelangen.

Heute scannen die Server von Postini, Inc. (www.postini.de) den kompletten ein- und ausgehenden IM- und Mail-Verkehr nach Viren und filtern Spam heraus. „Entscheidend war der bessere Schutz durch die noch aktuellere Wissensbasis beim Dienstleister, aber auch die Entlastung des eigenen Netzwerks und Mailservers“, erläutert Andreas Grund, IT Administration Netzwerke und Security bei FIBRO. Weil der interne Mail-Server nicht mehr direkt erreicht werden kann, ist das Netz auch vor Denial-of-Service-Attacken geschützt. „Der Administrationsaufwand ist geringer, und durch weniger Spam im Postfach sind die Mitarbeiter zufriedener“, zählt Grund weitere Vorteile auf. Zudem konnte er den bisherigen Mailrelay Server einsparen.

Postini Inc. wurde 1999 gegründet. Der Hauptsitz befindet sich in San Carlos in Kalifornien. Mit Zürich und Genf zählt Postini inzwischen weltweit zwölf Rechenzentren, unter anderem in Santa Clara (Kalifornien), Chicago, London und Amsterdam. Damit scannt der Dienstleister alle Mails seiner Kunden nach Viren und Spam, bevor sie das E-Mail-Gateway am jeweiligen Firmennetz erreichen, zurzeit ca. drei Milliarden E-Mails pro Woche. „Erwünschte E-Mails werden zum Empfänger weitergeleitet, während Spam im Web-basierenden, Passwortgeschützten Postini Message Center unter Quarantäne gestellt wird“, erläutert Kai Gutzeit, Regional Sales Director DACH von

Postini. Wenn eine Firma dies wünscht, erhalten die Mitarbeiter Zugriff auf ihre Quarantäne-Mails und die Möglichkeit, Filter nach ihren eigenen Wünschen einzustellen.

Das Restrisiko

Trotz der unbestrittenen Vorteile einer integrierten Lösung, zum Beispiel in Form einer Appliance, schrecken manche IT-Verantwortliche davor zurück, alles auf ein Pferd zu setzen. Bei einem (selten vorkommenden) Hardware-Defekt der Appliance verliert das Unternehmen auf einen Schlag den kompletten Viren-, Spam- und Hackerschutz.

Auch die Anschaffung einer identischen Reserve-Appliance, die in einem solchen Fall einspringt, bringt keine hundertprozentige Sicherheit. Denn dann läuft auf beiden Appliance-Servern die Software eines Herstellers. Es hat sich gezeigt, dass auch die Software namhafter Anbieter durch fehlerhafte Patches oder Signaturen den Virenschutz und die Firewall längere Zeit ausfallen ließen. Dann nützt auch ein Reserve-Server nichts.

Deshalb minimiert Jürgen Bechtel, Leiter IT-Management bei der Mennekes Elektrotechnik GmbH & Co. KG, das Risiko, indem er es nach dem Best-of-Breed-Ansatz streut. Das Unternehmen produziert im sauerländischen Kirchhundem mit 650 Mitarbeitern genormte industrielle Steckvorrichtungen für Industrie-Netzwerke. Seit Anfang 2003 ist das Zweigwerk im sächsischen Neudorf durch eine Online-Verbindung mit dem Server des Hauptwerkes in Kirchhundem verknüpft. Dadurch können die Produktionsabläufe in beiden Fabriken besser abgestimmt werden. Zudem kann die Fabrikation in Neudorf das im Hauptwerk installierte Warenwirtschaftssystem von SAP nutzen.

„Was die Sicherheit betrifft, haben wir das komplette Schutzkonzept neu gestaltet", berichtet Bechtel. Eine Firewall, eine demilitarisierte Zone (DMZ), ein dreistufiges Virenschutzkonzept und die Signierung der Mails sichern den Datenfluss zwischen Sachsen und dem Sauerland. Die Übertragung erfolgt verschlüsselt und nach außen durch eine VPN-Verbindung geschützt. Auch die Niederlassungen in Italien, Frankreich und Singapur sind so an das Firmennetzwerk sicher angeschlossen.

Der Einsatz einer Appliance ist dem erfahrenen IT-Leiter zu riskant. Bei einem Ausfall wäre die gesamte Produktion im Haupt- und Zweigwerk empfindlich gestört. „Bei unseren Randbedingungen ist mir eine Trennung von Viren-, Spamschutz und Firewall lieber, denn wenn die Appliance aussteigt, haben wir keine Sicherheit mehr", begründet IT-Leiter Bechtel seine Strategie.

Fazit

Ob sie in kleinen, mittleren oder großen Unternehmen eingesetzt werden, eines haben alle Appliances gemeinsam: Sie sind kostengünstiger als einzelne Komponenten und erfordern weniger Aufwand für die Installation und Administration. Und da die Komponenten aufeinander abgestimmt sind, können Firewalls in dieser Kombination optimal ihre Schutzmaßnahmen entfalten. Allerdings gilt auch im Appliance-Verbund: Die Firewall ist nur so gut wie ihre Konfiguration und die Plattform, auf der sie läuft. „Appliances müssen aktualisiert und gepflegt werden, sonst haben Angriffe aus dem Internet trotz High-Tech leichtes

INTERVIEW

Patrick Heinen ist Enterprise Technical Account Manager bei Symantec

Im Gespräch mit Business&IT über die Vorteile von Unified Threat Management für kleine und mittelständische Unternehmen

Business&IT: Welche Vorteile hat nach Ihr Meinung der Einsatz von Unified Threat Management?

Patrick Heinen: Unified-Threat-Management-Lösungen wie zum Beispiel Sicherheits-Appliances bieten gegenüber allein stehenden Produkten zahlreiche Vorteile. Sie enthalten in der Regel integrierte IT-Sicherheitstechnologien wie Virenschutz, Firewall, VPN und Spam-Filter in einer Lösung. Symantec hat bereits sehr früh diese Geräte-Gattung auf den Markt gebracht, weil wir den Bedarf bei unseren Kunden gesehen haben.

Heute geht es in Unternehmen oft nicht mehr darum, in jedem Bereich das beste Produkt auszuwählen, denn das kostet nicht nur mehr Zeit und Geld, sondern ist auch nach dem Kauf deutlich zeit- und arbeitsintensiver. Unternehmen suchen vielmehr nach einer pragmatischen Lösung, die sich schnell und unkompliziert implementieren und betreiben lässt. Und da liegen sie mit einer UTM-Lösung genau richtig.

Die Appliances sind bereits vorkonfiguriert. Das heißt, die einzelnen Technologien arbeiten reibungslos zusammen, sie lassen sich zentral verwalten, der IT-Administrator braucht sich nur mit einer Lösung vertraut zu machen, und er hat einen Ansprechpartner, wenn es Probleme geben sollte. Die Geräte lassen sich auch hochverfügbar auslegen, sodass bei einem Hardware-Defekt für umfassenden Schutz gesorgt ist.

Business&IT: Wie geeignet ist UTM für den Einsatz im Mittelstand?

Patrick Heinen: Gerade kleineren und mittleren Unternehmen empfehlen wir den Einsatz von integrierten Sicherheits-Appliances, und das Angebot wird von Unternehmen dieser Größe auch angenommen. Denn kleine und mittlere Unternehmen haben in der Regel nur wenig IT-Personal und suchen nach kombinierten Lösungen, die sich mit relativ geringem Aufwand verwalten lassen. Spezielle Lösungsangebote für kleinere Unternehmen können zudem preislich deutlich attraktiver sein als Einzellösungen. Bei Symantec gibt es zum Beispiel eine integrierte Appliance für ca. 100 Mitarbeiter bereits für knapp über 1000 Euro.

Spiel“, warnt Symantec-Spezialist Bilek. Auch der vom Hersteller unabhängige Sicherheitsexperte und SySS-Chef Schreiber schätzt UTM. Allerdings bringe UTM als Konzept für die Sicherheit nichts Neues, meint Schreiber: „UTM ist in erster Linie ein Marketing-Begriff für etwas, was es schon länger als Appliance gibt. Alles auf einer Plattform einzusetzen, ist keine neue Idee“. Dem Unternehmer oder dem IT-Verantwortlichen stelle sich wie bei einem Restaurantbesuch die Frage: „Bestelle ich das Tagesmenü oder esse ich à la Carte?“
Wer das Risiko eines Single Point of Failure vermeiden will, weil er sich keine Stillstandzeiten leisten kann, kommt um à la Carte als den Best-of-Breed-Ansatz und eine Mehr-Hersteller-Strategie nicht herum: mit allen Kosten treibenden Folgen nicht nur für die Anschaffungs-, Lizenz- und Wartungskosten, sondern auch für den Personalaufwand. Wer sich einen vorübergehenden Stillstand leisten kann, ist bei einer Appliance gut aufgehoben. Schreiber empfiehlt: „Jeder Firmenchef oder IT-Leiter sollte sich fragen: Wie lange kann ich ohne Außenverbindung bleiben, und wie viel kostet mich das?“ *hey*

INTERVIEW

Lutz Hausmann ist Geschäftsführer der Securepoint GmbH.

Securepoint ist ein international tätiges Unternehmen, das IT-Sicherheits-Lösungen entwickelt und vermarktet.

Business&IT: Wie lautet Ihre Definition von Unified Threat Management (UTM)?
Lutz Hausmann: UTM bedeutet, alle wichtigen Sicherheitsbedürfnisse unter guten Kostengesichtspunkten in einem System zusammenzufassen.
Bei der Auswahl muss man aber sehr aufpassen, denn leider wird von einigen Herstellern UTM ad absurdum geführt. Ein einfaches Beispiel: Ein Intrusion-Detection-System in einer UTM anzubieten ist derzeit nicht nur reines Marketing, sondern sogar ein Sicherheitsproblem. Den Anwendern wird damit eine Sicherheit vorgegaukelt, die es nicht gibt. Abgesehen davon, dass kaum jemand eine IDS-Meldung beurteilen kann, macht man das UTM-System gerade dadurch extrem unsicher, dass es eine aktive Komponente ist. Ein IDS macht derzeit deshalb wenig Sinn auf einer UTM Security Appliance.

Business&IT: Viele Unternehmen fahren stets eine Zwei-Hersteller-Strategie. Einen so genannten Single Point of Failure will niemand ohne Not riskieren. Ist UTM mittels einer Appliance vor diesem Hintergrund ein sinnvolles Angebot?
Lutz Hausmann: Die Antwort auf dese Frage hängt von den jeweiligen Umständen eines Unternehmens ab. Man kann aber definitiv feststellen, dass sowohl verteilte als auch Komplettpakete ihre Berechtigung besitzen. UTM wird landläufig auch etwas abschätzig als die „Eier legende Wollmilchsau“ bezeichnet. Zu Unrecht, denn ein System, das nur die einzige Aufgabe besitzt, Sicherheit zu schaffen, ist schon von seiner Konzeption her wesentlich geeigneter als Einzel-Sicherheitssysteme, die zum Beispiel auf einer Workstation laufen.
Man kann es auch umdrehen: Ein Single Point of Failure ist wesentlich leichter zu beheben oder zu erkennen als Probleme in verteilten Sicherheitssystemen. Denn ihm kann durch geeignete Maßnahmen, zum Beispiel Redundanz, Aktualität und Backup, wesentlich einfacher vorgebeugt werden.
Grundsätzlich kann man davon ausgehen, dass eine Sicherheit von 90 bis 95 Prozent für jedes Unternehmen bezahlbar ist. Sobald man aber darüber hinausgehen will oder muss, kostet jeder Prozentpunkt mehr fast genauso viel wie alle Maßnahmen davor. Man muss also gegeneinander abwägen, welche Sicherheitsbedürfnisse man hat, ob Maßnahmen realisierbar sind und was es kostet.

Business&IT: Eignet sich UTM für den Einsatz im Mittelstand?
Lutz Hausmann: Fast alle mittelständischen Unternehmen haben das Problem, dass ihre EDV-Fachkräfte so viel in ihrem Tagesgeschäft zu tun haben, dass die Sicherheit darunter leidet und sie nicht genug Zeit haben, sich entsprechend weiterzubilden. Außerdem haben wir sehr oft mit einer Situation zu tun, dass Netzwerk-Kenntnisse zu wenig ausgeprägt sind. Die Hersteller müssen also Produkte im Portfolio haben, die es trotzdem erlauben, ein hohes Maß an Sicherheit zu gewährleisten.
Deshalb muss hier ein klares Ja zu UTM gegeben werden, in der Regel ist ein kleines bis mittleres Unternehmen bei UTM sehr gut aufgehoben. Sobald aber die Sicherheitsbedürfnisse oder die benötigten Durchsatzraten höher sind, kommt man um verteilte Sicherheitssysteme nicht herum.
UTM bedeutet Einheitlichkeit, alle wichtigen Sicherheitsbedürfnisse werden durch eine Lösung erfüllt, und das unter guten Kostengesichtspunkten. Viele Unternehmen haben das aber noch nicht erkannt, da sie sich aus Zeitgründen nicht umfassend genug über den Markt informieren können oder auch, weil sie nicht ausreichend beraten werden. Das ändert sich aber zurzeit, und deshalb werden diese Produkte in Zukunft eine hohe Bedeutung erlangen.

Business&IT: Was bietet Securepoint an?
Lutz Hausmann: Securepoint bietet eine inzwischen sehr verbreitete UTM-Lösung für kleine und mittlere Unternehmen an, die praktisch alle wichtigen Sicherheitsbedürfnisse wie Firewall, VPN, Content-Filter, Virenscanner, Spam-Filter, Authentisierung, Quality of Service (QoS) und mehr abdeckt. Übrigens wurde die Securepoint Security Appliance gerade von den Lesern zweier namhafter Fachzeitschriften zum Produkt des Jahres 2006 gewählt.