

Astaro OrangePaper

Unified Threat Management auf dem Prüfstand

Der Weg durch den Angebotsdschungel

Autor:



Angelo Comazzetto
Produkt-Manager

Datum:

24.07.2009

Inhalt	Seite
Einleitung	2
Vorteile von Unified Threat Management	2
Produktangebot im Markt	3
Technologische Unterschiede	3
Einheitliches Management	4
Funktionstiefe	4
Beispiel Spam-Schutz	5
Beispiel URL-Filter	6
Mit den Anforderungen wachsen	7
Ein einfaches Lizenzmodell	7
Bedienungsfreundlichkeit	8
Stichpunkt Geschwindigkeit	10
Fazit	10

Einleitung

Lösungen für Unified Threat Management (UTM) haben in den vergangenen Jahren einen regelrechten Boom erlebt. Trotz schwächelnder Wirtschaft verzeichnet der Markt für Sicherheitslösungen aus einer Hand ein kontinuierliches Wachstum, und das Konzept, mehrere Sicherheitsfunktionen auf einer technologisch einheitlichen Plattform mit grafischer Benutzeroberfläche zusammenzufassen, wird immer populärer. Angesichts eines steigenden Wettbewerbsdruckes verfeinern die etablierten Anbieter regelmäßig ihr Produktangebot, während gleichzeitig neue Startup-Unternehmen fast täglich mit ihren eigenen UTM-Lösungskonzepten auf dem Markt kommen. Nie gab es mehr Wahlmöglichkeiten für den Kunden, was die Auswahl der richtigen Lösung natürlich auch erschweren kann. Denn die Produktvielfalt fordert ihren Tribut. Das Geringe auf dem im Jahr 2008 insgesamt drei Milliarden US-Dollar schweren Markt resultiert in einer unübersichtlichen Anzahl an Herstellerangeboten mit unterschiedlichster Funktionalität, Performance und Ausstattung. Dieses OrangePaper beschreibt, wie sich die unterschiedlichen Produktangebote einordnen lassen, was sich hinter den im Sicherheitsmarkt üblichen Begriffen verbirgt, damit Ihnen alle Informationen zur Verfügung stehen, um die für Ihr Netzwerk am besten geeignete Lösung zu finden.

Vorteile von Unified Threat Management

Vorteile einer einheitlichen Technologieplattform

Die Konsolidierung vieler Netzwerksicherheitsprodukte im Rahmen einer einheitlichen Appliance hat bekanntermaßen viele Vorteile. Auf Effizienz getrimmte UTM-Lösungen ersparen naturgemäß zeitaufwendige Administrationsarbeiten, wie sie für Einzelprodukte typisch sind, bei denen sich Administratoren mit mehreren Management-Oberflächen zurechtfinden müssen, die alle ein eigenes Fachvokabular und Produktdesign zugrunde legen. Firmware- und Versions-Updates müssen bei Einzellösungen regelmäßig eingespielt und daraus resultierende Neukonfigurationen per Hand durchgeführt werden, um das fehlerfreie Zusammenspiel der Produktfunktionen innerhalb der gesamten Sicherheitsumgebung zu gewährleisten. Durch eine steigende Anzahl an Sicherheitsprodukten wird darüber hinaus die Fehlersuche im Netzwerk ungleich komplizierter, da es viel mehr Möglichkeiten für Fehlkonfigurationen oder Systemkonflikte gibt und sich der Arbeitsaufwand für den Administrator bei der Problemlösung deutlich erhöht. Rechnet man die versteckten Lizenzkosten für Support, Wartung und Updates hinzu, die für jede zusätzliche Lösung neu anfallen, lohnt sich der Einsatz vieler Einzelprodukte finanziell gesehen sogar noch weniger.

Unified-Threat-Management-Lösungen dagegen können durch eine einheitliche grafische Administrationsoberfläche punkten, verursachen keine doppelten Lizenzgebühren und vereinfachen die Identifizierung von Systemkonflikten. Hinzu kommt, dass die Applikationen einer UTM-Appliance aufeinander abgestimmt sind und sich gegenseitig ergänzen, wodurch der Vorteil einer integrierten Systemarchitektur voll zur Geltung kommt. Eine UTM-Appliance kann zum Beispiel VPN-Verbindungen, die Mitarbeiter unterwegs über IPSec oder SSL aufbauen, nicht nur an zentraler Stelle entschlüsseln, sondern zugleich per Intrusion-Protection-System nach Sicherheitskriterien filtern. Dieser Ansatz ist gegenüber Einzellösungen deutlich überlegen, die in der richtigen Reihenfolge angeordnet werden müssen und eine aufwendige Konfiguration mit komplexen Routing- und Traffic-Regeln erfordern, um die korrekte Arbeitsweise aller eingesetzten Filter zu gewährleisten.

Produktangebot im Markt

Auf den ersten Blick ähneln sich UTM-Produkte

Auf den ersten Blick ähneln sich moderne UTM-Lösungen bei der Ausstattung, Funktionalität und Gesamtkonzeption. Nahezu alle Hersteller kombinieren verschiedene Einzellösungen von Drittanbietern, proprietäre und Open-Source-Technologien in einem Gerät und bewerben dieses als umfangreichste oder vollständigste „Best-Of-Breed“-Lösung mit allen Funktionen oder einfach nur als „All-in-One“. Die existierenden Einzellösungen wurden allerdings für einen ganz bestimmten Zweck entwickelt, beschränken sich in der Regel auf einen bestimmten Anwendungsbereich und verfügen deshalb auch über bestimmte Zusatzfunktionen und eine dedizierte Hardware-Plattform, die für eine ganz bestimmte Umgebung konzipiert wurde. Für eine effektive Kombination dieser Einzellösungen auf einer einheitlichen Plattform muss diese nicht nur ausreichende Geschwindigkeitswerte aufweisen, sondern auch eine adäquate Funktionalität in den unterschiedlichsten Umgebungen zur Verfügung stellen können, um bisher eingesetzte Geräte ersetzen und zukünftige Anforderungen erfüllen zu können.

Technologische Unterschiede

Worauf sollte man achten?

Die bloße Aneinanderreihung verschiedener Einzelfunktionen, wie sie häufig praktiziert wird, ist jedoch nur von geringem Wert, wenn nicht gleichzeitig alle Funktionen in einem einheitlichen Management-System integriert werden, ohne dass die Gesamtlösung zu komplex oder bedienungsfeindlich wird. Genau an diesem Punkt zeigen viele UTM-Lösungen deutliche Schwächen.

Einheitliches Management

*Zusammenfassen, nicht
aneinanderreihen*

Ein Hauptaugenmerk bei der Auswahl eines UTM-Produkts sollte daher auf dem Management liegen. Ist die Bedienungsoberfläche ausgefeilt und klar strukturiert? Ist die Benutzerführung einfach und verständlich damit die Benutzer in kürzester Zeit alle sicherheitsrelevanten Einstellungen durchführen können? Dabei geht es in erster Linie nicht darum, ob einem das Menüdesign der Benutzerschnittstelle zusagt, sondern ob alle Funktionsbereiche der Lösung nahtlos integriert sind. Viele UTM-Plattformen leiden darunter, dass die verschiedenen Module nicht vernünftig implementiert und nicht richtig miteinander verknüpft sind. Bei der Implementierung eines einfachen Webfilters kommt es zum Beispiel häufig vor, dass viele verschiedene Bereiche der Plattform unabhängig voneinander konfiguriert werden müssen. So muss z.B. der Content Filter aktiviert und richtig konfiguriert sein, aber zugleich auch andere UTM-Module so eingerichtet werden, dass sie mit dem Content-Filter zusammenarbeiten. So kann es z.B. nötig sein, den Paketfilter zu öffnen, Masquering-Regeln festzulegen oder den Download von Anti-Viren-Updates zu erlauben. Im Gegensatz dazu versetzt ein ausgereiftes UTM-Produkt den Administrator in die komfortable Lage, dass sich das Komplettsystem automatisch konfiguriert, sobald er den Content Filter an zentraler Stelle aktiviert.

Es ist also wichtig, dass moderne UTM-Lösungen über eine Vielzahl an Werkzeugen verfügen und es kommt darauf an, wie die Applikationen miteinander kombiniert werden und welche grafische Benutzeroberfläche zum Einsatz kommt. Noch wichtiger ist allerdings, wie funktionsreich und effektiv jedes Einzelfeature bei der Problemlösung in jedem Aufgabenbereich ist. Es kommt also auf die Funktionstiefe an.

Funktionstiefe

Funktionen unter der Lupe

Für die Beurteilung einer UTM-Lösung kommt es nicht nur darauf an, dass die gewünschten Funktionsbereiche im Datenblatt aufgelistet sind, sondern die integrierten Funktionen müssen genauestens unter die Lupe genommen werden. Beim Autokauf verhält man sich schließlich auch nicht anders und zieht neben dem Endpreis auch andere Aspekte wie die Qualität des Motors, unabhängige Pannenstatistiken und den durchschnittlichen Benzinverbrauch mit ins Kalkül ein. Und natürlich gibt es auch große Unterschiede zwischen den UTM-Lösungen, wenn man die Qualität der integrierten Komponenten einmal genauer untersucht.

Viel zu oft trifft man auf Lösungen, die bestimmte Produktfeatures nur rudimentär implementiert haben, was sich dann zwar in den Marketingbroschüren gut liest, aber in der Praxis als unbrauchbar erweist, wenn man die betreffen-

den Komponenten einem Vergleich mit dem direkten Wettbewerb unterzieht. Die folgenden beiden Kapitel beschreiben einige Beispiele, wie Features, die zunächst hinsichtlich ihrer Bezeichnung und Funktionalität ähnlich erscheinen, sehr starke Unterschiede aufweisen, wenn man ihre Funktionsweise und Leistungsmerkmale einem Realitätstest unterzieht.

Beispiel Spam-Schutz

Nicht alle E-Mail-Filter sind gleich aufgebaut.

Spam-Schutz lässt sich auf Basis unterschiedlicher Ansätze und Technologien umsetzen, auch wenn gegenüber dem Kunden nur lapidar die Rede von einem „Spam-Filter“ oder „Email-Scanner“ ist. Ein möglicher Ansatz ist zum Beispiel die Nutzung von RBL-Technologie („Real-Time Blackhole List“), die Absender-Adressen bekannter Spam-Versender verwendet. Allerdings wird eine Filterlösung kläglich scheitern, wenn sie vorwiegend auf dieser Basis unerwünschte E-Mails blockieren will, da es sich um einen rein reaktiven Ansatz bei der Spam-Bekämpfung handelt. Denn Spammer benutzen selten die gleiche Absenderadresse, da sie schnell identifiziert und im Rahmen statischer Erkennungslisten aufgelistet werden können, um zukünftige Zustellungsversuche unterbinden zu können. Obwohl dieser Ansatz also nur bedingt für einen effektiven Spam-Schutz geeignet ist, integrieren viele Anbieter nur diesen Minimalschutz, um im Rahmen ihrer Verkaufsstrategie vorgeben zu können, dass ihr Produkt „Email-Filterung“ oder „Anti-Spam-Funktionalität“ bietet.

Im Gegensatz dazu kombinieren qualitativ hochwertige Email-Filter mehrere Erkennungstechnologien, die leistungsstark genug sind, um sich mit dedizierten Email-Filterlösungen messen zu können. Ein sehr effektiver Ansatz der führenden Email-Filter ist beispielsweise, die explosionsartige Verbreitung neuer Spam-Nachrichten genauso zu behandeln wie einen Virenausbruch auch. Dafür beobachten und analysieren spezielle Systeme innerhalb der großen ISP-Backbones permanent den weltweiten E-Mail-Verkehr, kennzeichnen erkannte Spam-Mails automatisch und leiten entsprechende Fingerprints an zentrale Datenbanken weiter. Hierdurch lassen sich neue Spam-Wellen in Sekundenschnelle erkennen und an die Email-Filter der verteilten UTM-Lösungen kommunizieren. In Kombination mit herkömmlichen, inhaltsbasierten Filtermechanismen kann so eine sehr leistungsstarke Email-Filterlösung zur Verfügung gestellt werden. Funktionstiefe als Unterscheidungsmerkmal bedeutet in diesem Fall, dass zwei Produkte zwar einen „Email-Filter“ anbieten, der Effizienzgrad beider Lösungen aber vollkommen unterschiedlich ist, was die Bekämpfung der Spam-Problematik betrifft.

*Moderne URL-Filter bieten
völlig neue Möglichkeiten*

Beispiel URL-Filter

URL-Filter sind ebenfalls ein Beispiel dafür, wie unterschiedlich Lösungsansätze aussehen können. Die zahlreichen, auf dem Markt als Web/URL-Filter verfügbaren Produkte versprechen alle, das grundlegende Problem lösen zu können, wie sich der Zugriff auf erwünschte und unerwünschte Web-Seiten kontrollieren lässt, um ethischen, sicherheitstechnischen und juristischen Risiken aus dem Weg zu gehen. Während einige Lösungen nur minimale Funktionalität aufweisen, sind andere Produkte wiederum so komplex, dass umfangreiche Schulungen oder sogar Umstrukturierungen des Netzwerks erforderlich sind. Einige UTM-Lösungen verfügen über einen „Web-Filter“, der lediglich aus einer Black-/Whitelisting-Komponente besteht, um per Hand URL-Listen mit erlaubten und blockierten Webseiten zu erstellen. Der Effizienzgrad ist hier natürlich aus Unternehmenssicht sehr niedrig, denn das Internet verändert sich viel zu schnell, um alle betreffenden Webseiten erfassen zu können. Deutlich effektiver ist es, Webseiten automatisch verschiedenen Kategorien zuzuordnen, um Zugriffsversuche anhand der jeweiligen Klassifizierung steuern zu können. Aber auch hier arbeiten die verfügbaren Lösungen unterschiedlich effektiv. Einige UTM-Lösungen sortieren Hunderttausende gespeicherte Seiten in einer überschaubaren Anzahl an Kategorien auf dem Sicherheitssystem, die in regelmäßigen Zeitabständen über das Internet aktualisiert werden. Gegenüber der manuellen URL-Verwaltung ist das zwar ein Schritt in die richtige Richtung, aber trotzdem ist eine solche Implementierung vom Ansatz und Leistungsumfang her begrenzt.

Im Gegensatz dazu greifen die Marktführer auf einen riesigen Datenbestand klassifizierter Webseiten zu, die auf zentralen, über redundante Hochgeschwindigkeitsleitungen angebotenen Servern einen Milliardenbestand klassifizierter Seiten in dutzenden Kategorien vorhalten. Dieser Ansatz ist noch attraktiver, wenn die UTM-Appliances im laufenden Betrieb auch bisher nicht klassifizierte Seiten in Echtzeit zwecks Klassifizierung an die globale Datenbank weiterleiten können, um den Datenbestand kontinuierlich zu verbessern. Führende Lösungen ermöglichen es dem Administrator auch, die Filtermethode einfach umzudrehen, d.h. bei Bedarf zunächst alle Seiten zu blockieren und nur bestimmte Kategorien und aufgelistete URLs zuzulassen, um so den Administrator von der permanenten Filter-Feinjustierung und Überprüfung anhand von Reports zu entlasten.

Funktionstiefe als Unterscheidungsmerkmal bedeutet in diesem Fall, dass nicht nur mehr Möglichkeiten, sondern ganz neue Managementvarianten für den „URL/Webfilter“ einer UTM-Appliance verfügbar sind.

Wählen Sie eine UTM-Plattform, die mit Ihrem Unternehmen wächst.

Mit den Anforderungen wachsen

Weitere Schlüsselfunktionen einer UTM-Lösung betreffen Upgrade-Möglichkeit und Skalierbarkeit, um auf zukünftige Anforderungen vorbereitet zu sein. Der Sicherheitsmarkt verändert sich angesichts immer neuer Herausforderungen, denen die Hersteller mit neuen Werkzeugen, Produktversionen, Updates, Technologien und IT-Plattformen begegnen. Häufig wird der Wert skalierbarer Lösungen, die auf zukünftige Entwicklungen vorbereitet sind und dadurch für Investitionsschutz sorgen, unterschätzt. Die einfache automatisierte Aktualisierung der Produkt-Firmware auf die neueste Herstellerversion ist ein handfester Vorteil. Ein wichtiges Unterscheidungskriterium ist auch, ob sich die Leistungsstärke eines Systems erhöhen lässt, um zusätzliche User in die Sicherheitsumgebung einzubinden, und ob sich weitere Funktionen aktivieren lassen, wenn das im Rahmen des Unternehmenswachstums erforderlich wird. So ist es zum Beispiel sehr hilfreich, wenn weitere Appliances bei Bedarf zu einem Cluster-Verbund addiert werden können und automatisch die Gesamtlast ohne externe Loadbalancer auf alle Cluster-Einheiten verteilt wird. Die effektivsten Lösungen erlauben eine vollkommen dynamische Erweiterung eines Clusters im laufenden Betrieb und sorgen außerdem für Ausfallsicherheit und Hochverfügbarkeit im Rahmen eines Active/Active Clusters. Flexible Erweiterungsmöglichkeiten zahlen sich spätestens dann aus, wenn man bei steigenden Leistungsanforderungen nicht auf eine größere Hardware-Plattform wechseln muss, sondern sukzessive auch kleinere Upgrade-Schritte gehen kann.

Lesen Sie das Kleingedruckte.

Ein einfaches Lizenzmodell

Lizenzmodelle für UTM-Produkte sind oft komplex und sehr unterschiedlich aufgebaut. Obwohl einige Hersteller damit werben, dass ihre Hardware-Appliances unbegrenzte Benutzerzahlen zulassen, ist das jedoch selten tatsächlich der Fall. Früher war es häufig so, dass sich die Produktlizenzierung von Sicherheits-Appliances — wie bei reinen Softwarelösungen auch — nach der Anzahl gleichzeitig aktiver Benutzer bzw. IP-Adressen richtete. Mehrere Jahre lang war das die übliche Praxis, aber der Markt verlangte nach Veränderungen, hauptsächlich weil UTM-Appliances immer mehr unterschiedliche Funktionen integrieren. In einem Unternehmen wird zum Beispiel die „Box X“ eingesetzt, um sie als Firewall und VPN-Endpunkt für einige mobile Benutzer einzusetzen. In einem anderen Unternehmen wiederum ist die gleiche „Box X“ in voller Funktionalität mit E-Mail-, Web-, VPN- und IPS-Schutz und anderen Features im Einsatz. Beide nutzen das gleiche Produkt, aber der eine Kunde erreicht für mehr IP-Adressen eine effektive Filterung, während der andere

Kunde aufgrund der zusätzlich eingesetzten Funktionen früher an die Kapazitätsgrenzen der Hardware stößt. Bei den leistungsfähigsten und ausgefeiltesten UTM-Appliances stoßen Benutzer nicht an künstlich gesetzte Grenzen; die Hardware-Ressourcen sind bei der Prozessor- und Speicherkapazität so ausgelegt, dass alle Funktionen auch bei vollem Betrieb in ihrer Klasse zur Verfügung stehen, ehe sich ein Upgrade oder die Ankoppelung eines Zusatzgerätes im Cluster-Verbund empfiehlt.

Einige Unternehmen verwenden eine recht undurchsichtige Methodik, wie die pro Benutzer zugeteilten Ressourcen begrenzt oder lizenziert werden und definieren die User-Lizenz anhand der IP-Adresse, MAC-Adresse oder anderer Faktoren. Ein typisches Beispiel ist, dass mit einer „unbegrenzten Benutzerzahl“ geworben wird, aber die Anzahl gleichzeitiger Verbindungen eingeschränkt bleibt. In der Realität schützt die Box also nur eine bestimmte Anzahl an Usern, aber der Werbeslogan einer unbegrenzten Benutzerzahl kann trotzdem aufrecht erhalten werden. Andere Hersteller nutzen Bandbreitenbeschränkungen, um effektiv den maximalen Durchsatz einer Lösung zu limitieren, zum Beispiel durch Begrenzung des Internet-Uplinks (WAN) auf 1 Megabit pro Sekunde.

Ähnlich gelagert sind Fälle, bei denen eine bestimmte Funktionalität nur für die größeren Modell-Versionen einer UTM-Produktpalette verfügbar ist. Manche Anbieter beschränken manche Features, die im Markt gerade besonders gefragt oder neu sind, auf teurere Versionen oder aber sie verkaufen zur Umsatzsteigerung spezielle Lizenz-Codes, die zusätzlich erworben werden müssen. Zur Vermeidung von versteckten Zusatzkosten ist es also ratsam, beim Kauf der „UTM-Version 1000“ darauf zu achten, dass die eigentlich erwünschte Funktionalität nicht „UTM-Version 1000-C“ erfordert. Ein einfaches Produkt-Lizenzmodell erhöht dagegen die Wahrscheinlichkeit, dass der Kunde tatsächlich die für seine Anforderungen passende Lösung erwirbt.

Bedienungsfreundlichkeit

„Bedienungsfreundlichkeit“ rechtzeitig testen

Bei vielen Anbietern ist „Ease-of-use“, also einfache Bedienbarkeit, ein oft verwendeter Ausdruck. Im Kern geht es dabei um die Botschaft an potentielle Käufer, dass die Lösung über eine grafische Benutzeroberfläche, die heutzutage zum UTM-Standardumfang gehört, intuitiv administrierbar ist. Allerdings behauptet jedes Produkt, dass es in puncto „Bedienungsfreundlichkeit“ anderen Produkten deutlich überlegen sei. Der entwicklungsstechnische Reifegrad eines Produktes lässt sich jedenfalls schnell ermitteln, wenn man das Produktversprechen anhand einiger Screenshots oder einer Online-Demo oder vielleicht auch einer Testinstallation auf seine Richtigkeit überprüft. Die Unter-

schiede bei der Benutzerfreundlichkeit unterschiedlicher UTM-Lösungen treten deutlich zu Tage, wenn man das Layout der grafischen Benutzeroberfläche und die Anordnung der einzelnen Aufgabenbereiche auf Administratorebene beurteilt. Sind häufig genutzte Funktionen auf dem Bildschirm gut positioniert und beschränkt sich der Einsatz der Strg- oder Alt-Taste, von Rechtsklicks und anderen versteckten Befehlen auf ein vertretbares Maß, finden sich Administratoren schnell zurecht und müssen nicht proprietäre Sonderbefehle erlernen.

Naturgemäß ist es ohnehin eine subjektive Einschätzung, ob ein Produkt einfach bedienbar ist, variiert also von Benutzer zu Benutzer. Im Formel-1-Sport beispielsweise sind die hoch geschulten und erfahrenen Rennfahrer an die komplexe Steuerung der Boliden gewöhnt. Nur die Fahrrelite hat einen solchen Rennwagen unter Kontrolle, auch wenn es sich technisch gesehen lediglich um ein Automobil mit vier Rädern, Lenkung, Brems- und Gaspedal handelt, die eigentlich jeder Erwachsene kennt. Auch die neueste Generation der UTM-Lösungen weist viele Gemeinsamkeiten auf, verfügt im Regelfall über eine grafische Benutzeroberfläche mit ähnlicher Aufteilung, angeordnet nach Aufgabenbereichen mit Drop-Down-Menüs und Auswahlboxen. Die besten/neuesten Lösungen integrieren bereits typische Web-2.0-Funktionalität wie zum Beispiel AJAX-Technologie, die Benutzern eine schnelle Steuerung und eine zielgerichtete Konfiguration ermöglichen, ohne dass man dafür Expertenwissen über die jeweilige Technologie benötigt. Verwenden UTM-Lösungen dagegen immer noch Kommandozeilen, arbeiten mit client-basierten Management-Zusatzprogrammen oder benötigen sie für die Konfiguration unterschiedlicher Aufgabenbereiche sogar mehrere vollständig separate GUI-Umgebungen, empfiehlt sich der Wechsel auf vernünftig strukturierte Produkte, bei denen die Bedürfnisse des Users im Vordergrund stehen und die Technologie an die Konfigurationsabläufe angepasst ist.

Probieren geht (auch beim Kauf) über studieren

Bei der Produktevaluierung ist es ratsam, UTM-Lösungen im Rahmen einer Produktdemonstration näher kennenzulernen und sich die Bedienung des GUI in der Praxis zeigen zu lassen; alternativ kann man sich das System auch zu Testzwecken schicken lassen. Ein aussagekräftiger Aspekt ist dabei, welche Konfiguration ab Werk voreingestellt ist. Falls erst umfangreiche Konfigurationsarbeiten erforderlich sind, um das Produkt mit internen Sicherheitsrichtlinien in Übereinstimmung zu bringen, steigt das Risiko für Fehlkonfigurationen rapide – im Gegensatz zu Appliances, die in einem vollständig „abgesicherten“ Zustand ausgeliefert werden und nur Kommunikationspfade mit der Außenwelt öffnet, die explizit freigeschaltet wurden.

Stichpunkt Geschwindigkeit

Vorsicht bei den angegebenen Werten.

Die veröffentlichten Performance-Werte von UTM-Produkten sind für Kunden häufig verwirrend. Jeder Anbieter verwendet seine eigenen Richtwerte über die Leistungsfähigkeit des Produktes und die Bemessungsgrundlage ist dementsprechend unterschiedlich.

Es ist unmöglich, die Leistungsfähigkeit eines UTM-Produkts anhand einer einzelnen Zahl darzustellen. Wie in der Automobilindustrie auch haben Kunden unterschiedliche Anforderungen, was Geschwindigkeit, Zuverlässigkeit, Handhabung und Sicherheit betrifft. Zwar sind viele Angaben in Datenblättern und Marktübersichten nicht wirklich falsch, aber sie geben auch nur den Bestfall in einer bestimmten Kategorie wieder. Beispiel „E-Mail-Durchsatz für SMTP“: Wird hier ein Wert von 120.000 Nachrichten pro Stunde angegeben, muss man zugleich wissen, dass ein solches Ergebnis von mehreren Faktoren wie der Dateigröße gescannter Nachrichten, der getesteten Zeitdauer für Versand und Empfang von E-Mails sowie der Art und Weise abhängig ist, wie gefilterte Nachrichten aussortiert oder akzeptiert werden. Hochentwickelte Antispam-Verfahren geben beispielsweise viele Spam-Botschaften gar nicht erst an die Content-Scanner weiter, wodurch sich die Zahl der E-Mails, die alle Filterkomponenten durchlaufen, auf einen Bruchteil der vom UTM-Gateway erfassten Gesamtnachrichten reduzieren kann. Deshalb können die beworbenen Angaben für den Datendurchsatz bei gleicher Leistung stark variieren.

Durchläuft darüber hinaus die gleiche Lösung zwei verschiedene Testszenarien, kann es zu erheblichen Unterschieden beim Durchsatz kommen, je nachdem, ob man in Szenario eins den E-Mail-Filter samt aller verfügbaren Filteroptionen eingeschaltet hat oder in Szenario zwei nur eine einzelne Filter-Engine mit entsprechend reduziertem Ressourcenverbrauch aktiv ist. Addiert man dementsprechend auch noch die vielen anderen Kombinationsmöglichkeiten einer UTM-Appliance, vom VPN-Gateway bis zum Web-Filter, erhält man noch unterschiedlichere Geschwindigkeitswerte als Testergebnis.

Fazit

Löst das ausgewählte Produkt Ihr Problem?

Die oben angeführten Unterscheidungskriterien können sicherlich nur erste Ansatzpunkte für die Auswahl der richtigen Unified-Threat-Management-Lösung sein. Dafür ist der Markt für Sicherheitsprodukte mit einer Vielzahl an Anbietern in diesem Segment einfach zu unübersichtlich, ganz zu schweigen von der schier unendlichen Liste an Produkten und Features, so dass es in der Regel geschulten IT-Sicherheitsexperten vorbehalten bleibt, die Funktionsvielfalt einer Lösung mit den gefragten Systemanforderungen im Unternehmensnetzwerk in Übereinstimmung zu bringen. Häufig ist man als Kunde vom An-

gebot an UTM-Lösungen einfach überfordert, muss die technischen Fachbegriffe, Werbeversprechen und Leistungskataloge erst einordnen, um sich bei der Problemlösung auf die Kernfragen zu konzentrieren. Dabei hilft es, das Anforderungsprofil der gesuchten UTM-Lösung festzulegen, bevor man die für diesen Fall passenden Appliance mit entsprechend attraktivem Preis-Leistungsverhältnis auswählt.

Das vorgelegte Marketing- und Zahlenmaterial ist bei dieser Suche zumeist eher ablenkend. Stellen Sie sicher, dass Sie das Lizenzierungsmodell komplett verstanden haben und dass Sie flexible Upgrade-Möglichkeiten haben, um eine größtmögliche Investitionssicherheit für die UTM-Lösung zu erreichen. Achten Sie genau auf den Leistungskatalog des Produktes, um sicherzustellen, dass Sie den richtigen Grad an Funktionsvielfalt und -tiefe haben, um die Problemstellungen auch lösen zu können und nicht nur über eine Vielzahl an Features zu verfügen. Und natürlich sollten Sie sich ausreichend Zeit nehmen, um die Benutzeroberfläche der in Frage kommenden Lösung kennenzulernen, damit Sie Menüstruktur und Benutzerführung einordnen können.

Astaro's Produktangebot erfüllt Ihre Anforderungen

Für die Astaro AG ist es das erklärte Ziel, die Auswahl der richtigen UTM-Lösung zu vereinfachen. Seit acht Jahren vermarktet Astaro eine eigene Lösung und bietet die UTM-Appliance Astaro Security Gateway (ASG) sowie eine Reihe weiterer Produkte rund um das Thema Netzwerksicherheit an. Astaro stellt alle Features auf jeder ASG-Version zur Verfügung und mit Ausnahme der kleinsten Produktvariante werden auch alle Hardware-Appliances mit unbegrenzter Lizenzierung ausgeliefert. Astaro-Appliances sind daher im Unternehmensnetzwerk flexibel einsetzbar und der Administrator kann bedarfsgesteuert den Aufgabenbereich von Astaro Security Gateway im Laufe der Zeit erweitern, um dadurch andere Lösungen im Netzwerk zu ersetzen. Beim Produktdesign hat Astaro von Anfang an die Bedürfnisse der Administratoren und Benutzer berücksichtigt, damit alle benötigten Funktionen auch ohne umfassendes Wissen im Sicherheitsmarkt nutzbar sind. Der Astaro-Ansatz, Produktwünsche der Partner und Kunden direkt in die Entwicklung einzubeziehen und dadurch unmittelbaren Mehrwert zu generieren, sorgt für einen deutlichen Wettbewerbsvorsprung. Mit Astaro Security Gateway können Administratoren leistungsstarke Features mit wenigen Mausklicks aktivieren und ersparen sich umfangreiche Schulungen zum Erlernen der Funktionsweise. Das Produkt ist als Hardware- und Software-Appliance verfügbar, kann darüber hinaus im Rahmen einer Virtualisierungsplattform wie VMWare eingesetzt werden. Das ist besonders interessant für Unternehmen, die ihre eigene Virtualisierungsstrategie verfolgen oder die Astaro-Technologie im virtuellen Umfeld testen wollen. Ein Alleinstellungsmerkmal im Sicherheitsmarkt ist auch, dass

Astaro die volle Funktionalität der UTM-Lösung für Heimanwender mit einer kostenlosen Lizenz für bis zu zehn IP-Adressen zur Verfügung stellt. Benutzer können diese als ISO-Datei von der Astaro-Webseite herunterladen, auf ihrem Computer installieren und alle Funktionen (einschließlich des SSL VPN-Clients) zum Schutz ihres Heimnetzwerks gegen Viren und Spyware nutzen, Web Security einsetzen, E-Mails filtern und VPN-Tunnel zu anderen Lösungen aufbauen.

Mit Astaro Security Gateway von "UTM" zu "XTM"

Appliances aus dem Hause Astaro haben sich nicht nur in Deutschland zum Marktführer entwickelt, sondern zählen weltweit zu den führenden Sicherheits-Gateways. Angeregt durch die Fülle der Sicherheitsfunktionen von Astaro Security Gateway und ihrer tiefen, wohldurchdachten Integration hat das Marktforschungsunternehmen IDC Mitte 2008 ein neues Marktsegment für „eXtensible Threat Management“ (XTM) Security-Plattformen definiert. Laut IDC übertreffen XTM-Plattformen die gängigen UTM-Sicherheitslösungen durch Integration von besseren Management- und Netzwerksicherheitsfunktionen sowie Features zum Schutz gegen neu auftretende Sicherheitsbedrohungen für Unternehmensnetze. XTM-Appliances heben sich von den herkömmlichen UTM-Lösungen ab, weil sie über mehr High-End-Funktionalität und Features mit einer für den KMU-Markt ungewöhnlich hohen Bedienungsfreundlichkeit verfügen.

Einen Überblick über die Produktlinien von Astaro finden Sie unter www.astaro.de. Oder fordern Sie gleich Ihre Evaluierungs- oder Heimanwenderlizenz an und laden Sie eine Testversion unter www.astaro.de/try herunter. Online-Produktdemos für ausgiebige Live-Tests finden Sie unter: http://www.astaro.com/our_products/astaro_security_gateway/hardware_appliances/live_demos.

Kontakt



www.astaro.com

Europa, Mittlerer Osten, Afrika

Astaro AG
An der RaumFabrik 33a
76227 Karlsruhe Germany
T: +49 721 255 16 0
F: +49 721 255 16 200
emea@astaro.com

Amerika

Astaro Corporation
3 New England Executive
Park
Burlington, MA 01803
USA
T: +1 781 345 5000
F: +1 781 345 5100
americas@astaro.com

Asien-Pazifik-Region

Astaro K.K.
12/F Ark Mori Building
1-12-32 Akasaka Minato-ku
Tokio 107-6012, Japan
T: +81 3 4360 8350
apac@astaro.com

Dieses Dokument darf auf keine Weise, weder elektronisch noch mechanisch, insgesamt oder teilweise kopiert oder aus jeglichem Grund ohne die schriftliche Erlaubnis der Astaro AG vervielfältigt werden.

© 2009 Astaro AG. Alle Rechte vorbehalten. Astaro Security Gateway, Astaro Command Center und WebAdmin sind Marken von Astaro AG. Alle weiteren Markennamen sind Eigentum ihrer jeweiligen Eigentümer. Keine Gewährleistung für die Richtigkeit der in diesem Dokument enthaltenen Informationen.