Grafik: emojoez / shutterstock.com

Dossier

Unified Threat Management

In Kooperation mit **Boll Engineering**

Rundumblick für die Sicherheit

jor. Der Cyberspace ist ein gefährliches Pflaster. Die besonders Findigen unter den kriminellen Hackern denken sich tagtäglich neue Methoden aus, um die Rechner ihrer Opfer zu infiltrieren. Sicherheitsexperten sind mindestens genauso raffiniert, doch sie hinken den Angreifern notorisch hinterher. Und auf die Firewall allein ist ohnehin kein Verlass. Will sich ein Unternehmen, das mit sensiblen Daten arbeitet, möglichst gut schützen, sollte es sich mit Unified Threat Management (UTM) befassen, wie Patrick Michel, Principal Consultant beim auf IT-Security spezialisierten Distributor Boll Engineering, ab Seite 35 schreibt.

Egal, ob eine Box aus Metall oder eine virtuelle Appliance zum Einsatz kommt: Cybergefahren liessen sich nur mit einem 360-Grad-Ansatz bekämpfen, sagt Michel im Interview auf Seite 37. Michel erklärt, welche Cybergefahren derzeit besonders akut sind, was man dagegen tun kann und für wen eine UTM-Appliance interessant sein könnte. Ferner spricht er darüber, wie sich UTM ohne Leistungseinbussen implementieren liesse und warum der Best-of-Breed-Ansatz seiner Meinung nach nicht die beste Strategie für KMUs ist.

360-Grad-IT-Security: Sicherheitslücken schliessen und Bedrohungen stoppen

Unified-Threat-Management-Appliances erhalten laufend neue Funktionen. Entsprechende Lösungen, die mit einem umfassenden Set an Leistungsmerkmalen ausgerüstet sind, stehen für eine ganzheitliche IT-Security, bieten integriertes WLAN-Management und werden zur Schaltzentrale für das gesamte Firmennetzwerk.

DER AUTOR

Patrick Michel
Principal Consultant,
Boll Engineering

Netzwerksicherheit ist für alle Unternehmen matchentscheidend – egal, ob es sich um ein KMU oder einen Grosskonzern handelt. Den Grundstein jedes Sicherheitskonzepts bildet die Firewall: Herkömmliche Layer-4-Firewalls mit Stateful Inspection sperren oder öffnen anhand von Regeln für jede Verbindung bestimmte Netzwerk-Ports.

Unified Threat Management bringt umfassende Sicherheit

Das Basic Firewalling genügt jedoch nicht, um die immer raffinierteren Bedrohungen abzuwehren. Dafür braucht es Unified-Threat-Management-Appliances (UTM). Dabei werden möglichst viele Sicherheitsfunktionen in einem leistungsstarken System zusammengefasst. Typische UTM-Komponenten sind Antivirus und Antispam, VPN, Angriffserkennung und Angriffsabwehr (IDS/IPS) sowie URL-Filter zum Blockieren gefährlicher Webadressen. UTM-Appliances sind beispielsweise von Firmen wie Fortinet und Watchguard erhältlich, oft auch als virtuelle Appliance oder als Software-as-a-Service.

Im Laufe der Zeit sind zu den klassischen UTM-Features immer wieder neue Funktionen hinzugekommen. Dazu gehört etwa eine Application Firewall, auch Application Control oder Layer-7-Firewall genannt. Die UTM-Appliance sorgt in diesem Fall auch für die gezielte Freigabe oder Sperrung von Anwendungen, Webdiensten und Netzwerkservices.

Verschlüsselte und unbekannte Schädlinge erkennen

Eine weitere und besonders wichtige neuere UTM-Funktion ist das SSL-Scanning. Beim Surfen im Web, beim Austausch von E-Mails und bei der Nutzung webbasierter Businessanwendungen kommen praktisch nur noch per SSL verschlüsselte Verbindungen vor. Den verschlüsselten Verkehr kann die Firewall jedoch nicht analysieren – und dazu gehören auch Schadcode, gefährliche URLs und andere unerwünschte Inhalte.

Antivirus, Webfilter und Co. ergeben nur dann einen Sinn, wenn die Daten offen bereitstehen. Dazu muss die UTM-Appliance die SSL-Verschlüsselung aufbrechen und nach der Analyse die Daten wieder verschlüsseln. Diesen Vorgang nennt man SSL-Scanning. Technisch arbeitet das SSL-Scanning wie folgt: Die UTM-Appliance unterbricht transparent die eingehende SSL-Verbindung. Nach der Analyse baut sie eine neue SSL-Verbindung zum Empfänger auf. Dazu muss sie auf Basis des eigenen, auf der Appliance installierten CA-Zertifikats ein neues Zertifikat für den Client generieren. Auch dieser Vorgang, der in jeder Benutzer-Session immer wieder neu erfolgt, erfordert Rechenaufwand. Ausserdem muss das CA-Zertifikat der UTM-Appliance auf allen Clients in die Liste vertrauenswürdiger Zertifikate aufgenommen werden, den sogenannten Trust Store. Das SSL-Scanning wirkt sich also auch auf das Client-Management aus. Idealerweise arbeitet man mit Managed Clients, damit die Nutzer das CA-Zertifikat nicht manuell bestätigen müssen.

Mit Sandboxing, einem weiteren neueren UTM-Feature, lässt sich auch Schadcode erkennen, der von der Antivirus-Engine nicht als schädlich erkannt wurde. Dateien mit aktivem Code werden dabei in einer abgeschotteten virtuellen Umgebung ausgeführt. Eine Datei wird nur dann weitergeleitet, wenn dabei nichts Gefährliches passiert ist. Sandboxing ist sehr rechenaufwendig. UTM-Appliances nutzen dazu meist einen Cloud-Service des Herstellers. Da der Vorgang Zeit in Anspruch nimmt, eignet sich Sandboxing vor allem für Anhänge von E-Mails, die ja ohnehin nicht in Echtzeit übermittelt werden.

Unerwünschte Gäste abwehren

Manche UTM-Appliances ermöglichen Geo-IP-Firewalling, auch als Geoblocking bekannt. Damit kann die Kommunikation aus bestimmten Ländern komplett abgeblockt werden. Wer etwa im Onlineshop keine Kunden aus Asien bedienen möchte, kann dies per Geoblocking erreichen. Weniger sinnvoll ist es, bestimmte Länder wegen möglichem Hacking zu blockieren. Bösartige Hacker operie-

Bild: jpopba/iStock.com

ren nicht zwingend über Systeme aus dem Land, in dem sie sich befinden. Vergleichbar mit dem Geoblocking ist die Sperrung bestimmter IP-Adressen anhand ihrer Reputation. UTM-Hersteller pflegen dazu Listen von als gefährlich erkannten Systemen. Ein gutes Beispiel sind IP-Adressen von Botnetzen.

Das Netzwerk im Griff

Einige UTM-Hersteller haben zusätzlich zu den Sicherheitsfunktionen einen Wireless Controller in ihre Geräte integriert. Die UTM-Appliance verwaltet so auch alle Aspekte des WLAN, das damit in den Genuss der gleichen Sicherheit wie das LAN kommt. Der Wireless Controller im UTM-Gerät erlaubt es etwa, den Sicherheitsstandard WPA Enterprise zu nutzen. Dabei wird beim Verbindungsaufbau nicht nur der Preshared Key wie bei WPA2, sondern zusätzlich das Nutzer-Login überprüft. Das WLAN wird damit sicherer. Das ist zwar auch mit dedizierten Wireless-Lösungen möglich, doch die direkte Integration in eine Firewall vereinfacht die Verwaltung und Nutzung solcher Funktionen. UTM-Appliances mit integriertem Wireless Controller eignen sich besonders für KMUs oder Zweigstellen.

Eine weitere Funktion von UTM-Appliances neueren Datums ist SD-WAN. Das Gerät kann mehrere Internetanschlüsse zu einer redundant ausgelegten, einfach zu konfigurierenden VPN-Verbindung mit automatischem Failover zusammenfassen. Damit lässt sich ein teures, MPLS-basiertes Privatnetzwerk durch günstige Internetzugänge ersetzen.

Fortinet geht als erster Hersteller noch einen Schritt weiter: Zusätzlich zur Sicherheit und zum Wireless Controller ermöglicht integriertes Switch-Management, die gesamte Struktur des Netzwerks komplett über die Oberfläche der UTM-Appliance zu verwalten. So lassen sich etwa virtuelle Netzwerkunterteilungen (VLAN) direkt über die Oberfläche der UTM-Appliance definieren, und zwar gleichzeitig auf der Firewall und auf den Switches. Bisher musste ein VLAN auf beiden Systemen separat konfiguriert werden. Die Integration ermöglicht zudem, das gesamte Netzwerk bis hin zum einzelnen Client zu visualisieren. So entsteht eine bisher unerreichte Übersicht, und alle Umgebungen – LAN, WLAN und Sicherheit – lassen sich einheitlich bedienen.

UTM – auch ohne Hardware

Fast alle UTM-Anbieter offerieren ihre Lösung nicht nur in Form von Hardwaregeräten, sondern auch als virtuelle Appliance, die sich auf Systemen im eigenen Rechenzentrum oder in einer Cloud-Umgebung wie AWS oder Azure betreiben lässt. Einzelne Anbieter gehen komplett in die Cloud und stellen einen UTM-Dienst als Software-as-a-Service zur Verfügung. Ein Vorteil ist, dass auch mobile Mitarbeitende ohne weiteren Aufwand eingebunden sind und überall das gleiche Mass an Sicherheit gewährleistet ist. Es muss keine lokale Hardware installiert und verwaltet werden. Der Zugriff auf das Netzwerk und das Management der Sicherheitsfunktionen erfolgen über ein Webinterface.

Fast alle UTM-Anbieter offerieren ihre Lösung nicht nur in Form von Hardwaregeräten, sondern auch als virtuelle Appliance.

« Ein integriertes Security Framework schafft umfassende Sicherheit »

Patrick Michel, Principal Consultant beim IT-Security-Distributor Boll Engineering, spricht im Interview über Aspekte der Netzwerksicherheit und wie sich Cybergefahren mit einem 360-Grad-Ansatz wirksam bekämpfen lassen.

Interview: Joël Orizet

Cybersecurity zählt seit Jahren zu den «Hot Topics». Mit welchen Gefahren werden Firmen konfrontiert?
Patrick Michel: Cyberkriminelle nutzen jede Gelegenheit, um in Unternehmensnetzwerke einzudringen und Schaden anzurichten – vom Ausspionieren von Geschäftsgeheimnissen über Erpressung per Ransomware und Nutzung der IT-Ressourcen zu eigenen Zwecken bis zum Lahmlegen des ganzen Betriebs. Dabei werden die Attacken immer raffinierter – und ständig kommen neue Angriffsmethoden hinzu.

Wie lassen sich die vielfältigen Gefahren erfolgreich abwehren?
Zum einen sollten Firmen eruieren, wo ihre grössten Businessrisiken liegen und anhand dieser die Investitionen tätigen. Zum andern setzen nahezu alle Unternehmen Firewalls ein, um Firmennetzwerke oder Datacenter zu schützen und zu segmentieren. Sie ermöglichen zudem den Schutz der Clients. Die dazu eingesetzten Funktionen reichen vom reinen Firewalling über Content Scanning bis hin zu SD-WAN. Dabei wird die Liste immer länger, die IT-Security-Funktionen werden komplexer. Die Nutzung der einzelnen Funktionen hängt davon ab, vor welchen Angriffsvektoren die Firewall schützen soll. Fortschrittliche UTM-Appliances bieten einen integralen Ansatz beziehungsweise eine nahtlose Verschmelzung sich ergänzender Mechanismen in einer Plattform.

UTM-Appliances sind mit zahlreichen Funktionen befrachtet. Wie lässt sich das ohne Leistungseinbussen bewerkstelligen?
Eine clevere Antwort auf diese Frage liefert der IT-Security-Lösungsanbieter Fortinet. Dieser gewährleistet die Leistungsfähigkeit seiner Systeme durch dedizierte ASIC-Prozessoren, die besonders leistungshungrige Funktionen von der CPU offloaden. Eine Kombination, die selbst in anspruchsvollen Umgebungen für genügend Performance zu einem attraktiven Preis sorgt.

Sind UTM-Appliances primär etwas für KMUs oder adressieren sie auch die Bedürfnisse grösserer Firmen?
Hersteller von Enterprise-Firewalls implementieren typischerweise ein Subset gängiger UTM-Funktionen in ihre Plattformen und sind in der Regel nicht auf den KMU-Markt ausgerichtet. Dann gibt es Hersteller, die ausschliesslich UTM-Firewalls für KMUs anbieten. Zu guter Letzt gibt es Hersteller wie etwa Fortinet, die alle Segmente mit einer Plattform adressieren.

Welche Aspekte sprechen im Vergleich zu einem Best-of-Breed-Ansatz für eine UTM-Appliance-Strategie?
UTM-Appliances bieten zahlreiche Funktionen in einem Gerät und sind somit eine perfekte Lösung für anspruchsvolle KMUs mit begrenzten Budgets. Zu beachten ist zudem, dass sich die direkte Anbindung von Wireless Access Points, Switches und Endpoint-Software an UTM-Firewalls mehr und mehr durchsetzt. Dadurch entsteht eine sogenannte Security Fabric. Diese vereinfacht die Verwaltung und bietet Sicherheitsfunktionen und Automatisierungen bis zum einzelnen Access Port und Client. Somit profitieren KMUs von Security-Funktionen, die sonst nur durch teure Best-of-Breed-Lösungen zur Verfügung stehen. Dies ist angesichts der zunehmenden Komplexität und der Verschmelzung von Netzwerk und Security ein wichtiger Faktor.

« UTM-Appliances bieten zahlreiche Funktionen in einem Gerät und sind somit eine perfekte Lösung für anspruchsvolle KMUs mit begrenzten Budgets. »

Patrick Michel, Principal Consultant, Boll Engineering

Fast alle UTM-Anbieter offerieren ihre Lösung auch als virtuelle Appliances, die sich in Cloud-Umgebungen betreiben lassen. Was ist davon zu halten?
Das war und ist eine logische Entwicklung, da sich die Virtualisierung von Servern und Angeboten wie Infrastructure-as-a-Service immer mehr durchsetzen. Dort braucht es letztlich auch Firewalls. Da diese nicht physisch installiert werden können, werden Software-Appliances eingesetzt. Das ist heute Standard.

Was halten Sie von Software-as-a-Service-Anbietern, die klassische UTM-Firewall-Funktionalitäten in der Cloud anbieten?
Definitiv ein spannender Ansatz und auch ein logischer Schritt durch die starke Cloudifizierung von Datacenter und Services. Ich rechne damit, dass vermehrt klassische Anbieter von Appliances auch in diese Richtung gehen. Schon jetzt setzen diese auch auf Cloud-Management der Appliances. Der nächste Schritt wird UTM-Firewall-Funktionalität im Software-as-a-Service-Cloud-Modell sein.