# Universelle Bedrohungsabwehr

**Know-how** Bei UTM Appliances hat sich einiges getan. Zu den klassischen Firewall-Funktionen sind viele neue Features hinzugekommen, bis hin zur integrierten Zentrale für die Sicherheits- und Netzwerkverwaltung.

*Von Patrick Michel*

Netzwerksicherheit ist für alle Unternehmen unabdingbar, egal ob KMU oder Grosskonzern. 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. Gleichzeitig werden die Attacken immer raffinierter, und ständig kommen neue Angriffsmethoden hinzu.

## Firewall versus UTM

Am Anfang jedes Sicherheitskonzepts steht die Firewall: Herkömmliche Level 4 Firewalls mit Stateful Inspection kontrollieren den Netzwerkverkehr in der Transportschicht und sperren oder öffnen für jede Verbindung aufgrund von definierten Regeln bestimmte ein- und ausgehende Netzwerk-Ports.

Solches Basic Firewalling bietet heute bereits fast jeder Internet Router, den man für den Heimgebrauch erstehen kann. Mehr Funktionalität als herkömmliche Router bieten UTM Appliances (Unified Threat Management): Möglichst viele Sicherheitsfunktionen werden in einem leistungsstarken System zusammengefasst. Typische UTM-Komponenten sind Antivirus- und Antispamfunktionen und virtuell-private Netzwerkverbindungen (VPN) via IPSec oder SSL für sichere Verbindungen vom Internet ins Unternehmensnetzwerk, zum Beispiel für mobile Mitarbeitende oder zur Anbindung von Aussenstellen. Zu den klassischen UTM Features gehören ferner Angriffserkennung und Angriffsabwehr (Intrusion Detection/Prevention, kurz IDS/IPS) und URL-Filter zum Blockieren gefährlicher Web-Adressen.

Unified Threat Management ist jedoch nicht beim ursprünglichen Funktionsumfang stehengeblieben. Im Lauf der Zeit sind immer wieder neue Funktionen hinzugekommen. Dazu gehört etwa eine Application Firewall, je nach Anbieter auch Application Control genannt. Die UTM Appliance kontrolliert dann nicht nur die Ports, sondern sorgt auch für die gezielte Freigabe oder Sperrung von Anwendungen. Dabei kann es sich um Webdienste wie Facebook oder Twitter, aber auch um generelle Netzwerk-Services handeln. Da die Application Firewall im Schichtenmodell der Kommunikation auf Ebene 7 greift, nennt man sie auch Layer 7 Firewall.

## SSL wird aufgebrochen

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 Business-Anwendungen 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.

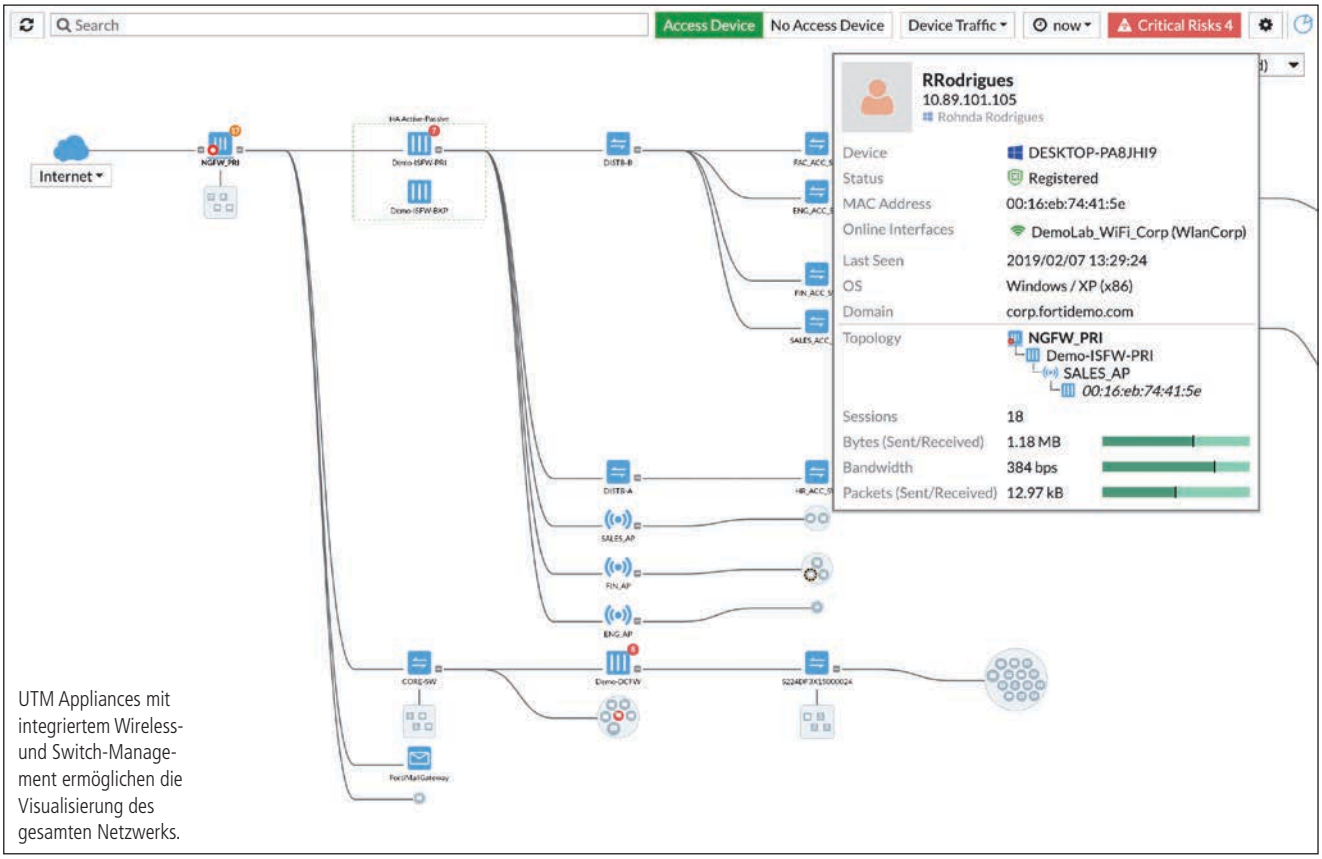
Antivirus, Webfilter und Co. ergeben nur dann einen Sinn, wenn die übermittelten Daten für die Analyse offen zur Verfügung stehen. Dazu muss die UTM Appliance die SSL-Verschlüsselung aufbrechen und nach der Analyse die Daten wieder verschlüsseln. Dies erfordert einiges an Rechenleistung und stellt hohe Ansprüche an die Hardware. Die leistungsfähigeren UTM-Geräte nutzen teilweise dafür spezialisierte Chips, sodass die CPU-Belastung im Rahmen bleibt.

Technisch arbeitet das SSL Scanning wie folgt: Die UTM Appliance terminiert 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 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.

## Malware im Sandkasten

Signaturbasierte Antivirusfunktionen sind gut bei der Abwehr von bekanntem Schadcode. Bisher unbekannte Schädlinge können sie jedoch nicht eruieren. Hier kommt Sandboxing ins Spiel: Von der Antivirus-Engine als nicht schädlich beurteilte Dateien, die aktiven Code enthalten, werden in eine abgeschottete virtuelle Umgebung geladen und dort ausgeführt. Nur wenn auch dann nichts Gefährliches passiert ist, wird die Datei weitergeleitet.

Grössere Unternehmen betreiben für das Sandboxing eine eigene Infrastruktur mit leistungsfähiger Hardware. UTM Appliances für den KMU-Einsatz nutzen dazu meist einen Cloud Service des Her-




UTM Appliances mit integriertem Wireless- und Switch-Management ermöglichen die Visualisierung des gesamten Netzwerks.

stellers, da enorme Ressourcen benötigt werden. Sandboxing hat allerdings einen Nachteil: Es kann Minuten dauern, bis die Analyse beendet ist. Es eignet sich deshalb vor allem für Anhänge von E-Mails, die ja ohnehin nicht in Echtzeit übermittelt werden – da wird eine Verzögerung schon mal toleriert.

Bei direkt übermittelten Files, zum Beispiel bei ganz normalen File-Downloads über den Browser, wäre die Nutzerakzeptanz dagegen gering. Deshalb besteht oft die Option, den ersten Download einer unbekannten Datei zuzulassen, sie direkt an den Empfänger zu leiten und sie parallel dazu in die Sandbox zu schicken. Dann ist zwar potentiell ein Client infiziert, weitere Downloads werden nach der Analyse aber gesperrt.

## Land X unerwünscht

Bereits etwas länger im Funktionsumfang mancher UTM Appliance ist das Geo IP Firewalling, auch als Geoblocking bekannt. Der UTM-Hersteller stellt dafür eine laufend gepflegte Liste von länderspezifischen Adressobjekten bereit. Auf dieser Basis kann die Kommunikation aus bestimmten Ländern oder ganzen Kontinenten vollständig abgeblockt werden. Wer etwa in seinem Online-Shop keine Kunden aus Asien empfangen möchte, kann dies per Geo IP Firewalling erreichen.

Weniger sinnvoll ist es, bestimmte Länder wegen möglichem Hacking zu blockieren. Zwar gelten einige Gegenden der Welt als besonders dicht von Cyberkriminellen bevölkert, aber bösartige Hacker operieren nicht zwingend von Systemen aus dem Land, in dem sie sich effektiv befinden. Verschleierungstaktiken sind hier der Standard. Geoblocking reduziert somit die Anzahl potentieller Angreifer. Es ist aber ein zweischneidiges Schwert: Auch mobilen Mitarbeitenden, die in einer geblockten Region unterwegs sind, bleibt der Zugang verwehrt.

Vergleichbar mit dem Geoblocking, aber wesentlich sinnvoller im Einsatz ist die Blockierung bestimmter IP-Adressen anhand ihrer Reputation. UTM-Hersteller pflegen dazu Listen von als gefährlich erkannten Systemen, die meist problemlos blockiert werden können. Ein gutes Beispiel sind IP-Adressen von Botnetzen.

## UTM über Security hinaus

Schon mehrere UTM-Hersteller haben zusätzlich zu den Sicherheitsfunktionen einen Wireless Controller in ihre Geräte integriert. Als Ergänzung verkaufen sie passende Managed Access Points. Die UTM Appliance verwaltet dann nicht nur die Sicherheit im ganzen Firmennetzwerk, sondern auch alle Aspekte des WLAN.

Das kabellose Netz kommt dadurch in den Genuss der gleichen Sicherheit wie das LAN, inklusive sicherem, vom internen WLAN-Verkehr separierten, Gastzugang. Die Access Points und WLAN Clients lassen sich zentral über die gewohnte Oberfläche der UTM Appliance verwalten, eine lokale Konfiguration ist nicht erforderlich. Und die WLAN Clients sind durch die UTM-Funktionen umfassend geschützt. Der Wireless Controller im UTM-Gerät erlaubt es beispielsweise, 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 kleinere und mittelgrosse Firmen oder Zweigstellen. Grossunternehmen mit umfangrei-

chen, architektonisch verteilten Büro- und Produktionsflächen werden eher auf dedizierte Wireless Controller setzen, die noch leistungsfähiger sind.

Eine weitere Funktion von UTM Appliances neueren Datums ist SD-WAN. Das Gerät kann mehrere Internet-Anschlüsse 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.

## Volle Kontrolle über das Netzwerk

Erste Anbieter gehen noch weiter: Zusätzlich zur Sicherheit und zum Management des Wireless-Netzwerks ermöglicht integriertes Switch Management, die gesamte Struktur des Netzwerks komplett über die Oberfläche der UTM Appliance zu konfigurieren, zu verwalten und zu überwachen. So lassen sich etwa virtuelle Unterteilungen des Netzwerks (VLANs) 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 von Sicherheits- und Networking-Funktionen macht es zudem möglich, das gesamte Netzwerk mit allen Details und Sicherheitshinweisen 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

Praktisch alle UTM-Anbieter offerieren ihre Lösung nicht nur in Form von Hardware-Geräten, 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. Doch ein Nachteil besteht: Man ist völlig auf den Anbieter und auf die Verfügbarkeit des Dienstes angewiesen. Sollte er ausfallen, läuft nichts mehr. ■


### DER AUTOR

**Patrick Michel** ist ein «alter Hase» in der Schweizer IT-Security-Szene. Er beschäftigt sich seit 1996 mit IT-Sicherheit und hat sich dabei mit unterschiedlichen Security-Themen auseinandergesetzt. Er gilt als ausgewiesener, langjähriger Firewall-Experte und hatte in seinem beruflichen Werdegang die unterschiedlichsten Positionen inne. Seit 2011 ist er beim Security-Distributor Boll Engineering tätig, aktuell als Head of Sales. Davor war er unter anderem Senior Security System Engineer bei Fortinet, COO bei Swisssign, Senior Security Consultant bei Celeris und CTO bei Telindus.