UTM-Security im Aufwind

Komplexere Sicherheitsanforderungen brauchen neue Funktionen. Im Security-Bereich ist UTM (Unified-Threat-Management) schon seit langer Zeit ein Thema unter den Herstellern. Ziel von UTM ist es, möglichst viele Sicherheitsaufgaben mit einer Hardware zu bewerkstelligen und so eine vereinte Abwehr gegen Schädlinge zu bilden. Bis anhin waren diese All-in-One-Lösungen ausschliesslich im höheren Preissegment angesiedelt. Nun sind die UTM Geräte auch für KMUs (Klein und Mittelständige Unternehmen) erschwinglich.

Trend zu "Unified"
Firmennetzwerke sind immer grösseren Gefahren ausgesetzt. Um die Sicherheit der Firmendaten und des gesamten Netzwerkes zu garantieren, braucht es somit immer bessere und komplexere Sicherheitslösungen. Eine herkömmliche Stateful-Packet-Inspection-Firewall (SPI-Firewall) wird den heutigen Gefahren und Angriffen nicht mehr gerecht. Die Prüfung der Zugangsberechtigung der Datenpakete durch SPI ist eine sehr wichtige Basisfaunktion, doch sollten die Pakete auch nach Viren, bestimmten Attacken-Mustern und schädlichen Codes untersucht werden, damit die Sicherheit gewährleistet werden kann. Auch das Ausfiltern von Spam-E-Mails ist heute ein wichtiger Schutzfaktor. Der Trend geht darum klar in Richtung All-in-One-Lösungen, die zum Ziel haben, möglichst viele Sicherheitsaufgaben mit einer Hardware zu bewerkstelligen.

UTM löst bestehende Sicherheitslösungen ab
Die neuen UTM-Firewalls bieten einen umfassenden Schutz dank Intrusion-Detection-Prevention, Anti-Virus, Anti-Spam und Content-Filter. So werden auf mehreren Ebenen die verschiedensten Gefahren und Attacken bekämpft. Ein grosser Vorteil dieser All-in-One-Lösungen ist der einfache Unterhalt. Gerade in KMUs ist dies ein grosses Bedürfnis, denn so können die Kosten für zusätzliche Geräte und die Wartung reduziert werden.

UTM-Funktionen
All-in-One-Lösung mit Intrusion-Prevention, Anti-Virus, Anti-Spam und Content-Filter, welche die bereits bestehenden Sicherheitsfunktionen (wie Stateful-Packet-Inspection, VPN, Loadbalancing, Bandbreitenmanagement, etc.) ergänzt.

Application Control
Erkennt Datenverkehr applikationsnah und nicht erst am Port oder über das Protokoll. Damit lassen sich die Sicherheitsrichtlinien für Applikationen einhalten. Zudem wird die Kontrolle über Applikationen erleichtert, die trotz vertrauenswürdiger Ports und Protokolle keine Standard-Ports, Port-Hopping oder Tunneling verwenden.

Anti-Virus
Die Anti-Virus-Funktion vergleicht Dateien mit Viren-Signaturen und neutralisiert so bereits Viren beim Eintreffen ins Netzwerk. Der Virenschutz auf dem Mailserver und Desktop wird somit sinnvoll ergänzt.

Anti-Spam
Die Anti-Spam-Funktion vergleicht E-Mails mit Spam-Signaturen. So werden Spam-Mails erkannt, die häufig auch Würmer und Trojaner über Attachments beinschleusen. Auch einen Schutz vor Phishing-Mails wird geboten. Die eingehenden Mails werden geprüft und die Spam-Mails markiert. Der Benutzer entscheidet im Mail-Client, wie das als Spam markierte Mail zu behandeln ist, z. B. Verschieben in einen definierten Spam-Ordner oder automatisches Löschen.

Intrusion-Detection-Prevention
Eine herkömmliche Firewall ist nur auf der Zugriffsebene wirksam, während das IDP-System auch den Inhalt der Datenübertragung analysiert. Es kann Attacken durch Würmer, Trojaner und Backdoors sowie modifizierte Versionen einen Schädlings erkennen und blockieren, und dies auch nur anhand von Erkennungsmustern oder abnormalem Verhalten. Auch Peer-to-Peer- oder Instant-Messaging-Applikationen werden abgeblockt.

Content-Filter
Der Content-Filter kontrolliert die Internetzugriffe, was in Unternehmen ein immer häufigeres Bedürfnis ist. Einerseits hilft die Blockade von einschlägigen Web-Kategorien beim Durchsetzen der Firmenrichtlinien und andererseits schützt sie vor schadenhaftem Code, die über solche Sites eingeholt werden. Reports geben Aufschluss über den Web-Sites-Zugriff. Die Privatsphäre der Mitarbeiter bleibt gewahrt, da die Reports gesamthaft und ohne Bezug zu einzelnen Personen erscheinen.

Data Loss Prevention
"Data Loss Prevention" ist der Schutz gegen den unerwünschten Abfluss von Daten, der Schaden verursacht und auch bemerkt wird, während "Data Leakage Prevention" der Schutz gegen ein vermutetes, aber nicht messbares und manchmal auch im Einzelfall gar nicht feststellbares Weitergeben von Informationen an unerwünschte Empfänger steht. Alles weitere unter Wikipedia