Stefan Strobel

FIREWALL, NÄCHSTE GENERATION

Ein kleiner Exkurs in die Netzwerksicherheit

Vor mehr als 20 Jahren kamen die ersten Firewalls zum Einsatz. Im Lauf der Jahre hat sich deren Funktion grundlegend verändert.

Die meisten Unternehmen haben zu Beginn der 90er Jahre begonnen, sich mit Netzwerksicherheit zu beschäftigen. Zu dieser Zeit wurde das Internet in Deutschland kommerziell verfügbar und TCP/IP als Protokoll wurde für Unternehmen interessant. Erste kommerziell verfügbare Firewall-Produkte kamen auf den Markt und erste Bücher erschienen in den Regalen der Buchhandlungen.

Die Hersteller, die den Markt in dieser frühen Phase bestimmt hatten, waren Check Point mit der ersten Version seiner Firewall-1, Raptor mit der Eagle-Firewall und TIS mit der Gauntlet-Firewall. Während Gauntlet und Raptor Eagle heute vom Markt verschwunden sind, ist Check Point nach wie vor einer der bekanntesten Anbieter. Auf technischer Seite hat Check Point den Markt damals mit der Einführung seiner „stateful multilayer inspection" revolutioniert. Das Konzept, das heute jeder als „deep packet inspection" (DPI) kennt, war damals umstritten und alle anderen Firewall-Produkte basierten auf individuellen Proxies für die wichtigen Protokolle, allenfalls ergänzt durch generische TCP-Relays.

Für Sicherheitsexperten war eine Firewall zunächst kein Produkt, sondern ein Gesamtkonzept, das aus Filtern und Applikationsgateways beziehungsweise Proxies bestand. Über die Jahre hat sich jedoch der Sprachgebrauch gewandelt und die Struktur am Übergang zum Internet wird heute eher DMZ-Struktur oder Firewall-Umgebung genannt, während der Begriff Firewall selbst tatsächlich mit den Filterkomponenten assoziiert wird.

Parallel zu den ersten Firewalls haben sich VPN-Produkte etabliert, die eine verschlüsselte Verbindung zwischen Niederlassungen oder von mobilen Geräten zum Rechenzentrum über das Internet ermöglichen. Firewall-Produkte haben dies als Zusatzfunktion bereits in den 90er Jahren angeboten und heute gibt es kaum noch kommerzielle Firewall-Produkte, die keine VPN-Funktionalität integriert haben.

Kein ausreichender Schutz

Schon sehr früh war klar, dass Paketfilter und Proxies alleine nicht ausreichen, um vor den Gefahren aus einem externen Netz zu schützen. Die ersten prominenten Viren- und Wurmvorfälle haben dies einer breiten Öffentlichkeit vor Augen geführt. Klassiker wie „I love you", „Melissa" oder der „SQL Slammer" haben einer weiteren Produktkategorie zum Durchbruch geholfen: den Virenschutz- beziehungsweise Content-Security-Gateways.

Die ersten Produkte wie Mimesweeper konzentrierten sich auf die E-Mail-Übertragung und analysierten an Mails angehängte Dateien. Etwas später kamen Produkte von Aladdin, Cacheflow (heute BlueCoat) oder TrendMicro, die auch Datei-Downloads über den Browser abdeckten. Finjan (heute M86 Security) war der erste Hersteller, der auch aktiven Code in Webseiten (Java und Active-X) auf Basis seines Verhaltens filterte, ein Ansatz, den man heute vor allem bei Lösungen gegen gezielte Angriffe findet. Ergänzend erschienen URL-Filter-Produkte von Firmen wie Websense, SurfControl, Webwasher und anderen, die versuchten, URLs zu kategorisieren und so den Zugriff auf gefährliche oder unerwünschte Websites zu verhindern.

In den 90er Jahren ging man noch davon aus, dass das Perimeter, also die Grenze des internen Netzes zum Internet, mit Firewalls und Content-Security ausreichend geschützt werden kann. Dennoch begann eine erste Verschiebung des Schwerpunktes hin zur Sicherheit im internen Netzwerk. Manche Unternehmen versuchten, das interne Netz mit zusätzlichen Firewall-Filtern weiter in Segmente zu gliedern und so die Sicherheit zu erhöhen, andere wollten eher mit IDS-Systemen Angriffe im internen Netz erkennen. Die frühen Netzwerk-IDS-Produkte wie ISS Realsecure, Network Flight Recorder oder später auch Snort basierten zunächst primär auf Mustererkennung in Paketen. Dieser Ansatz kam jedoch schnell an seine Grenzen und konnte mit den schnell steigenden Übertragungsbandbreiten im internen Netz nicht mithalten. Die Firma Network-Ice war vermutlich der erste kommerzielle Anbieter, der eine überzeugende IDS-Engine auf den Markt brachte. Diese dekodierte zunächst das mitgelesene Protokoll, bevor weitere Musterprüfungen angewendet wurden, was zu einer Erhöhung der möglichen Bandbreite und zu einer Verbesserung der Erkennungsleistung führte. Network-Ice wurde jedoch nicht besonders alt, denn ISS übernahm der Mitbewerber recht schnell und integrierte die neue Technik in die eigenen Produkte. Erst später kamen Player wie TippingPoint (HP), Intruvert (McAfee) und Sourcefire (kommerzielle Snort-Variante, heute Cisco) auf den Markt. Heute werden die Lösungen nicht mehr als IDS, sondern als IPS vermarktet, da sie meist als Gateway im Datenverkehr erkannte Angriffe ausfiltern sollen.

Hype-Thema IPS

Um die Jahrtausendwende war IDS/IPS ein Hype und zahlreiche größere Firmen implementierten derartige Produkte im Glauben, dass sie damit ihre Sicherheit deutlich erhöhen könnten. In den Jahren danach schalteten jedoch viele Organisationen die Produkte wieder ab, da sie erkannten, dass der Betriebsaufwand in keinem vernünftigen Verhältnis zum Sicherheitsgewinn steht und die eigentlich notwendige Überwachung der Produkte rund um die Uhr zu teuer ist.

Ein anderer Aspekt der Sicherheit im internen Netz ist die Frage nach dem Zugang zu diesem Netz. Ein Besucher im Firmengebäude soll sein Notebook nicht einfach in eine Netzwerksteckdose stecken können und so Zugriff auf die interne IT-Infrastruktur bekommen. In den meisten Firmennetzen in Deutschland ist jedoch nach wie vor keine Netzwerkzugangskontrolle (Network Access Control, NAC) implementiert, auch wenn entsprechende Produkte von Cisco, Microsoft oder spezialisierten Anbietern wie Forescout bereits seit fast zehn Jahren verfügbar sind. Die Grundidee dieser Produkte ist, dass jedes mit dem Netzwerk verbundene Gerät zunächst anhand einer Policy geprüft wird. Solch eine Policy kann beispielsweise nur firmeneigene Geräte erlauben, wenn diese bestimmten Sicherheitsanforderungen genügen und fremde Geräte automatisch mit einem Gäste-LAN verbinden.

Wenn Netzwerkzugangskontrolle nicht umgesetzt wird, dann oft aufgrund eines Missverständnisses. Viele Unternehmen glauben entweder, dass die Filterung von MAC-Adressen ausreichend Sicherheit bietet oder dass NAC nur machbar ist, wenn man flächendeckend 802.1x verwenden kann und dafür auch eine PKI zur Verfügung hat. Beides ist so nicht richtig. 802.1x und Zertifikate sind zwar ein möglicher Weg zur Umsetzung von NAC, Spezialanbieter wie Forescout oder auch Portnox bieten jedoch sehr elegante Lösungen, die auch in heterogenen Umgebungen und mit einfachen oder älteren Switches gut funktionieren. Eine reine Filterung von MAC-Adressen dagegen ist allenfalls eine geringe Hürde, die einen kompetenteren Angreifer kaum fernhalten kann.

Schon relativ früh kamen Hersteller auf die Idee, Firewall-Filter, Content-Security-Filter und Angriffserkennung in einem gemeinsamen Produkt zu integrieren. Vor allem für mittelständische oder kleinere Unternehmen war es schlicht zu teuer, eine Firewall-Struktur aufzubauen, die aus zahlreichen teuren Einzelprodukten bestand. Firmen wie Astaro oder Watchguard, die beide um die Jahrtausendwende gegründet wurden, besetzten diese Lücke mit Produkten auf Basis von Linux und Open-Source-Security-Komponenten, für die sich der Begriff „Unified Threat Management" (UTM) etabliert hat. Nahezu alle anderen Hersteller zogen nach und heute gibt es Dutzende von Firewall-Produkten, die auch als UTM-Lösungen vermarktet werden. Der Funktionsumfang ist in den letzten 10 Jahren kontinuierlich angewachsen.

Ungefähr zur gleichen Zeit rückten Web-Applikationen stärker in den Fokus der Angreifer und der Sicherheitsexperten. Angriffstechniken wie SQL-Injection oder Cross-Site-Scripting wurden auf zahlreichen Sicherheitskonferenzen vorgeführt und verfeinert; existierende Firewalls konnten die Angriffe weder erkennen noch verhindern, da sie auf Protokollebene wie legitime Zugriffe auf Web-Server aussehen.

Sanctum und Kavado waren die ersten Anbieter von Web-Application-Firewalls (WAF). WAF werden im Rechenzentrum vor die eigenen Webserver geschaltet und erkennen und verhindern Angriffe auf der Applikationsebene, indem jedes einzelne Feld eines Web-Formulars beziehungsweise jeder Parameter einer URL gegen Black- und White-Listen geprüft werden. Inzwischen sind sowohl Sanctum als auch Kavado vom Markt verschwunden und der WAF-Markt wird von Herstellern wie Imperva, DenyAll oder F5 und Citrix dominiert, wobei letztere die WAF-Funktionen in ihre Load-Balancer integriert haben.

Next Generation Firewall

Im Jahr 2007 kam Palo Alto Networks mit seiner ersten „Next Generation Firewall" auf den Markt und 2009 veröffentlichte Gartner ein Paper, in dem sie den Begriff „Next-Generation Firewall" (NGFW) definierten. Wenngleich der Begriff nicht geschützt ist und heute fast alle Hersteller von Firewalls ihre Produkte als „Next Generation" bezeichnen, so ist der entscheidende Unterschied eine neue Filter-Engine. Dabei wird in einem gemeinsamen Schritt das tatsächlich verwendete Protokoll und der Benutzer, der das Protokoll verwendet, unabhängig von Port-Nummern identifiziert und gefiltert. Gleichzeitig werden IPS-Funktionen ausgeführt. Bei klassischen Firewalls oder älteren UTM-Appliances wurden mehrere separate Paketverarbeitungen für die Filterung und Angriffserkennung durchlaufen.

Die heute bekannten Firewall-Hersteller nehmen fast alle für sich in Anspruch „Next Generation Firewalls" zu bauen, wobei jeder Hersteller den Begriff ein wenig anders auslegt. Während Palo Alto und der deutsche Hersteller Adyton vor allem ihre integrierten Engines in den Vordergrund stellen, ist es bei Check Point die in den letzten Jahren etablierte Software-Blade-Architektur; bei Fortinet die Filterung mit mehreren spezialisierten Prozessoren beziehungsweise ASICs und bei Watchguard die umfassende Integration von Zusatzfunktionen in einer gemeinsamen GUI. Eine andere Nische, bei der „Next Generation" weniger eine Rolle spielt, besetzen die deutschen Firewall-Hersteller Genua und Lancom. Beide werben mit „Made in Germany" und einer Zertifizierung vom BSI, dem Bundesamt für Sicherheit in der Informationstechnik.

Katz-und-Maus-Spiel

Betrachtet man die Entwicklung der Netzwerksicherheit in den letzten 20 Jahren, so

Bild: Adyton Systems

Darstellung der Komponenten einer Next Generation Firewall

wurden Weiterentwicklungen der Sicherheit meist durch Entwicklungen in der IT und Netzwerktechnik beziehungsweise durch eine Weiterentwicklung auf der Seite der Angreifer getrieben.

Derzeit drängen wieder neue Sicherheitslösungen auf den Markt, die eine weitere Schwachstelle in bestehenden Sicherheitsstrukturen adressieren: gezielte professionelle Angriffe mit individueller Malware, die mit den bisherigen Virenschutz- und Content-Security-Gateways nicht erkannt werden können. Die amerikanischen Hersteller sprechen dabei von „Advanced Persistant Threats" (APTs) beziehungsweise Lösungen zu Schutz vor APTs.

Firmen wie FireEye, Ahnlab oder Cyphort ergänzen die bestehenden Firewall-Strukturen, indem sie übertragene Dateien in eine virtuelle Infrastruktur kopieren und dort zur Ausführung bringen. Schädliches Verhalten soll so erkannt werden können, auch wenn die Malware als solche noch nicht bekannt war. Ein alternativer oder ergänzender technischer Ansatz konzentriert sich auf die Analyse der ausgehenden Kommunikation und versucht, dort die Kommunikation von Malware mit ihren sogenannten „Command & Control"-Servern zu erkennen. Beide Ansätze basieren auf der Erkennung eines bestimmten Verhaltens und sind damit leider auch von professionellen Angreifern umgehbar. Der professionelle Angreifer muss nur selbst die betroffenen Sicherheitslösungen besitzen und kann dann seine Malware so weit variieren, bis ihr Verhalten nicht mehr erkannt wird.

Interessant ist auch, dass einige Firewall-Hersteller diesen Ansatz bereits in ihre Firewalls integriert haben. Check Point bietet dafür eine eigene Blade an, Palo Alto sein Zusatzprodukt Wildfire sowie die Endgeräte-Software des gerade zugekauften Herstellers Cyvera, und Watchguard durch OEM-Integration des Produktes von Lastline. Der Vorteil einer solchen Integration für den Endkunden liegt auf der Hand: Durch die bestehende Firewall müssen alle Datenpakete sowieso hindurch. Der Aufwand für die Integration und auch für die Beschaffung einer Maßnahme gegen APTs ist so deutlich geringer.

Alternativ zu den Anti-APT-Lösungen auf Basis von Erkennungsmechanismen im Netzwerk bietet sich ein ebenfalls neuer Ansatz an, bei dem die Endgeräte immunisiert werden. Prozesse, die mit Daten aus externen beziehungsweise nicht vertrauenswürdigen Quellen arbeiten, werden dabei innerhalb des Betriebssystems virtualisiert und schädliches Verhalten von Malware – egal ob bekannt oder bisher unbekannt – kann so keinen Schaden mehr anrichten. Der bisher einzige Hersteller dieser Technik ist die Firma Bromium, die von ehemaligen Entwicklern des Xen-Hypervisors gegründet wurde. (ll)