TEC WORKSHOP

Link: https://www.tecchannel.de/a/die-firewall-der-neuen-aera,2044492

Cloud Computing verändert Anforderungen

Die Firewall der neuen Ära

Datum: 06.09.2013
Autor(en): Werner Kurzlechner

Firewalls alter Machart erfüllen in Zeiten von Cloud Computing ihre Aufgaben nur noch bedingt. Deshalb müssen die zukünftigen IT-Brandmauern noch intelligenter konstruiert sein, wenn sie feuerfest sein sollen. Aus der Wolke selbst kommt dafür Arbeitsentlastung.

Die Firewall ist mittlerweile ein klassisches Security-Instrument – aber als „klassisch" gelten auch so einige Bauwerke in Griechenland, die eigentlich Ruinen sind. Sind Firewalls überhaupt noch zeitgemäß, da im Zeichen des Cloud Computings eine neue Ära anbricht? Die Antwort darauf ist ziemlich eindeutig: in ihrer altbekannten Form alleine in jedem Fall nicht. Der digitale Schutzwall gegen Brandherde, was „Firewall" im Wortsinn ja bedeutet, hat in der Vergangenheit ganz alleine viele Gefahren gebannt. Inzwischen wird es wieder wichtiger, zusätzlich zu diesem Mauerwerk fleißige Feuerwehrleute zur Hand zu haben. So plädiert Forrester Research für eine „Neuerfindung des Sicherheitsbewusstseins", um eine „Human Firewall" verfügbar zu haben. Vor allem Social Media und Cloud Computing lassen nach Einschätzung der Forrester-Analysten Nick Hayes und Andrew Rose bewährte Kontrollmechanismen zunehmend ins Leere laufen. Daher benötigten die Unternehmen geschultes Personal, um Schwachstellen zu erkennen und die Firmen-IT zu schützen.

Dieser Schritt hin zu verstärkter Aktivität und Bewusstseinsbildung ist sicherlich unumgänglich. Aber auch technologisch dreht sich die Erde weiter. Die Analysten von Gartner empfehlen – nicht nur im Hinblick auf die Datenauslagerung in die Wolke – den Kauf von „Next Generation Firewalls" (NGFW). Traditionelle Firewalls seien nicht mehr in Lage, die Codes zu erkennen, mit denen Cyberkriminelle von heute arbeiten. Security-Anbieter haben auf diese Herausforderung beispielsweise durch Malware Inspection reagiert, einen seit längerem im Anti-Virus-Bereich benutzten Ansatz: heruntergeladene Files werden zwischengespeichert und dann in einem zweiten Schritt durchleuchtet. Diese Methode birgt allerdings ihre eigenen Sicherheitsrisiken in sich, weil etwa der Memory-Speicherplatz an Kapazitätsgrenzen getrieben werden kann. Hinzu kommt eine ausgeprägte Latenz.

1. Gartner definiert neue Generation

Vor diesem Hintergrund hat Gartner Merkmale einer NGFW definiert. Eine NGFW wendet demnach Deep Packet Inspection (DPI) an, indem Intrusion Prevention System (IPS) und Application Intelligence & Control integriert werden. So soll der Inhalt der benutzten Daten visualisiert werden. Beinhalten sollte eine Firewall der nächsten Generation laut Gartner mindestens: bekannte Firewall-Funktionen wie Network Adress Translation (NAT), Stateful Protocol Inspection (SPI) und Virtual Private Networking (VPN); eine integrierte signatur-basierte IPS-Maschine; Application Awareness, umfassende Stack-Visibilität und granulare Kontrollen; Funktionen, die Informationen von außerhalb der Firewall aufnehmen; einen Upgrade-Pfad, der zukünftige Bedrohungen und Informationsquellen berücksichtigt; SSL-Entschlüsselung, um unerwünschte verschlüsselte Apps zu identifizieren.

Das alles ist einerseits ein alter Hut, weil Gartner sich bereits seit Jahren für NGFWs stark macht. Zugleich handelt es sich für die meisten Anwender aber offenkundig immer noch um Zukunftsmusik. Lediglich 8 Prozent der Firmen nutzen momentan dieses Instrument; in den kommenden fünf Jahren soll der NGFW-Anteil auf 30 Prozent steigen. Das prognostizierte kürzlich Gartner-Analyst Greg Young. Als Trend macht Young ferner aus, dass SSL VPN komplett in die Firewall integriert wird. Überdies versuchten die Anwender, weiterhin möglichst von einem einzigen Firewall-Anbieter ausgerüstet zu werden. Aufschlussreich ist das vor dem Hintergrund, dass auf Anbieterseite momentan ein massives technologisches Wettrüsten stattfindet, über das Ellen Messmer für unsere amerikanische Schwesterpublikation Network World berichtet. Insofern darf man zuversichtlich gestimmt sein, dass Firewalls in Zukunft so konstruiert sein werden, dass sie immer noch einen Nutzen haben.

2. Cloud entlastet Firewall

Dieser Ansicht ist auch Wieland Alge, General Manager EMEA beim Security-Anbieter Barracuda Networks. Alge macht sogar überaus positive Wechselwirkungen zwischen der Firewall und Cloud Computing aus. Die Nutzung von cloud-basierten Security-Dienstleistungen habe etwa den angenehmen Nebeneffekt, die mitunter von Firewalls verursachten Performance-Probleme zu beheben. Das geschehe, indem asynchrone Workloads aus der Gefahrenzone geleitet und in cloud-basierte Content-Filter geleitet werden. „Das erlaubt es, die Firewall-Infrastruktur im Enterprise-Umfeld zu skalieren, weil die Computing-Power in der Cloud praktisch unbegrenzt ist", so Alge. Für die Administratoren ändere sich bei diesem Ansatz nichts. Wie bisher seien sämtliche Firewall-Funktionen über eine einzige Konsole steuerbar. Die IT-Umgebung lasse sich so sauberer und vorhersehbarer gestalten; zugleich seien cloud-basierte Scanning-Methoden besonders kostengünstig.

Die Cloud bezeichnet Alge als „seltsames Ding", weil es plötzlich intern und extern Daten und Apps gibt. Der Firewall fielen so Aufgaben zu, die früher Application Delivery-Kontrolleure zu erledigen. Gemeint ist damit beispielsweise, den Zugang zu bestimmten Anwendungen zu beschleunigen, den Traffic einer bestimmten User-Gruppe zu priorisieren oder Zugang zu bestimmten Daten freizuschaufeln. Es reiche jedenfalls nicht mehr aus, beim Datenverkehr Hürden für Eindringlinge aufzustellen, weil das auch die Prozesse der Mitarbeiter lähmen könnte. Auf der Agenda stehe stattdessen „Deep Application Detection": Anwendungen identifizieren und für die richtigen User bereitzustellen.

„Auch nach dem Übergang in die Cloud wird eine Firewall weiterhin nötig sein", schlussfolgert Alge. „Die Cloud wird sich zum Pendant der Firewall entwickeln, das einige Aufgabenbereiche übernimmt; trotzdem wird der Bedarf an einer Firewall weiterbestehen."
