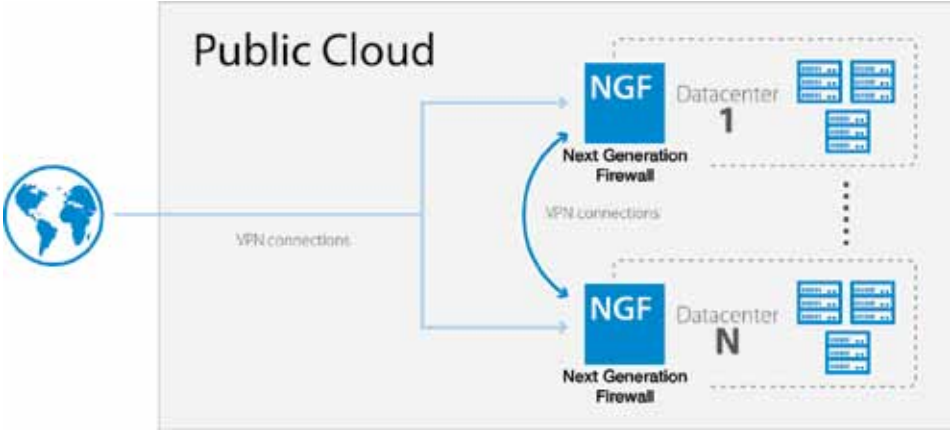
Kein Mut zur Lücke: Application-Firewalls für die sichere Cloud

Sicherheit dort herstellen, wo sich Anwendungen und Daten tatsächlich befinden

Wieland Alge, VP & GM EMEA bei Barracuda Networks

Längst haben Unternehmen und Organisationen die Vorteile, die das Arbeiten in der Cloud bietet erkannt – sei es der einfache Fernzugriff auf wichtige Daten, die effizienten Kollaborationsfunktionen oder die Entlastung der IT-Teams, da eine zeit- und kostenaufwändige Hardwarewartung entfällt. Im Zuge der Migration in die Public Cloud können Unternehmen jedoch auf eine Lücke zwischen dem bestehenden Schutz vor Ort und den neuen Sicherheitsanforderungen in der Cloud stossen. Diese gilt es unbedingt zu schliessen.



Wo die Public Cloud an ihre Grenzen stösst

Virtuelle Security Appliances gibt es schon länger. Sie bieten Tools wie Deep Packet Inspection in einem portablen, einfach bereitzustellenden Format für Private Clouds und virtuelle Rechenzentren. Angesichts der Weiterentwicklung von Public Cloud-Lösungen wie etwa Microsoft Azure, stellt der Schutz geschäftskritischer Applikationen in diesen Umgebungen eine erhebliche Herausforderung für IT-Teams in Unternehmen dar. Während Azure und ähnliche Produkte optimale Hardware-Sicherheit gewährleisten, fehlt es ihnen an geeigneten Workloadspezifischen Security-Lösungen etwa für den Schutz vor Exploits, bei der Implementierung von Anti-Malware-Lösungen oder der Abwehr komplexer, gezielter Angriffe. Solch fehlende Unterstützung auf der Anwendungsebene bedeutet für die Unternehmens-IT mitunter ein hohes Risiko. Beispielsweise, wenn datengesteuerte Applikationen auf VMs in der Cloud ablegt werden.

Sicherheit in der Cloud über das Grundsätzliche hinaus

Während on-Premises-Sicherheitslösungen wie Firewalls, VPNs oder IPS einen robusten Schutzschild bieten, unterliegen Anwendungen innerhalb von Cloud-Umgebungen lediglich einem Basis-Schutz, den gemeinsame Dienste oder das Server-Betriebssystem bieten. Cloud-Servicebetreiber wissen überdies nicht, was zum normalen Datenverkehr ihres Kunden gehört oder wobei es sich bereits um bösartigen Datenverkehr handelt. Um den Anforderungen an die Sicherheit in der Cloud zu entsprechen, müssen IT-Teams neue Sicherheits-Layer anhand eines virtuellen Sicherheitssystems implementieren, das sich innerhalb der Organisationsumgebung befindet. Eine Next Generation Firewall kann aufbauend auf Anwendungstransparenz und Kenntnis der Benutzeridentität, den Datenverkehr sowie die Bandbreite intelligent verwalten und IT-Administratoren dabei unterstützen, die Kontrolle über ihr Netzwerk zurückzuerlangen.

Die Lücke schliessen

Eine Cloud-basierte virtuelle Firewall adressiert eine Reihe von Sicherheitsanforderungen, darunter:

- Sicheres Rechenzentrum: Eine virtuelle Firewall kann Datenverkehr zum oder vom Internet, zwischen virtuellen Netzwerken oder zwischen den Mandaten filtern und verwalten, um das virtuelle Rechenzentrum zu schützen. Sie kann zudem ein physisches Rechenzentrum sicher auf die

Cloud erweitern, was vor allem dann wichtig wird, wenn Lösungen in die Cloud migriert werden sollen und daher eine sichere Verbindung zwischen der Cloud-Umgebung und der lokalen Infrastruktur benötigt wird.

- Sicherer Fernzugriff: Während die für die Konfiguration von VPN-Gateways eingesetzten Standard-Tunnel aus Verschlüsselungs- und Datenschutzperspektive auf jeden Fall sicher sind, bieten sie nicht das Mass an Steuerung, das zahlreiche IT-Konzerne mit ihrer Hardware-basierten Firewall erreichen. Eine virtuelle Firewall liefert die fortschrittliche Zugriffsrichtlinien-, Filter- und Verbindungsverwaltung, die für die Bereitstellung von Client-Zugriff auf die Cloud erforderlich ist. Mit Blick auf verschlüsselte Inhalte stellt die virtuelle Firewall sicher, dass alle Daten (unabhängig von Quelle oder Zielort) den gleichen Schutzmassnahmen unterliegen, die eine Hardware-basierte Firewall vor Ort bieten würde.
- Identität: Da die meisten Cloud-Plattformen nicht dafür entwickelt wurden, bösartige Absichten zu erkennen und darauf zu reagieren, ist die virtuelle Firewall für die Aufrechterhaltung der Integrität und Vertraulichkeit von Apps und Daten massgeblich. Sie sollte sich in die Lösungen der meisten namhaften Anbieter von Zugriffskontrolllösungen integrieren lassen und ein breites Spektrum granularer, richtlinienbasierter Filter-Tools bieten.
- Verwaltung: Während Cloud-Anbieter typischerweise Mandantenisolation und -sicherheit bieten, wird für eine effektive Verwaltung der Mandantenumgebung eine Cloud-basierte Firewall benötigt. Diese wird für das Management der Performance, der Nutzung, der Sichtbarkeit, des Reportings, der Konfiguration und der sonstigen Funktionen eingesetzt, für die normalerweise interne Verwaltungstools zur Anwendung kommen. Die Sicherung von Anwendungen und Daten in der Cloud ist mit eigens dafür entwickelten Tools viel einfacher. Eine Cloud-basierte Application-Firewall kann dort Sicherheit

bieten, wo sich die Anwendungen sowie die Daten tatsächlich befinden, und so die Lücke zwischen der Netzwerksicherheit on-Premises und den Anforderungen an die Cloud-Sicherheit schliessen. In diesem Fall ist «kein Mut zur Lücke» die bessere und vor allem sichere Entscheidung.

ÜBER BARRACUDA NETWORKS (NYSE: CUDA)

Barracuda vereinfacht die IT-Infrastruktur durch Cloud-fähige Lösungen, die es Kunden ermöglichen, ihre Netzwerke, Applikationen und Daten standortunabhängig zu schützen. Über 150.000 Unternehmen und Organisationen weltweit vertrauen den leistungsstarken, benutzerfreundlichen und kostengünstigen Lösungen, die als physische oder virtuelle Appliance sowie als Cloud- oder hybride Lösungen verfügbar sind. Beim Geschäftsmodell von Barracuda steht die Kundenzufriedenheit im Mittelpunkt. Es setzt auf hochwertige IT-Lösungen auf Subskriptions-Basis, die das Netzwerk und die Daten der Kunden umfassend schützen. Weitere Informationen sind auf www.barracuda.com verfügbar.

www.barracuda.com