

Duell ‐ Enemy at the Gates



Thorsten Freitag, 2011-22-11

Aktuelle Geschäftsabläufe sind von Datenverbindungskanälen abhängig. Aber jeder Kanal, den ein Unternehmen öffnet, stellt zugleich ein entsprechendes Risiko für den Datenverkehr der Webanwendung in und aus Ihrem Rechenzentrum dar. Nicht nur die Zahl der DDoS-Angriffe (Distributed Denial of Service) nimmt zu, es treten auch immer mehr technisch ausgefeilte Angriffe auf Anwendungsebene auf, in zum Teil nie dagewesener Form.

Die Wikileaks-Angriffe Ende des Jahres 2010 haben dazu geführt, dass viele Unternehmen ihre Vorstellungen von einem effektiven Schutz für ihre Webanwendungen neu überdacht haben, die ja im Grunde „Fenster zur Welt“ sind. Einige der großen Unternehmen mussten selbst erleben, wie herkömmliche Firewalls von Drittanbietern aufgrund der immensen Datenmasse geradezu umfielen. Ihre Fähigkeit, Millionen an neuen Verbindungen zu verarbeiten, erwies sich als unzulänglich.

F5 gab vor kurzem eine globale Umfrage (darunter mehrere Hundert Unternehmen aus Europa) unter mittelständischen und großen Unternehmen in Auftrag, um den Stand der Dinge neben den in den Medien berichteten Fällen zu ermitteln. Die Antworten von Mitarbeitern des gehobenen Managements ließen darauf rückschließen, dass es bei 100 % der Unternehmen in den letzten 12 Monaten zu Cyber-Angriffen kam, die finanzielle Verluste nach sich trugen.

Die Kosten dieser Verluste belaufen sich auf mehrere Hunderttausend Euro. Zugleich lassen sich Cyber-Angriffe aber auch immer schwerer abwehren, wobei vor allem DNS, Network-Layer-DoS und verschlüsselte Daten die größten Schwachstellen sind.

Auch wenn bereits zwischen einem Drittel und der Hälfte der Unternehmen bereits Application Delivery Controller (ADCs) als eine der wichtigsten Komponente in ihrer Sicherheitsinfrastruktur verwenden, denken nahezu 100 % der Unternehmen darüber nach, ADCs zu integrieren. Dies ist vermutlich nicht weiter überraschend, wenn man bedenkt, dass 42 % der Unternehmen bekennen, dass bei ihnen bereits einmal eine Firewall aufgrund der Network-Layer DoS-Verkehrslast zusammengebrochen ist.

Neues Landschaftsbild: neuer Ansatz

Geschäfts- und Technologie-Manager gaben an, dass Application Delivery Controller eine wichtige Rolle als Firewall für Internetrechenzentren spielen und sogar einige der herkömmlichen Sicherheitsvorkehrungen für Webanwendungen ersetzen. Unsere Botschaft ist einfach: Das technologische Landschaftsbild hat sich geändert, in gleichem Maße haben sich auch die Anforderungen an die Sicherheitsbereitstellung und Kontrolle geändert.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com