Mobile Payment sicherer machen!

max, 2012-04-04

Bei Spiegel Online las ich einen interessanten Artikel über einen „Dateneinbruch“. **Hacker stehlen 1,5 Millionen Kreditkartennummern!**

Das ist tragisch für betroffene Kreditkartennutzer, die auf die Sicherheit der Technik angewiesen sind und Ihren Kreditinstituten vertrauen. Das ist aber ebenso tragisch für Banken, die allein schon aus Seriösitätsgründen, eine der Grundlagen für Ihr Geschäft, ihren Kunden den höchsten Sicherheitsstandart garantieren sollten.

DDos-Angriffe sind nicht neu

Derartige Aktivitäten sind nicht neu: DDoS-Angriffe legten 2010 die Websites der Schweizer Postbank, Mastercard und Visa stundenlang zum Teil auch tagelang lahm. Das Paypal-Transaktionsnetzwerk wurde auch gestört, aber nicht vollständig zum Erliegen gebracht. Zu den Angriffen bekannt hat sich „Operation Payback“, ein loser Zusammenschluss anonymer Internet-Aktivisten aus dem Umfeld des Imageboards 4chan, die unter dem Deckmantel „Anonymous“ auch mit anderen Angriffen bekannt wurden.

Abwehr/Minderung

Um solche Überlastungen von kritischer IT-Infrastruktur zu vermeiden gibt es mehrere Möglichkeiten. Genügend Ressourcen um den Angriff zu überstehen ist eine Art. Man kann natürlich auch die Absender-IP-Adresse(n) des Angreifers in der Firewall im Angriffsfall manuell sperren, sodass diese Pakete verworfen werden. Eine dynamische zudem aber aufwendigere Vorgehensweise besteht im laufenden Abgleich der IP-Adressen mit Sperrlisten. Ebenso kann sich eine dynamische Filterung auf Datenmengen beziehen. Jeder IP-Adresse, die dabei einen einstellbaren Grenzwert (z. B. Datenvolumen pro Zeit) überschreitet, kann der Zugang komplett verweigert oder dessen Bandbreite beschränkt werden. Man muss dabei allerdings beachten, dass man möglicherweise auch legale Anwender blockt, denn im Internet werden Proxies eingesetzt, was dazu führt, dass viele Rechner mit der gleichen Absender-IP-Adresse am Ziel erscheinen. Das Verwenden von SYN-Cookies ist eine effektive Art zur Abschwächung von SYN-Flooding-Angriffen.

Schutz auf Netzwerk- und Applikationsebene

F5 Networks hat sehr viele umfangreiche DoS/DDoS-Lösungen in den „Application Delivery Controllern“ mit dem Namen BIG-IP integriert. Dieser Schutz umfasst Angriffe auf Netzwerkebene und Applikationsebene, denn die BIG-IP kann zwischen einem realen Browser und einem Rechner auf dem ein Skript abläuft unterscheiden. Sie unterstützt natürlich auch SYN-Cookies oder Dynamic Reaper gegen SYN-Flooding-Angriffe und kann Slowloris- und Slow POST-Angriffe von den Servern fernhalten. Die BIG-IP VIPRION kann bis zu 64 Millionen zeitgleiche Verbindungen aufrechthalten. Die BIG-IP bietet auch spezielle Lösungen gegen DNS-Angriffe, wie hoch skalierbare DNS Performance Lösungen mit DNSSEC-Unterstützung.

Haben wir ihr Interesse an Sicherheit geweckt? Dann lege ich Ihnen einen Artikel unseres Kollegen Alfredo Vistola, online zu finden bei der Computerwoche, ans Herz!

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