Ziehen Sie die richtigen Lehren aus den Spamhaus-Attacken?

Ralf Sydekum, 2013-03-06

Unsere Infosecurity Umfrage 2013 enthüllte eine besorgniserregende Tendenz: Viele Organisationen haben Probleme, mit den sich ständig weiterentwickelnden Sicherheitsbedrohungen Schritt zu halten. Ein großer Teil der Befragten gab auf der Infosecurity Europe 2013 Ende April in London zu, dass es ihnen schwerfällt, DNS-Verstärkungsangriffe (Reflection Attacks) zu verstehen. Und das, obwohl sich die größten Angriffe dieser Art erst kurz zuvor ereigneten. Nur 10 Prozent der Befragten Sicherheitsexperten waren überzeugt, dass sie die Funktionsweise der DNS-Verstärkungsangriffe verstehen und erklären können. Nur elf Prozent waren sich vollständig sicher, dass die normalen Abläufe nicht unterbrochen werden, falls eine derartige Attacke ihr Unternehmen treffen sollte.

Die Vielzahl der modernen Sicherheitsbedrohungen sorgt für große Verunsicherung unter den Befragten. 87 Prozent sind überzeugt, dass die Bedrohungen durch Cyber-Kriminelle, Hacktivisten und Hacker ihr Business stärker als je zuvor gefährden. Fast jeder Vierte nennt den BYOD-Trend als Hauptursache, warum seine Organisation anfälliger ist als zuvor. Auch die zunehmende Komplexität der Sicherheitsbedrohungen und ein Wechsel der „Bad Guys“ sorgen für Kopfzerbrechen: Anstatt mit Hackern sehen sich die Experten zunehmend mit Spionage und politisch motivierten Angriffen konfrontiert.

In unserer Umfrage kamen auch weitere Bedenken hinsichtlich des Schutzes der Infrastruktur und von Applikationen ans Tageslicht. So waren 83 Prozent der Befragten nicht überzeugt, dass die IT-Infrastruktur ihrer Organisation über konsistente Regeln in den Aufgabenfeldern „Sicherheit und Verfügbarkeit von Anwendungen“ verfügt.

„Die Größe und die Methode der Spamhaus-Attacken haben Weckruf-Charakter. Aber die Wahrheit ist, dass viele Sicherheitsexperten immer noch unzureichend auf diese neue Art von DDoS-Attacken vorbereitet sind und sich Sorgen über die potenziellen Auswirkungen eines derartigen Angriffs auf ihre Organisation machen“, ist demensprechend das Fazit von Joakim Sundberg, Worldwide Security Solution Architect hier bei F5.

Unternehmen möchten von den Vorteilen der erhöhten Agilität der Infrastruktur und den reduzierten Kosten profitieren, die aus einem Umzug in die Cloud resultieren. Gleichzeitig ist für sie sehr wichtig, alle Hintertüren für potenzielle Angreifer zu schließen. Konventionelle Firewalls sind dazu leider nicht geeignet, sie versagen im Zuge der Migration von Applikationen in die Cloud. F5 rät Ihnen daher dringend zu einer Application Delivery Firewall.

Wir bei F5 beobachten die Thematik und haben bereits dazu Stellung bezogen. Unsere Blogbeiträge zum Angriff auf die Süddeutsche Zeitung, zu den Attacken auf die Großbank JPMorgan Chase und zum Spamhaus-Angriff geben wertvolle Infos zum technologischen Hintergrund sowie erste Tipps und Hinweise, wie man sich erfolgreich schützen kann. In einem zweiten Schritt stehen Ihnen unsere Sicherheits-Experten gerne für weitere Fragen zur Verfügung. Sprechen Sie uns an!

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