WebWizard Blitz-News – Thema: Sicherheit – vom 17.12.2008

95% Spam 2009

Genau fünf Jahre nach Inkrafttreten des US-amerikanischen CAN-SPAM-Gesetzes prognostiziert Barracuda Networks für das kommende Jahr Spam-Anteile von knapp über 95 Prozent, die vor allem durch vermehrte Botnets-Angriffe verursacht werden.

Eine Analyse der mehr als einer Milliarde E-Mails, die täglich auf Barracuda Spam Firewalls treffen, zeigt, dass die Spam-Menge während des Jahres 2008 nahezu unverändert bei 90 bis 95 Prozent aller eingehenden E-Mails lag.

"Während das Jahr allmählich dem Ende zugeht, fragen sich viele, ob die Spam-Flut im kommenden Jahr tatsächlich noch schlimmer werden kann", so Stephen Pao, Vice President für den Bereich Product Management bei Barracuda Networks. "Einige Faktoren deuten darauf hin, dass 2009 ein leichter Spam-Anstieg zu erwarten ist. Gleichzeitig möchten wir aber daran erinnern, dass sich auch der Anteil seriöser Emails jedes Jahr erhöht."

Einer der Faktoren, die auf ein vermehrtes Spam-Aufkommen in den nächsten Monaten schließen lassen, ist das Auftreten von Spam aus Ländern, die bisher nicht für die Verbreitung unerwünschter E-Mails bekannt waren. So stehen etwa Brasilien und die Türkei an zweiter bzw. fünfter Stelle der von Barracuda Central aufgestellten Top-Ten-Liste der Spam-Ursprungsländer.

USA (24%)	Brasilien (7%)
Russland (6%)	Kanada (5%)
Türkei (4%)	Niederlande (4%)
Deutschland (4%)	China (3%)
UK (2%)	Polen (2%)

"Auffällig ist die Platzierung dieser Länder im Vergleich zu den üblichen Verdächtigen wie China und Russland", so Pao. "Unserer Meinung nach liegt der Grund unter anderem in der wachsenden Anzahl der Haushalte mit Breitbandinternetanschluss sowie in der starken Zunahme von Rechenzentren in verschiedenen Ländern rund um den Globus. Mit der steigenden Verfügbarkeit von Breitbandanschlüssen wächst natürlich auch die Reichweite von Botnet-Aktivitäten. Und gerade ungesicherte Rechenzentren sind die idealen Opfer für Hacker und Malware-Angriffe."

Bei der Analyse der mehr als eine Milliarde E-Mails, die täglich auf Barracuda Spam Firewalls treffen, wurde klar, dass die Mehrzahl der Spam-Kampagnen 2008 auf verborgene Absenderidentitäten setzte. Ausgespähte Web-Sites, die Nutzung kostenloser Hosting-Anbieter sowie der wechselweise Einsatz neuer Web-Domains innerhalb ein und derselben Spam-Kampagne – all diese Techniken sollten 2008 die wahre Identität der Spammer verbergen.

Neben Botnet-Aktivitäten und Techniken zur Identitätsverschleierung fielen 2008 vor allem die gekonnt gefälschten Phishinig-E-Mails auf, die auf Social-Engineering setzten. Allein im letzten Quartal nutzten mehrere Spam-Kampagnen vertraute Marken wie Microsoft und Google oder solche mit größerer Kundenbindung wie Hallmark und McDonald's, um User zur Preisgabe persönlicher Kundendaten aufzufordern oder sie dazu zu bringen, unwissentlich verseuchte Daten auf ihre Rechner herunterzuladen. "Natürlich sind Phishing-Versuche keine Neuerscheinung, dennoch ist die Professionalität der Fälschungen teilweise ziemlich erstaunlich", so Pao.