

Europa löst die USA als Spam-Hochburg ab – 12.02.2008

Rund 44 Prozent der weltweit verschickten unerwünschten Werbe-Mails stammen bereits aus Europa. Die USA sind auf einen Anteil von 35 Prozent zurückgefallen. Vor einem halben Jahr war dieses Verhältnis noch umgekehrt, ergibt eine aktuelle Untersuchung des US-Softwareherstellers .

Zurückzuführen sei dies unter anderem auf die Zunahme von Breitbandverbindungen in Europa. Im Top-10-Ranking der Länder mit den meisten Nutzern von schnellem Internet pro 100 Einwohner würden europäische Staaten bereits acht Plätze belegen. Der Ort des Versands der unerwünschten Nachrichten sei aber nicht immer ident mit dem Sitz des Urhebers. Nachdem viele Spammer von sich ablenken wollten, würden die Werbe-Mails oft mittels Trojaner über andere geographischen Regionen verschickt. Insgesamt sind im Jänner 2008 rund 78,5 Prozent der elektronischen Nachrichten als Spam identifiziert worden.

USA bei Phishing weiter voran

Bei Phishing-Mails haben die Vereinigten Staaten hingegen weiterhin mit 42 Prozent die Nase vorne. E-Commerce- und Bankenseiten standen dabei erneut am stärksten im Visier der Betrüger. Abgesehen von nicht länderspezifischen Domains wie .com, .net oder .org waren russische Phishing-Seiten (10 Prozent) am häufigsten, gefolgt von Frankreich (9 Prozent) und Deutschland (7 Prozent). Auf dem Vormarsch sieht Symantec außerdem betrügerische Websites, die auf von Laien einfach zu nutzenden fertigen Anwendungen basieren. Zwar sei die Anzahl eigenständiger Phishing-Seiten um 9,4 Prozent gesunken, Websites mit sogenannten "Phishing-Toolkits" hätten laut Untersuchung hingegen um 31 Prozent zugenommen.

Durch die Toolkits werde auch technisch weniger versierten Personen die Erstellung von täuschend echt erscheinenden Seiten ermöglicht, erklärte Candid Wüest, Sicherheitsexperte bei Symantec.

Inzwischen komme es aber zu regelrechten Grabenkämpfen zwischen den Kriminellen, weil die Programmierer der Phishing-Kits Hintertüren einbauen würden. "Stiehlt ein Phisher mit Hilfe dieses Werkzeugs dann sensible Daten, so werden diese heimlich direkt an den Urheber des Kits gesendet. Auf diese Weise betrügen sich die Kriminellen gegenseitig", so Wüest.

(APA)

<http://www.wirtschaftsblatt.at/home/schwerpunkt/itnews/312768/index.do>