



Kampf gegen Internet-Kriminalität: Verisign-Chef engagiert sich stärker für naiin!

Mitteilung vom 07. September 2005

Berlin – Der Deutschland-Geschäftsführer von VeriSign, Marcus Ross, hat das weltweit führende IT-Sicherheitsunternehmen verlassen, um sich künftig noch stärker bei der Wirtschaftsinitiative „no abuse in internet“ (naiin) engagieren zu können. Das gab die Initiative, die sich dem Kampf gegen Internet-Kriminalität verschrieben hat, am Mittwoch in Berlin bekannt. Ross soll vor allem die Bekämpfung des so genannten „Phishing“ weiter vorantreiben.

„Der Passwort-Diebstahl über manipulierte Websites hat sich zu einem neuen Schwerpunkt unserer Arbeit entwickelt“, erklärt naiin-Präsident Arthur Wetzel sichtlich zufrieden mit der personellen Verstärkung seines Teams. Über 33 Millionen Phishing-Attacken könnten derzeit pro Woche verzeichnet werden, so Wetzel. Und auch deutsche Bankkunden geraten immer wieder ins Visier der Passwort-Diebe.

„Wir gehen davon aus, dass die deutsch-sprachigen Phishing-Attacken gegenwärtig nur von ein paar wenigen Gangs initiiert werden“, erläutert Sicherheitsexperte Ross, der ab sofort für die Entwicklung effizienter Gegenmaßnahmen bei naiin verantwortlich zeichnet. „Darauf deuten beispielsweise identische Formulierungen und Rechtschreibfehler in den Mailings hin.“ Zugleich kündigte er eine umfassende auf den europäischen Raum ausgerichtete Anti-Phishing-Kampagne an.

„Es ist richtig, dass wir zur Zeit eine europäische Task Force aufbauen, die sich diesem Problem verstärkt annehmen wird“, bestätigte Wetzels. Ziel sei es, in Zusammenarbeit mit Internet-Nutzern, Providern und Geldinstituten die Bedrohung durch das Phishing binnen kürzester Zeit zu eliminieren. Die Task Force soll noch im Herbst dieses Jahres ihre Arbeit aufnehmen. Weitere Details will naiin in Kürze bekannt geben.

Hintergrund: Phishing

Beim Phishing handelt es sich um eine Form des Trickbetrugs, bei denen Methoden des Social Engineerings zur Anwendung kommen. Das Ziel eines Phishers besteht darin, an Passwörter und geheime Zugangsdaten von Internet-Usern zu gelangen. Im Allgemeinen versenden Kriminelle im Namen von seriösen Unternehmen Massen-E-Mails, in denen die Empfänger unter falschem Vorwand zum Besuch einer manipulierten Website aufgefordert werden. Dort sollen diese dann vertrauliche Informationen wie Passwörter, Kreditkarteninformationen oder Online-Banking-Daten aktualisieren. Besonders fies: Die E-Mails und Websites sind im Layout von vermeintlich vertrauenswürdigen Unternehmen wie Banken gehalten.