

Tatort Internet

Das organisierte Verbrechen macht vor dem Internet nicht halt. Mit bössartiger Software und weltweiten Netzwerken erbeuten Betrüger bei PC-Anwendern und Banken jährlich Millionen. Drei Experten erläuterten an der Veranstaltungsreihe „Verletzlichkeit der Informationsgesellschaft“ Sicherheitsrisiken des Internets und Möglichkeiten im Kampf gegen Internetkriminalität.



Stefan Frei vom Computer Engineering and Networks Laboratory der ETH Zürich demonstrierte, wie sich Betrüger an ahnungslosen Internetnutzern bereichern.

Spam-E-Mails landen meist ungelesen im virtuellen Papierkorb. Was jedoch, wenn man per E-Mail von der Firma des genutzten Online-Bezahlsystems plötzlich dazu aufgefordert wird, aufgrund eines Systemupdates seine gesamten Personalien inklusive seiner Kreditkarten-Nummer erneut auf der Firmenwebsite zu registrieren. Laut Studien fallen im Durchschnitt bis zu 40 Prozent der Internetnutzer auf solche betrügerischen E-Mails und Websites rein, die punkto Domain, Layout und Tonalität meist nur

sehr schwer vom Original zu unterscheiden sind. Bei den raffiniertesten sogar bis zu 90 Prozent.

Drei Referate zu den Themen Trickbetrügerei im Internet, Trojanische Pferde beim E-Banking und virtuelle Geldwäscherei machten vergangenen Donnerstag im Audimax der ETH Zürich den Auftakt zur Veranstaltungsreihe „Verletzlichkeit der Informationsgesellschaft“. Im Jahre der Informatik will die EMPA in Zusammenarbeit mit der Stiftung Risiko Dialog mit sechs Events auf die Risiken im Zusammenhang mit der Informatik aufmerksam machen.

Professionelle Netzwerke und virtuelle Geldwäscherei

Stefan Frei vom Computer Engineering and Networks Laboratory der ETH Zürich machte in seinem Referat klar, dass das Bild vom einsamen Hacker, der mit Pizza nächtelang vor seinem Computer sitzt und in fremde Systeme eindringt, längst überholt ist. Das „Phishing“, also Versuche über gefälschte WWW-Adressen an persönliche Daten eines Internetnutzers zu gelangen, geht auf weltweit organisierte Gruppen zurück, die äusserst professionell sowie profitabel arbeiten. Alleine im Jahr 2006 verloren englische Banken umgerechnet 97 Millionen Schweizer Franken durch Betrügereien an ihren Kunden. Entsprechende Zahlen für die Schweiz gibt es zurzeit noch nicht, doch gehen Schätzungen ebenfalls von Millionenverlusten aus.

Da es sich beim Betrug mittels Internet um ein relativ neues kriminelles Phänomen handelt, greifen die etablierten Schutzfunktionen und Gegenmassnahmen des Staates nur noch bedingt. Frei demonstrierte wie sich Kriminelle im Internet bis zur Identitätslosigkeit verstecken können. Bei seinem Demonstrationsbeispiel stand der Server mit der gefälschten Homepage in Hong Kong, die Internetdomain wurde in Palästina registriert und die E-Mail-Domain entstammte den USA. „Wohin schicken Sie nun die Polizei?“, fragte Frei rhetorisch das Publikum und beschrieb damit das Dilemma der Gesetzeshüter. Zusätzlich werden die Domains und die Standorte der Websites ständig geändert, so dass die aufgebauten Systeme enorm flexibel sind. „Macht die Polizei einen Schritt in die richtige Richtung, sind die Betrüger meist schon wieder zehn Schritte voraus“, so Frei.

Gelder waschen

Ein weiterer Grund dafür, dass Internetbetrüger nur schwer zu fassen sind, liegt in den relativ guten Möglichkeiten um „dreckiges“ Geld auf dem Internet reinzuwaschen, wie Marc Henauer von der nationalen Koordinationsstelle zur Bekämpfung der Internet-Kriminalität (KOBIK) und Melde- und Analysestelle Informationssicherung (MELANI) erklärte. Das Prinzip entspricht der herkömmlichen Geldwäscherei. Der Anonymitätsgrad der Täter auf dem Internet

ist jedoch höher. Zudem ist es laut Henauer sehr einfach sich auf dem Internet schnell und ohne grossen finanziellen Aufwand multiple Identitäten zu verschaffen, so zum Beispiel über Briefkastenunternehmen, die auf der gesamten Welt per Mausklick eröffnet werden können. Da die Gesetzgebungen punkto Deklarationspflichten von Geldern in den einzelnen Ländern stark differieren, können die Herkunftsspuren von Geldern über mehrere Schritte praktisch vollständig ausgelöscht werden. Eine zusätzliche Möglichkeit zur Geldwäsche bietet der Kauf von virtuellen Gütern mit realem Geld, wie dies zum Beispiel bei „Second Life“, einer dreidimensionalen virtuellen Umgebung, möglich ist.

Keine neuen Gesetze nötig

In der Podiumsdiskussion nach den einzelnen Referaten, befassten sich die Experten auch mit der Frage, wie die Internetkriminalität effizient angegangen werden kann. Eine ausdrückliche Regelung der strafrechtlichen Verantwortlichkeit der Provider, wie sie im Bundesrat im Februar besprochen und abgelehnt wurde, erachtet auch Stefan Frei als unnötig. Damit würden eher Vorteile für die Provider und nicht die Endverbraucher geschaffen. Zudem sei den Betrügern mit nationalen Gesetzen nicht zu begegnen, da diese international operierten. Für Frei muss deshalb das Bewusstsein der Internetnutzer gegenüber dem „Phishing“ und Risiken der virtuellen Welt verbessert werden – unter anderem durch Kampagnen und eine vertiefte Auseinandersetzung mit dem Thema in den Schulen. Er appellierte jedoch auch an die Softwarehersteller, die Möglichkeiten zum Selbstschutz der PC-Nutzer zu verbessern und vor allem zu vereinfachen. Für Marc Henauer ist in Zukunft auch eine Produkthaftung der Softwarehersteller denkbar. Rolf Gartmann, von der Organisation SWITCH/SWITCH-CERT, forderte die Zuhörer dazu auf, ihre Computer und vor allem auch die benutzte Software durch Updates laufend auf den neusten Stand zu bringen, da Sicherheitslücken in den Systemen von den Herstellern kontinuierlich behoben werden.

Die Referenten waren sich einig: Einen vollumfänglichen Schutz vor Internetkriminalität wird es nie geben. Ein Grund um nachts schlecht zu schlafen, wie der Moderator mutmasste, sei diese jedoch nicht. Wie einst beim Aufkommen der Automobile, müsse auch der Umgang mit Risiken der noch jungen Internetkriminalität erst gelernt werden. Je länger je besser werde man jedoch die Gefahren in den Griff kriegen, so die Voraussage der Experten.

Links und Referenzen:

- [Stiftung Risiko Dialog: Veranstaltungsreihe „Verletzlichkeit der Informationsgesellschaft“](#)
- [Computer Engineering and Networks Laboratory \(TIK\)](#)
- [Koordinationsstelle zur Bekämpfung der Internetkriminalität](#)
- [Gefahren im Internet erklärt von der Melde- und Analysestelle Informationssicherung](#)
- [Information Security Society Switzerland ISSS](#)

Leserkommentare:

Autor: Samuel Schläfli | Veröffentlicht: 11.03.08