

18. März 2008

# medien heft

---

## Internet-Kriminalität

### Verletzlichkeit der Informationsgesellschaft

Martin Fischer

Heute will kaum jemand mehr auf die Vorteile der neuen Informations- und Kommunikationstechnologien verzichten. Und wer den Nutzen des Internets einmal kennen gelernt hat, nimmt oft auch ein gewisses Risiko beim Datentransfer in Kauf. Doch zwischen Sorglosigkeit und diffusen Ängsten fehlt es zumeist an einem adäquaten Sicherheitsbewusstsein. Was die Information erleichtert, die Kommunikation beschleunigt und die Wirtschaft beflügelt erweist sich daher oft als die Achillesferse der Informationsgesellschaft.

Das Internet als Ort des grenzenlosen Austausches gerät zunehmend in den Sog von Kreisen, die gerade diese Offenheit für illegale Zwecke missbrauchen. Bei Privatperson ist neben der Privatsphäre auch das Bankkonto bedroht, während Firmen ihre Portale von Piraten gefährdet sehen, die für den Transfer schmutziger Gelder missbraucht werden. Die Behörden schliesslich sind zunehmend mit einer professionellen Internet-Kriminalität konfrontiert, der mit bestehenden Gesetzen kaum mehr beizukommen ist.

Solche Schwachstellen der Informationsgesellschaft unter die Lupe zu nehmen war Ziel der am 6. März an der ETH Zürich durchgeführten Veranstaltung „Internet-Kriminalität – Die Verletzlichkeit der Informationsgesellschaft“. Mit Sicherheitsfragen rund um das E-Banking befasste sich Rolf Gartmann vom „Computer Emergency Response Team“ (CERT) des „Swiss Education & Research Network“ (SWITCH), während Sicherheitsforscher Stefan Frei von der ETH Zürich die kriminellen Mechanismen anhand konkreter Betrugfälle demonstrierte. In welchem grösseren Kontext heute der Missbrauch im Internet zu sehen ist, zeigte Marc Henauer von der „Koordinationsstelle zur Bekämpfung der Internet-Kriminalität“ (KOBIK) und der „Melde- und Analysestelle Informationssicherung“ (MELANI).

---

#### Impressum

Medienheft (vormals ZOOM K&M), ISSN 1424-4594

Herausgeber: Katholischer Mediendienst, Charles Martig; Reformierte Medien, Urs Meier

Redaktion: Judith Arnold, Adresse: Medienheft, Badenerstrasse 69, Postfach, CH-8026 Zürich

Telefon: +41 44 299 33 11, Fax: +41 44 299 33 91, E-Mail: [redaktion@medienheft.ch](mailto:redaktion@medienheft.ch), Internet: [www.medienheft.ch](http://www.medienheft.ch)

kostenloser Bezug via Internet oder Newsletter: [www.medienheft.ch/mailling\\_abo/](http://www.medienheft.ch/mailling_abo/)

## Browser Poisoning – Sicherheitsproblem des E-Banking

*Phishing* und andere Formen böswilliger Manipulation von Browsern, Betriebssystemen und Applikationen stellt die ganze Online-Geschäftswelt vor neue Herausforderungen – insbesondere die Banken. Rolf Gartmann von SWITCH/CERT fragt sich daher, ob man den Webbrowsern überhaupt noch trauen kann.

Tatsächlich lassen sich eingebaute Hindernisse, die von Sicherheitsexperten als garantiert unüberwindbar ausgegeben werden, in Tests leicht aushebeln. Das zeigen simulierte Hacker-Attacken, bei denen es immer wieder gelingt, bei gängigen Banktransaktionen an sensible Daten zu kommen. Auf der anderen Seite sind auch eindeutige Defizite im Sicherheitsbewusstsein der Anwender festzustellen, was sie zur leichten Beute von Cyberkriminalität werden lässt. Dabei sehen sich die Kunden bereits jetzt mit immer höheren technischen Anforderungen konfrontiert, die von Nicht-Fachleuten kaum noch zu bewältigen sind, wie Gartmann einräumt.

Laut eines Forschungsberichts von Google (04.02.2008) ist gegenwärtig von etwa 3 Mio. böartigen Weblinks auszugehen und von rund 1,3 Prozent aller Suchanfragen, die über einen präparierten Weblink böartige Programme (*Malware*) auf die Festplatte von arglosen Nutzern einschleusen. Die „Verschmutzung“ der Benutzeroberfläche (*Browser Poisoning*) ist deshalb so gefährlich, weil sie nicht die einzige Falle ist, die dem Nutzer im Internet auflauert. Hinzu kommt das so genannte *Social Engineering*, das durch manipulative Tricks via E-Mail sensible Kundendaten erbeutet, böartige Programme (*Malware*) auf dem Computer installiert und sensible Benutzerdaten unbemerkt weiter vermittelt. Ein bekanntes Beispiel aus der Vergangenheit ist das „I love you“-Virus, das über E-Mail grosse Verbreitung finden konnte. Neue Bedrohungsszenarien stellen auch so genannte *Drive-By-Angriffspfade* dar, bei welchen das blosses Aufrufen einer URL ausreicht, um den Computer mit schädlicher Software zu infizieren.

Die Kombination von Gaunertricks und von Software-Schädlingen, die für den Laien nur schwer erkennbar sind, schafft die Voraussetzung, um Sicherheitsmechanismen wie Firewall und Virenschutz auszuschalten oder zu umgehen. Ein beliebter Trick von Gaunern ist, eine Website so zu gestalten, dass sie dem Portal einer Bank zum verwechseln ähnlich sieht. Gibt der treuselige Bankkunde Benutzer- und Passwort in Textfelder ein, so können diese Daten von den Urhebern der gefälschten Webseite abgefangen und die Bank-Konten geplündert werden. Zwar stellen die Banken mit *Fraud Detection*-Systemen rasch Unregelmässigkeiten im Kontenverlauf fest, aber eigentlich ist es dann schon zu spät.

Während Banken über ausgeklügelte Sicherheitssysteme verfügen, um die Risiken bei elektronischen Transaktionen weitgehend zu minimieren, ist das benutzerseitige Kommunikationsfenster eine eigentliche Schwachstelle. Denn die Browser sind, wenn sie auf den Markt kommen, nie auf alle Eventualitäten vorbereitet und ein ständiges Ziel von Hackern. Sicherheitslücken offenbaren sich oft erst im Nachhinein und die Browser – wie übrigens auch andere Anwendersoftware und die Betriebssysteme – müssen daher fortwährend aktualisiert werden. Viele Nutzer verzichten aber aus Bequemlichkeit auf die Installation so genannter Sicherheitspatches und öffnen damit Angriffen von Hackern Tür und Tor.

Am besten kann man sich vor Betrugereien im Internet schützen, wenn man sich des Sicherheitsrisikos bewusst ist und eine regelmässige Aktualisierung der Programme vornimmt. Dazu gehört insbesondere auch der Virenschutz, der in keinem Computer-

system fehlen sollte und nur durch ein regelmässiges *update* die neuesten Viren, Würmer und trojanischen Pferde erkennen kann. Wer ganz sicher gehen will, kein Opfer von Internet-Attacken zu werden, entscheidet sich für eine Kombination von Betriebssystem und Browser, die nicht zu den gängigen Softwarepaketen gehören. Denn „Monokulturen“, wie sie z.B. Microsoft häufig auf den Computern installiert, haben eine massenhafte Verbreitung und gehören deshalb zu den bevorzugten Zielen von Internet-Attacken. Bereits die Systeme von Apple sind dafür bedeutend weniger anfällig.

### Phishing – Trickbetrüger auf Datenfang

*Phishing*, der arglistige Versuch, über gefälschte E-Mails oder Webseiten an vertrauliche Daten zu gelangen, ist auch ein Forschungsgegenstand von Stefan Frei, Dozent an der ETH Zürich im IT-Sicherheitsbereich. Als „ethischer Hacker“ weist er auf eine sehr aktive und kreative *Underground Community* hin, die sich dem Ausnehmen von unvorsichtigen Anwendern verschrieben hat. Dabei räumt er mit den Klischees auf, dass es sich bei Hackern um clevere Jungs handelt, die sich einen Lausbubenstreich erlauben: „Heute haben wir es mit hochgradig organisierten, professionellen Verbrechern zu tun, die schnell und wendig operieren“. Im Internet lässt sich heute auf alle erdenkliche Arten viel Geld verdienen – legal wie auch illegal. Dem relativ kleinen Risiko für die Hacker steht den britischen Banken laut einer Studie der BBC ein Schaden von rund 45.7 Mio. £ gegenüber (vgl. BBC, 13.12.2006).

Um illegalen Zugriff auf ein Bankkonto zu bekommen, legen professionelle Betrüger im Quellcode von Webseiten versteckte Verweise an, um die Nutzer auf „gekaperte Webseiten“ zu führen und ihnen dort ihre persönlichen Daten abzunehmen. Dabei sind die Spuren für Spezialisten nur schwer zurückzuverfolgen, auch wenn sich Indizien wie unterschiedliche Schriftarten, widersprüchliche Informationen oder verdächtige Personaldaten auf den gefälschten Webseiten ausmachen lassen. Gesetzliche Massnahmen und Gegenstrategien gegen solches Treiben hinken der Entwicklung immer hinterher. Klar ist lediglich, dass die unwissenden Betroffenen von gekaperten Plattformen rechtlich nicht belangt werden können.

Anders steht es mit den *Money Mules*, den „Geldesel“, die sich für illegale Geldtransaktionen instrumentalisieren lassen. Wer eine E-Mail erhält mit der Bitte, einem Fremden zu helfen, sein Erbe anzutreten, sollte von solchen Geschäften die Finger lassen. Denn Unwissen schützt vor Strafe nicht, und ehe man es sich versieht, kann man der Mithilfe zur Geldwäscherei beschuldigt werden. Die Drahtzieher hingegen werden kaum je entdeckt. Eine weitere Geissel der Informationsgesellschaft ist *Mule Recruitment*. Darunter versteht man Geldwäscherei, die über undurchsichtige Firmenwebseiten abgewickelt wird. Zu diesem Zweck werden „gehackte“ Computer zu so genannten *Botnets* zusammengeschlossen. *Botnets* sind zuweilen riesige Netzwerke von illegal erschlossenen und kontrollierten Rechnern, welche ohne Wissen ihrer Besitzer zu eigentlichen „Geldwaschmaschinen“ umfunktioniert werden. Über *Money Mules* schliesslich wird das schmutzige Geld wieder in den legalen Geldkreislauf zurückgeführt.

### E-Laundering – Geldwäscherei im Internet

Die strafrechtliche Verfolgung von *E-Laundering*, der Geldwäscherei im Internet, ist nicht trivial, denn der Ablauf ist kaskadenartig über verschiedene Computersysteme verteilt, die sich in verschiedenen Ländern befinden und somit unterschiedlichen ge-

setzlichen Bestimmungen unterliegen. Zum Beispiel ist die Registrierungspraxis bei *Domain-Name-Providern* nicht überall transparent, weshalb die Identität von Domain-Besitzern nicht immer ausgemacht werden kann. Dies schafft Grauzonen im Internet.

Nach Einschätzung von Frei befinden wir uns immer noch in einer frühen Phase der Internet-Entwicklung, was die Handhabung und Kulturtechnik betrifft. Gemäss einer Studie der Universitäten Harvard und Berkeley (2006) sind rund 90 Prozent einer Versuchsgruppe auf betrügerische Tricks einer manipulierten Webseite hereingefallen. Eine Erkenntnis daraus ist, dass sich datensichere Abläufe im Internet erst einspielen müssen. Dazu sind gezielte Bildungsmassnahmen erforderlich, um bei den Nutzern das nötige Sicherheitsbewusstsein zu schaffen.

Die Erwartungen an den heutigen „Normal-User“ bezüglich Sicherheit im Internet sind allerdings bereits jetzt für viele an der Grenze des Zumutbaren. Denn abstrakte Risiken in komplexen Systemen sind schwer erkennbar. Es braucht daher eine interdisziplinäre Sensibilisierung der Nutzer. Oder mit anderen Worten: Der Kreativität der Betrüger muss mit der Kreativität der Nutzer begegnet werden.

Organisiertes Verbrechen missbraucht ungeschützte Computer als Plattformen für illegale Transaktionen, und die kritische Masse ist heute in vielfacher Hinsicht erreicht. Immer grössere Datenmengen und der Zuwachs an Benutzern schaffen eine Unübersichtlichkeit, die den Missbrauch erleichtert. Die Behörden werden nicht müde, auf die organisierte Kriminalität im Internet hinzuweisen, die übrigens auch als „Rentabilitätsindikator“ für das Online-Geschäft gelesen werden kann. Denn heute muss man von einer Korrelation zwischen Geldwäscherei im Internet (*E-Laundring*) und dem legalen elektronischen Handel (*E-Commerce*) ausgehen, so Marc Henauer, Vertreter von KOBIK/MELANI. Je rentabler die Online-Geschäfte, desto lukrativer die Cyberkriminalität.

Viele Kriminelle gehen auch im Internet nach bekannten Strickmustern ihren klassischen Tätigkeiten nach, allerdings auf dem letzten Stand der Technik und mit professionellem Know-how. Bei *E-Laundring* zum Beispiel wird „dreckiges Geld“ angelegt (*Placement*) und die Spuren anschliessend verwischt (*Layering*). Dies geschieht, indem die Geldwäscher schriftliche Belege vermeiden oder zum Verschwinden bringen (*Breaking of Paper Trail*). In der Regel werden solche Gelder möglichst „rechtshilfesicher“ angelegt, das heisst, auf Grund von unterschiedlichen Rechtsauffassungen oder mangels internationaler Abkommen werden strafrechtliche Konsequenzen umgangen. Derart gewaschene Gelder werden anschliessend wieder in das legale Wirtschaftssystem eingegliedert (*Re-Integration*) und der Kreislauf ist geschlossen.

Der Abwicklung solcher Geschäfte kommt die Virtualität des Internets natürlich entgegen, da es multiple Identitäten zulässt, welche die ideale Voraussetzung für illegale Transaktionen schaffen. Der hohe Anonymitätsgrad, die Geschwindigkeit des Datentransfers sowie die unterschiedliche Auslegung von Richtlinien und Gesetzen seitens der Finanzinstitute und Behörden schaffen für Kriminelle ein minimalisiertes Risiko. In der Grauzone zwischen legalen *Offshore*-Unternehmen und illegalen Geldanlagen spielt neben vorgespülten und wechselnden Identitäten auch die Verwendung von virtuellem Geld eine nicht zu unterschätzende Rolle. Zum Beispiel kann der *Lindon Dollar*, der in der virtuellen Spielwiese *Second Life* im Umlauf ist, jederzeit wieder in harte Währung eingetauscht werden, nachdem das Geld „strafverfolgungssicher“ investiert worden ist.

### Virtuelle Risiken – reale Schäden

Wie Marc Henauer erklärt, erfolgt die Strafverfolgung vorwiegend nach statistischen Vorgaben. Delikte, die zwar existieren, aber auf Grund ihrer „virtuellen Erscheinungsform“ schwer nachweisbar sind, fallen dabei oft durch die gesetzlichen Maschen. Trotz vieler strafrechtlicher Grauzonen sollten die Behörden aber vermehrt in die Pflicht genommen werden und Verdachtsmomente bei MELANI melden, so Henauer. Kommt jemand zu Schaden, kennen zwar viele Banken eine Kulanz, das heisst, es werden Teile der Schadenssumme zurückerstattet. Solche Reparaturleistungen beruhen aber auf Freiwilligkeit der Banken und es besteht kein Rechtsanspruch seitens der Kunden.

Trotz immer raffinierterer Umgehungsgeschäfte sind die Banken der eigentliche „Flaschenhals“ im Geldtransfer, weshalb sich gerade bei den Banken immer wieder illegale Geldströme nachweisen lassen. Hinweise auf unlautere Geschäfte sind etwa Unregelmässigkeiten im Zahlungsverkehr, so genannte Ausreisser, die beim *Fraud Management* der Banken und Kreditinstitute auffallen.

Auch wenn beim *E-Banking* schon zahlreiche Vorkehrungen gegen Internet-Kriminalität bestehen, werden bei der Entwicklung neuer Lösungen die Sicherheitsüberlegungen oft zu spät einbezogen. Das „Restrisiko“ wird dabei grösstenteils dem Endnutzer aufgebürdet. Abgesehen davon, dass bei vielen Anwendern das Risikobewusstsein nur unzureichend ausgebildet ist, müssten die Sicherheitsvorkehrungen von Banken viel benutzerfreundlicher werden. Hier fehlt es an gezielten Schulungen auf allen Bildungsstufen, die den Laien ebenso erreichen wie den Experten.

Wie unterschiedlich der Handlungsbedarf eingeschätzt wird, zeigte etwa der jüngste Entscheid des Bundesrates, auf ein Gesetz zur gezielten Bekämpfung der Internet-Kriminalität zu verzichten (NZZ, 29.02.08). So schwierig es ist, den virtuellen Mächtschaften habhaft zu werden, so bescheiden ausgebildet ist das Problembewusstsein.

Martin Fischer ist freier Journalist

Die von Thomas Dübendorfer moderierte Veranstaltung „Internet-Kriminalität – Die Verletzlichkeit der Informationsgesellschaft“ fand statt am 6. März 2008 im Auditorium Maximum der ETH Zürich. Die Veranstaltung wurde durchgeführt von der „Information Security Society Switzerland“ (ISSS) im Rahmen der „Informatica 08“ und einer Veranstaltungsreihe der Stiftung „Risiko-Dialog“, unterstützt von „Zurich Information Security Centre“ (ZISC) und „Swiss Security Day“.

Es war die erste Veranstaltung der Reihe „Verletzlichkeit der Informationsgesellschaft“ der „Eidgenössischen Materialprüfungsanstalt“ (EMPA) und der „Stiftung Risiko-Dialog“, die es sich zum Ziel gesetzt hat, für gesellschaftliche Fragen und Risiken im Umgang mit den neuen Informations- und Kommunikationstechnologien zu sensibilisieren. Die Stiftung stützt sich auf eine öffentlich-rechtliche Trägerschaft bestehend aus Vertretern der Wissenschaft, Wirtschaft und Verwaltung, darunter Cisco Systems Schweiz GmbH, Siemens Schweiz AG, die Hasler Stiftung, die Hochschule St. Gallen (HSG), die ETH Zürich, der Eidgenössische Datenschutzbeauftragte (EDÖB) und das Bundesamt für Kommunikation (BAKOM). Weitere Themen der Veranstaltungsreihe sind: „Pergament oder Elektronik – Hat die Vergangenheit noch Zukunft?“ (08.05.), „Geschlossene Informationsgesellschaft? Digitale Kultur zwischen geistigem Eigentum und offenem Zugang“ (05.06.), „Datenschutz: In Zukunft überflüssig oder lebenswichtig?“ (25.09.), „Blackout: Vernetzt – verletzt?“ (29.10.) und „Computer im Körper: Vom homo sapiens zum Roboter?“ (27.11.).

Programm:

<http://www.risiko-dialog.ch/Veranstaltungen>

<http://informatica08.ch/misc/Verletzlichkeit.pdf>

# medien heft

## Links:

Bundespolizei (FEDPOL):

<http://www.fedpol.admin.ch/fedpol/de/home.html>

Eidgenössische Materialprüfungsanstalt (EMPA), Abteilung Technologie & Gesellschaft:

[http://www.empa.ch/plugin/template/empa/124/\\*/--/l=1](http://www.empa.ch/plugin/template/empa/124/*/--/l=1)

Informatikstrategieorgan Bund (ISB):

<http://www.isb.admin.ch/>

Informatica 08:

<http://www.informatica08.ch>

<http://informatica08.ch/de/magazine/article/verletzlichkeit-der.html>

Information Security Society Switzerland (ISSS):

<http://www.issss.ch/>

Melde- und Analysestelle Informationssicherung (MELANI):

<http://www.melani.admin.ch/>

Stiftung Risiko-Dialog:

<http://www.risiko-dialog.ch/Themen/Kommunikationstechnologien/313>

Swiss Security Day:

<http://www.swisssecurityday.ch>

Swiss Education & Research Network (SWITCH):

<http://www.switch.ch>

SWITCH Computer Emergency Response Team (CERT):

<http://www.switch.ch/cert/>

Zurich Information Security Centre (ZISC):

<http://www.zisc.ethz.ch/>

## Quellen:

BBC News: "Online banking frauds 'up 8'000%'". December 13th, 2006:

[http://news.bbc.co.uk/2/hi/uk\\_politics/6177555.stm](http://news.bbc.co.uk/2/hi/uk_politics/6177555.stm)

Furger, Michael (2008): Rechtsexperte für den Cyberspace – Christian Schwarzenegger, Rechtsprofessor. In: Neue Zürcher Zeitung, 03. März 2008:

[http://www.nzz.ch/nachrichten/zuerich/rechtsexperte\\_fuer\\_den\\_cyberspace\\_1.682121.html](http://www.nzz.ch/nachrichten/zuerich/rechtsexperte_fuer_den_cyberspace_1.682121.html)

Gerny, Daniel (2008): Verzicht auf Gesetz gegen Internetkriminalität. In: Neue Zürcher Zeitung, 29.02.2008:

[http://www.nzz.ch/nachrichten/schweiz/verzicht\\_auf\\_gesetz\\_gegen\\_internetkriminalitaet\\_1.680465.html](http://www.nzz.ch/nachrichten/schweiz/verzicht_auf_gesetz_gegen_internetkriminalitaet_1.680465.html)

Google Technical Report provos-2008a: „All Your iFRAMEs Point to Us“. Niels Provos, Panayiotis Mavrommatis, Moheeb Abu Rajab, Fabian Monrose. February 4th, 2008:

<http://research.google.com/archive/provos-2008a.pdf>

Harvard University/ UC Berkeley (2006): „Why Phishing Works“. Rachna Dhamija, J.D. Tygar, Marti Hearst:

[http://people.seas.harvard.edu/~rachna/papers/why\\_phishing\\_works.pdf](http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf)

Informatikstrategieorgan Bund (ISB) (2007): Schweizerische Eidgenossenschaft (2007): Informationssicherung. Lage in der Schweiz und international. Halbjahresbericht 2007/1 (Januar bis Juni); in Zusammenarbeit mit der Koordinationsstelle zur Bekämpfung der Internet-Kriminalität (KOBIK).

Schwarzenegger, Christian (2008): Strafbare Handlungen im Internet – wer ist verantwortlich? Fehlende gesetzliche Regelung in der Schweiz schafft Rechtsunsicherheit. In: Neue Zürcher Zeitung, 28. Januar 2008:

[http://www.nzz.ch/nachrichten/medien/strafbare\\_handlungen\\_im\\_internet\\_wer\\_ist\\_verantwortlich\\_1.660813.html](http://www.nzz.ch/nachrichten/medien/strafbare_handlungen_im_internet_wer_ist_verantwortlich_1.660813.html)

Swissinfo.ch (2008): Kein neues Gesetz zur Bekämpfung der Cyberkriminalität. 28.02.2008.

Der Text befindet sich im Internet unter:

[http://www.medienheft.ch/kritik/bibliothek/k08\\_FischerMartin\\_01.html](http://www.medienheft.ch/kritik/bibliothek/k08_FischerMartin_01.html)