

# Aufrüstung der Cyber-Kriminellen

Artur P. Schmidt 13.11.2004

## Neue Dimension des Phishing beim Online-Banking: Von nachgebauten Websites zu Trojanern und zur direkten Manipulation der Websites von Banken

**Mit fremden Kartennummern bestückte Netzverbrecher können sehr leicht jede Menge Produkte bestellen und ihre elektronischen Spuren verwischen. Der Karteninhaber hat dann die Zeche zu bezahlen. Zwar zeigen sich Kreditkartenfirmen noch kulant, wenn dem Karteninhaber keine grobe Fahrlässigkeit im Umgang mit seinem Plastikgeld nachzuweisen ist, jedoch dürfte sich dieser Trend umkehren, wenn die Häufigkeit der Angriffe weiter deutlich zunimmt. Der in Hamburg ansässige "Chaos Computer Club" hat deutschen Banken schon öfters vorgeführt, wie leicht ein sogenannter "Kontoklau" durchgeführt werden kann. Die trojanischen Cyberpferde traben mittlerweile immer häufiger durch die Festplatten der User und spähen diese nach Passwörtern aus, das sogenannte Password-Fishing oder Phishing.**

Im Juli dieses Jahres warnte [1] die Deutsche Postbank ihre Kunden vor Pishing-Versuchen von Cyber-Kriminellen. Die Täter versenden E-Mails an willkürliche Mailadressen und Postbankkunden, in denen sie dazu aufrufen, einen Link anzuklicken. Einmal draufgeklickt wird der ahnungslose Kunde auf eine Webseite weiter geleitet, die genauso wie die Online-Banking-Seite der Postbank aussieht. Dort werden dann sämtliche Kontodaten wie PIN oder Transaktionsnummer vom Kunden verlangt.

Da ein Nutzer in der Online-Welt, ohne es oftmals zu merken, eine Menge Datenspuren (z.B. bei der Nutzung von Internetdiensten oder beim Einkaufen mit Kreditkarten) hinterlässt, ist es sehr viel einfacher, vorliegende Daten aus verschiedenen Anwendungszusammenhängen global zu recherchieren, zu verknüpfen und zu Profilen zu aggregieren (Persönlichkeitsprofile). Hierdurch kann jedoch die informationelle Selbstbestimmung ausgehöhlt werden, da Nutzer die Kontrolle darüber verlieren können, wer zu einem bestimmten Zeitpunkt was über eine andere Person weiß.

### Angriffswellen aus dem Osten

Die mangelnde Authentizität der Daten ermöglicht es den Cyberkriminellen zunehmend, die Identität eines anderen anzunehmen ("Identity-Theft"), ohne auswertbare Spuren einer solchen Manipulation zu hinterlassen. Dadurch werden besonders beim E-Commerce die Teilnehmer gezwungen, unter dem echten Namen aufzutreten, auch wenn dies gar nicht erforderlich wäre. Mit dem schlichten Betrachten einer Webseite oder mit einem Computerspiel fangen sich die User immer häufiger unliebsame Gäste ein und der ahnungslose User verliert die Kontrolle über seinen Rechner.

Trotzdem neigen deutsche Banken immer wieder zur Verharmlosung. Immer öfter verschicken Betrüger E-Mails, bei denen Kunden aufgefordert werden, Zugangsdaten zu ihren Bankkonten einzugeben. Das Phishing könnte ein großes Problem werden, wie Christian Pauli, Jurist beim Bundesverband der Verbraucherzentralen (VZBV), betont. Die Attacken kommen hierbei überwiegend aus Osteuropa, wie dies auch bei den Kunden der Postbank der Fall war. Sie wurden von Massenmails überschwemmt, die auf eine gefälschte Postbank-Webseite mit dem Länderkürzel für Russland führten. Die in Singapur ansässige OCBC Bank wurde ebenfalls Opfer eines Phishing-

Angriffs auf ihre Internet-Banking-Kunden. Die Website, auf der OCBC-Kunden vorgespiegelt wurde, sie seien auf der Original-Bank-Homepage und sollten ihre persönlichen Daten bekannt geben, wurde in Rotchina gehostet.

Der Hintergrund hat es in sich

In den USA ist in den vergangenen zwölf Monaten nach Schätzung der Marktforschungsfirma Gartner ein Schaden von über 2,4 Mrd. US-Dollar entstanden. Um solchen Attacken begegnen zu können, hat Deutschlands größter Internetanbieter T-Online jetzt seine Geschäftsbedingungen geändert. Nunmehr behält sich der Konzern vor, "bestimmte Leistungsfunktionalitäten, insbesondere die E-Mail-Kommunikation" zu sperren, wenn Kunden wissentlich oder unwissentlich zur Verbreitung von Internetschädlingen beitragen. Auch bei den Banken wird ausdrücklich darauf verwiesen, dass Kunden zum sorgfältigen Umgang mit ihren Zugangsdaten verpflichtet sind.

Doch bereits diesen Sommer meldete [2] der E-Mail-Sicherheitsdienst MessageLabs, dass es neue Methoden gibt, Log-In-Daten von Anwendern des Online-Banking zu stehlen, ohne dass die Anwender zum Mithelfen verführt werden müssen. Mussten bislang codierte Webseiten besucht werden, reicht es nunmehr aus, wenn man eine Phishing-Mail betrachtet. Im Hintergrund installiert sich ein Script, das alle Banking-Daten abfängt, sobald sich ein Benutzer beim nächsten Mal bei seiner Bank einloggt. Mit diesem simplen Trick können die Kriminellen schnell die Konten der Betroffenen leer räumen. Abhilfe bietet einzig ein Filter beim Provider oder das Abschalten von Windows Scripting Host. Die Zahl krimineller Mails, die von MessageLabs gefunden werden, steigt jedoch stetig an. Zwei weitere Beispiele belegen ebenfalls, dass die Angreifer zu immer raffinierteren Strategien übergehen:

Trojanisches Pferd attackiert britische Bank-Kunden

Sicherheitsexperten haben einen Red Alert [3] ausgerufen gegenüber einem Trojaner, der entworfen wurde, um in die Konten von britischen Bankkunden einzubrechen. Der Banker-AJ Trojaner (Troj/Banker-AJ) attackiert Kunden gemäss der Sicherheitsfirma Sophos nachfolgende Banken: Abbey, Barclays, Egg, HSBC, Lloyds TSB, Nationwide und NatWest.

Der Trojaner lauert auf infizierten Windows-PCs, bis die User ihre Zugangsdaten auf die Konten eingeben. Dann schlägt der kriminelle Code zu, um die Passwörter abzugreifen und fertigt Screenshots an. Diese Informationen werden dann auf die Rechner von entfernten Hackern überspielt, die dann in die Kundenkonten eindringen können. Neue Phishing-Methoden wie diese greifen immer weiter um sich und sind deshalb so gefährlich, weil diese keine gefälschten Seiten zum Abgreifen der Daten benutzen, sondern weil darauf gewartet wird, bis der User die realen Bankseiten aufruft.

Angriff auf den Original-Content australischer Banken

Phishers benutzen mittlerweile eine Betrugstechnik, die selbst den vorsichtigsten Kunden zum Narren halten kann. Die US-Firma SurfControl warnte [4] vor einigen Tagen, dass ihre Forscher eine Taktik beobachtet haben, die Fehler in der Webseite der australischen Banken SunTrust Bank und Citibank Australia nutzen. Phischer ersetzen Content auf den Originalseiten der Bank mit gefälschten Seiten, wodurch kein Kunde ernsthaft Verdacht schöpft.

In der Vergangenheit setzten Phischer vor allem auf Alarmtechniken, um Kunden zur Eingabe ihrer Daten auf gefälschte Sites zu bewegen. Dabei beuteten sie auch Sicherheitslücken in Microsofts Internet Explorer aus. Die neue Technik ist jedoch technisch so weit vorangeschritten, dass für Bankkunden kaum mehr eine Chance besteht herauszufinden, ob er sich auf sicherem Terrain bewegt.

## Auf Kryptographie setzen

Wenn Kunden aufgefordert werden: "Geben Sie uns Ihre E-Mail-Adresse, Ihre Anschrift und Ihre Kreditkartennummer" sollten bei diesen immer rote Alarmlichter angehen. Der beste Schutz bleibt deshalb nach wie vor, niemals vertrauliche Informationen auf ein unverlangtes E-Mail zu geben, auch wenn es von einer Firmenadresse versandt wurde. Auch sollte niemals auf Links von Webseiten geklickt werden, die in unaufgefordert zugesandten Meldungen eingebettet sind.

Heute durchläuft die Bestellung eines Konsumenten das Internet meist wie ein nicht verschlossener Brief. Es ist kein Problem für computerbewanderte Nutzer, mit einigen einfachen Kniffen die persönlichen Daten von Kunden abzulesen. Deshalb wird es zukünftig immer wichtiger, dass Daten ausreichend verschlüsselt sind, um so einen wirksamen Schutz herbeizuführen. Themen wie Tele-Shopping, Online-Banking, Kryptographie und Steganographie müssen Hand in Hand weiterentwickelt werden, um der kriminellen Manipulation von Daten Einhalt gebieten zu können.

In diesem Kontext wird auch die elektronische Beweisführung immer wichtiger. Der Begriff elektronische Beweisführung, im englischen auch Computer Forensics genannt, tauchte im Jahr 1991 erstmals auf und beschreibt den Einsatz von auf Computern basierenden Untersuchungs- und Analysetechniken, um potenzielle elektronische Beweise für Gerichte zu liefern. Nur wer sich den Herausforderungen der elektronischen Beweisführung stellt und seine Daten durch modernste Sicherungsmethoden schützt, ist vorbeugend in der Lage, finanzielle Schäden zu vermeiden.

## Links

- [1] <http://www.heise.de/newsticker/meldung/49049>
- [2] <http://www.heise.de/newsticker/meldung/52935>
- [3] <http://www.sophos.com/virusinfo/articles/ukbanktrojan.html>
- [4] <http://www.surfcontrol.com/news/newsitem.aspx?id=691>

**Telepolis** Artikel-URL: <http://www.telepolis.de/r4/artikel/18/18805/1.html>

---

Copyright © Heise Zeitschriften Verlag