

Presseinformation

BITKOM-Tipp

Zahl der Phishing-Opfer erreicht Höhepunkt

- Im vergangenen Jahr 4.100 Fälle mit 19 Millionen Euro Schaden
- 2008 erstmals Rückgang möglich
- Die wichtigsten Tipps gegen Datenklau beim Online-Banking

Berlin, 2. September 2008

Deutlich mehr Internetnutzer sind im vergangenen Jahr Opfer von Passwort-Betrügern geworden. Die Zahl der Phishing-Fälle beim Online-Banking ist erneut stark gestiegen – um 25 Prozent. Das geht aus einer Hochrechnung des Hightech-Verbandes BITKOM hervor, die sich auf die neuesten Daten der Landeskriminalämter stützt. Bundesweit hoben Kriminelle in mehr als 4.100 Fällen rund 19 Millionen Euro von Konten der Geschädigten ab. Die Schadenssumme liegt um ein Viertel höher als 2006. „Der Geheimzahlen-Klau hat durch immer raffiniertere Betrugsmethoden seinen bisherigen Höhepunkt erreicht“, sagte BITKOM-Präsidiumsmitglied Prof. Dieter Kempf bei der Vorstellung der Erhebung. Die meisten Opfer melden Bayern, Baden-Württemberg und Berlin.

2008 ist erstmals seit Jahren ein Rückgang der Phishing-Zahlen möglich. „Die Daten für das erste Halbjahr lassen erwarten, dass die Opferzahlen deutlich sinken“, gab Kempf bekannt. Da noch nicht alle teilnehmenden Bundesländer Zahlen für dieses Jahr genannt haben, handelt es sich aber um eine vorläufige Prognose. Statistisch gesehen ist sogar eine Halbierung der Fallzahlen denkbar. Auch die durchschnittliche Schadenshöhe nimmt demnach ab: Waren es 2006 und im vergangenen Jahr noch rund 3.700 Euro, so fehlen dieses Jahr nach jeder illegalen Überweisung im Schnitt etwa 3.200 Euro. In manchen Fällen gelingt es, betrügerische Überweisungen zu stoppen oder das Geld zurückzubuchen.

„Im Wettrüsten mit den Kriminellen stehen Verbraucher, Banken und die IT-Branche wieder etwas günstiger da“, kommentiert Prof. Kempf die positive Entwicklung. „Es trägt offensichtlich Früchte, dass die Wirtschaft immer bessere Sicherheitsmaßnahmen anbietet und die Nutzer

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel. +49. 30. 27576-0
Fax +49. 30. 27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Christian Spahr
Pressesprecher
Telekommunikation & Recht
Tel. +49. 30. 27576-112
Fax +49. 30. 27576-400
c.spahr@bitkom.org

Lutz Neugebauer
Bereichsleiter Sicherheit
Tel. +49. 30. 27576-242
Fax +49. 30. 27576-409
l.neugebauer@bitkom.org

Dr. Guido Brinkel
Bereichsleiter Medienpolitik
Tel. +49. 30. 27576-221
Fax +49. 30. 27576-400
g.brinkel@bitkom.org

Präsident
Prof. Dr. Dr. h. c. mult.
August-Wilhelm Scheer

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Presseinformation

Zahl der Phishing-Opfer erreicht Höhepunkt

Seite 2

umfassend informiert.“ Dem BITKOM reichen allerdings die rechtlichen Mittel gegen den Online-Betrug nicht: Bisher ist der Kontodaten-Klau nicht eindeutig verboten – die Polizei kann meist erst aktiv werden, wenn bereits ein Schaden vorliegt. „Schon der Versuch muss hart bestraft werden“, fordert BITKOM-Präsidiumsmitglied Kempf. „Wir brauchen dringend ein belastbares Gesetz gegen Phishing.“

Die Zahl der Betrugsversuche hat auch international zugenommen: Die Anti-Phishing-Initiative APWG registrierte in ihrer jüngsten Statistik vom Dezember 2007 weltweit über 25.000 Attacken pro Monat. Die Betrüger unterhielten rund 25.000 falsche Bank-Webseiten; die meisten davon in den USA (33 Prozent), China (22 Prozent) und Russland (9 Prozent). Lediglich drei Prozent der gefälschten Homepages waren in Deutschland registriert. „Schärfere Gesetze sind deshalb nur eines von mehreren Mitteln gegen Phishing“, erklärt Prof. Kempf. „Am wichtigsten ist es, die Maschen der Kriminellen zu kennen und die jeweils neuesten Schutzmethoden zu nutzen.“

Ein Grund für die bislang steigende Zahl der Phishing-Opfer sind immer effizientere Betrugsmethoden. Die meisten Betrüger setzen nicht mehr auf einfache E-Mails mit Links zu gefälschten Bank-Seiten, wo arglose Nutzer selbst ihre Kontodaten eingeben. In mindestens drei von vier Fällen, so eine BITKOM-Schätzung, schicken Kriminelle per E-Mail ein „Trojanisches Pferd“ – ein Schadprogramm, das Geheimzahlen im Hintergrund ausspäht und weiterleitet. Eine andere Art von Schadprogrammen leitet die Nutzer beim Online-Banking heimlich auf gefälschte Seiten weiter.

Nicht nur die Betrüger, auch die Banken haben indes aufgerüstet: Transaktionsnummern (TANs) sind zumeist nicht mehr beliebig einsetzbar, sondern an weitere Sicherheits-Hürden gekoppelt. Manche Kreditinstitute erhöhen den Schutz mit Kartenlesegeräten. Zukünftig könnten Überweisungen durch den elektronischen Personalausweis abgesichert werden. Er ist für 2010 geplant und soll dank eines Chips auch Web-

Presseinformation

Zahl der Phishing-Opfer erreicht Höhepunkt

Seite 3

Dienste sicherer machen. 55 Prozent der Internet-Nutzer würden den digitalen Ausweis beim Online-Banking einsetzen, ergab eine repräsentative Umfrage von forsa und BITKOM.

Zwar erstatten viele Banken einen Phishing-Schaden, wenn der Nutzer nicht grob fahrlässig gehandelt hat. Ob die Kunden einen Anspruch darauf haben, ist in der Rechtsprechung aber nicht eindeutig. Vorsorge ist deshalb unverzichtbar. „Mit ein paar Grundregeln lässt sich das Risiko leicht minimieren“, so Prof. Kempf. „Dann ist Online-Banking eine sehr sichere Dienstleistung, die zu Recht hohe Akzeptanz genießt.“ Insgesamt nutzen rund 22 Millionen Deutsche die Internet-Kontodienste ihrer Bank. Das geht aus Daten der europäischen Statistikbehörde Eurostat hervor und entspricht 35 Prozent der Einwohner zwischen 16 und 74 Jahren. Im EU-Vergleich liegen die Deutschen beim Internet-Banking auf Platz 7. Weit vorn sind Finnland und die Niederlande – dort nutzen jeweils zwei Drittel der Bevölkerung Online-Bankdienste.

Der BITKOM nennt die wichtigsten Anti-Phishing-Tipps:

1. Gesundes Misstrauen bei E-Mails

Banken bitten ihre Kunden nie per E-Mail, vertrauliche Daten im Netz einzugeben. Diese Mails sind immer gefälscht: Am besten sofort löschen. Das gleiche gilt für dubiose E-Mails von Unbekannten – vor allem, wenn eine Datei angehängt ist. Dahinter könnte ein Schadprogramm stecken, zum Beispiel ein Phishing-Trojaner. Solche verdächtigen Dateien auf keinen Fall öffnen! Auch dann nicht, wenn in der E-Mail mit einer Kontosperrung gedroht wird. Solche Einschüchterungen zählen zum Arsenal von Betrügern, um Bankkunden unter Druck zu setzen. PC-Nutzer sollten Drohungen ignorieren und Phishing-Mails nie beantworten.

2. Den Computer vor Schädlingen schützen

Eine gute Sicherheitsausstattung ist entscheidend. Ein Anti-Viren-Programm und eine so genannte Firewall, die den PC vor schädlichen Dateien aus dem Netz schützen, müssen vor der ersten Web-Sitzung

Presseinformation

Zahl der Phishing-Opfer erreicht Höhepunkt

Seite 4

installiert werden. Für diese Programme und das Betriebssystem des PCs werden regelmäßig Aktualisierungen angeboten. Nutzer sind gut beraten, die Updates umgehend zu installieren – am besten automatisch. Öffentliche Computer oder Internet-Cafés sind für Bankgeschäfte wenig geeignet.

3. Vorsicht beim Aufruf der Bank-Webseite

Beim Online-Banking sollte man die offizielle Adresse der Bank immer direkt eingeben oder über eigene Lesezeichen (Favoriten) aufrufen. Maßgeblich ist die Adresse, die die Bank in ihren offiziellen Unterlagen angibt. Die Verbindung zum Bankcomputer muss verschlüsselt sein. Das ist erkennbar an den Buchstaben „https“ in der Web-Adresse und einem Schloss- oder Schlüssel-Symbol im Internet-Programm (Browser). Zukünftig erkennen Verbraucher sichere Webseiten auch an einer grün hinterlegten Adresszeile, wenn sich der Betreiber vorab einer unabhängigen Prüfung unterzogen hat.

4. Moderne Transaktions-Verfahren nutzen

Für Überweisungen und andere Kundenaufträge sind Transaktionsnummern (TANs) nötig. In den Anfängen des Online-Bankings konnten die Nutzer einen solchen Code aus einer Liste frei wählen. Sicherer ist das iTAN-Verfahren, bei dem die Codes nummeriert sind. Ein Zufalls-generator der Bank bestimmt, welche TAN aus der Liste eingegeben werden muss. Noch weniger Chancen haben Kriminelle beim mTAN-Verfahren: Die Transaktionsnummer wird dem Kunden aufs Handy geschickt und ist nur wenige Minuten gültig. Weitere aktuelle Schutzverfahren sind eTAN und HBCI, bei denen der Kunde als Zusatzgeräte einen TAN-Generator oder ein Kartenlesegerät nutzt. PC-Nutzer sollten ihre Bank fragen und möglichst auf die modernsten Verfahren umstellen.

5. Mit Geheimzahlen richtig umgehen

Passwort (PIN) und Transaktionsnummern nicht auf dem PC speichern. Auch eine automatische Speicherung im Internet-Programm (Browser) ist riskant. Ein frei wählbares Passwort fürs Online-Banking sollte

Presseinformation

Zahl der Phishing-Opfer erreicht Höhepunkt

Seite 5

mindestens acht Zeichen lang sein und möglichst aus einer zufälligen Reihenfolge von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Fürs Online-Banking unbedingt ein separates Passwort wählen – keines, das auch für andere Dienste im Web genutzt wird. Empfehlenswert ist auch, die PIN regelmäßig zu ändern.

6. Falls es zu spät ist – Schadensbegrenzung

Nicht immer ist das Geld sofort weg, wenn Kriminelle eine Sicherheitslücke ausgenutzt haben. Opfer sollten zuerst die Bank alarmieren: Wenn eine Phishing-Überweisung nicht lange zurückliegt, kann sie manchmal noch gestoppt oder rückgängig gemacht werden. Entsteht doch ein finanzieller Schaden, unbedingt Anzeige bei der Polizei erstatten. Das ist nötig, um Geld von der Bank zurückzubekommen. Falls der Kunde nicht grob fahrlässig gehandelt hat, zeigen sich viele Banken kulant.

Zur Methodik der BITKOM-Erhebung: Erfragt wurden die Zahlen der Phishing-Fälle, in denen illegale Banktransfers stattgefunden haben, sowie die dabei geflossenen Summen. Quelle sind alle teilnehmenden Landeskriminalämter. Es sind Daten zu insgesamt elf Bundesländern vorhanden, die für rund 90 Prozent der deutschen Bevölkerung stehen, sowie eine Hochrechnung für ganz Deutschland.

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.200 Unternehmen, davon 900 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software, IT-Services und Telekommunikationsdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für bessere ordnungspolitische Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.