institut für
finanzdienstleistungen e.V.

infobrief 25/05

Dienstag, 16. August 2005 AT

Stichwörter

Online-Banking, Kontosicherheit, Abfischen von Zugangsdaten (*Phishing*)

A Sachverhalt

Vor einem Jahr, am 27. August 2004, hatte der VZBV vor einer neuen Methode der Datenbeschaffung und der Plünderung von Bankkonten, auch *Phishing* genannt, gewarnt. Ein Jahr später nehmen die Probleme mit der Datenabfrage zu. Einige Kreditinstitute wie die Postbank und die Dresdner Bank haben inzwischen darauf reagiert und ihre Sicherheitsstandards angepasst (FAZ online vom 9. Aug. 2005). Üblicherweise werden die Kunden in einer E-Mail aufgefordert, im Internet ihre Bankverbindungsdaten (Kontonummer und IBAN) anzugeben sowie das Kennwort (PIN) und einige Transaktionsnummern (TAN). Die Täter nutzen die Zugangsdaten, um von den Kundenkonten Geld zu überweisen. Aus aktuellem Anlass werden Möglichkeiten beschrieben, wie sich Kunden bei erfolgtem *Phishing* verhalten sollten und welche Rechtsansprüche bestehen.

B Stellungnahme

B.I Entstehung und Arten des Phishing

Durch das Online-Banking wurde den Verbrauchern ein großer Teil der Arbeit der Schalterangelstellten übergeben. Zum Ausgleich senkten viele Kreditinstitute in der gleichen Zeit die Gebühren für Girokonten. Das Outsourcing der Arbeit von den Kreditinstituten auf die Kunden war leider ein dornenreicher Weg, weil innerhalb der letzten 10 Jahre der Verbraucher zum Versuchskaninchen für unausgegorene Systeme wurde, angefangen von Dongles und Disketten, die man in den Computer steckt und die dann nicht funktionierten, über die Nutzung von Standardsoftware wie Quicken und MS-Money, die dann durch eigene Banksoftware abgelöst und nicht mehr gepflegt wurden, den Einstieg über T-Online, der dann abrupt zugunsten des Internets aufgegeben wurde und schließlich dem Allheilmittel des HBCI-Standards, der dann doch kein Standard wurde.

Jetzt scheint ein vorläufiges Ende der Odyssee erreicht zu sein, doch neue Belastungen kommen auf die Verbraucher zu. Eine E-Mail mit dem Absender der Volksbanken Raiffeisenbanken bittet Kunden dieser Bank mit den Worten:

"Die wichtige Mitteilung": "Der technische Dienst der Bank fuhrt die planmassige Aktualisierung der Software durch. Fur die aktualisierung der Kundendatenbank ist es notig, Ihre Bankdaten

iff institute for financial services | registered association | Director: Prof. Dr. Udo Reifner

Rödingsmarkt 31/33 Fon +49(0)40 30 96 91 - 0 www.iff-hamburg.de info@iff-hamburg.de HaSpa, BLZ 200 505 50
D-20459 Hamburg Fax +49(0)40 30 96 91 - 22 www.money-advice.net USt-IdNr. DE 17 434 03068 Kto. 1238 122921

erneut zu bestätigen. Dafuer mussen Sie unseren Link (unten) besuchen, wo Ihnen eine spezielle Form zum Ausfullen angeboten wird."

Der Link führt dann tatsächlich auf die Seite der Volksbanken, dort jedoch auf ein Image, das über die Seite gelegt ist und die PIN und 10 TANs abfragt. Man sollte meinen, dass kein Verbraucher den Banken ein solches Deutsch mit Grammatikfehlern und ohne Umlaute zutraut. Das ist aber leider nicht so wie Fälle aus der Praxis beweisen, die das Abfischen der Geheimnummern arglos ermöglichen. Ähnliche E-Mails erhält man im Namen der Postbank, Deutschen Bank, der Sparkassen, der Commerzbank, von Southtrust, CharterOne Bank und anderen etwa mit der Zeile:

"Sehr geehrter Kunde! Wir sind erfreut, Ihnen mitzuteilen, dass Internet - Ueberweisungen ueber unsere Bank noch sicherer geworden sind!... Dafuer muessen Sie unsere Seite besuchen, wo Ihnen angeboten wird, eine spezielle Form auszufuellen. In dieser Form werden Sie ZWEI FOLGENDE TAN - CODEs, DIE SIE NOCH NICHT VERWENDET HABEN, EINTASTEN."Dear Deutsche Bank Customer, We find that some of our members no longer have access to their email addresses. As result DeutscheBank server sent this letter to verify e-mail addresses of our clients. You must complete this process by clicking on the link below and entering in the small window your Deutsche Bank online access details." Oder: "Auf Grund dessen, bitten wir unsere Kunden instдndig, eine spezielle Form der zusдtzlichen Autorisation auszufьllen"

Bei vielen E-Mails fehlen regelmäßig die Umlaute, was auf ausländische Absender hindeutet. Oft ist auch die Sprache altmodisch und holprig, weil die Texte anscheinend mit Online-Tools Wort für Wort aus dem Englischen übersetzt werden. Mit der Zeit werden die Texte und die Methoden jedoch raffinierter werden. Üblich ist, dass die sichtbare Webadresse auf den ersten Blick mit der Adresse der Bank übereinstimmt.

Die Methoden der Abbuchungen sind unterschiedlich. Teilweise werden nur kleine Beträge abgebucht, um nicht aufzufallen (Computerwoche online vom 27. Juni 2005). Denkbar ist auch die Abbuchung größerer Beträge unmittelbar nach Weitergabe der Zugangsdaten.

B.II Rechtliche Bewertung

B.II.a Wirksame Überweisung?

Die Überweisung ist in § 676a BGB als gesonderter Überweisungsvertrag geregelt. Er kommt nach den allgemeinen Regeln zum Schuldrechtsvertrag durch Angebot und Annahme zustande (Gößmann/Look WM 2000 Sonderbeilage Nr. 1 S. 30 f.). Da der Kunde beim *Phishing* überhaupt keine Willenserklärung zur Überweisung abgeben will, sondern nur den vermeintlichen Anweisungen seines Kreditinstitutes zur Schadensvermeidung oder Sperrung von Online-Zugängen oder der vermeintlichen Aktualisierung von Software-Programmen etc. folgt, fehlt es in diesen Fällen an einer Willenserklärung des Kunden zu einer rechtsgeschäftlichen Handlung. Der Kunde hat auch Dritte nicht bevollmächtigt, Überweisungsaufträge zu erteilen. Eine Anscheins- und Duldungsvollmacht kommt ebenfalls nicht in Betracht, weil das Kreditinstitut davon ausgehen muss, dass die Überweisung vom Kunden selbst und nicht von einer Dritten Person kommt. Ein Überweisungsvertrag kommt daher nicht zustande.

Auf der anderen Seite ist das Kreditinstitut verpflichtet, bei einer wirksam erteilten Überweisung des Kunden diese „unverzüglich" gem. § 676a BGB vorzunehmen. Das Kreditinstitut kann bei der Verwendung von PIN und TAN nicht erkennen, ob die Weisung von dem Kunden oder durch Missbrauch eines Dritten veranlasst wird. Es wird daher regelmäßig zu einer Abbuchung der Geldbeträge auf ein fremdes Konto kommen.

Grundsätzlich muss das Kreditinstitut das Zustandekommen eines Überweisungsvertrages beweisen, wenn sie sich darauf beruft, für ihr Tätigwerden einen Ausgleich vom Kunden in Höhe des überwiesenen Betrages zuzüglich etwaig anfallender Gebühren zu verlangen. Ein Fälschungsrisiko der Unterschrift unter einen Überweisungsauftrag in Papierform trägt grundsätzlich das Kreditinstitut (Palandt § 676a BGB Rz. 11). Fraglich ist, ob die Verwendung von PIN und TAN als Beweis vor Gericht ausreicht, dass der Kunde einen Überweisungsauftrag erteilt hat. Aufgrund des seit einem Jahr bekannten Problems des Phishing und Aussagen von Experten, die den Schaden jährlich auf 70 Millionen Euro schätzen, ist die missbräuchliche Verwendung von PIN und TAN durch Dritte bekannt. Daher ist die Verwendung von PIN und TAN allein nicht dazu geeignet, den Beweis für einen Überweisungsauftrag des Kunden zu erbringen.

B.II.b Rückholbarkeit von erfolgten Zahlungen

Um ungerechtfertigte Abbuchungen von Konten auf einfache Art rückabwickeln zu können, sehen die AGB der Kreditinstitute Stornoklauseln vor. Die Stornoklausel in den AGB (Nr. 8 (1) AGB-Sparkassen) sieht vor, dass bis zum Rechnungsschluss ungerechtfertigt erhaltene Beträge von Konten Dritter zurückbuchbar sind (Bankrechts-Handbuch-Schimansky § 47 Rz. 32b). Reagieren die Kunden unverzüglich nach Erkennung des Missbrauchs ihres Kontos und verständigen das eigene Kreditinstitut, so können die überwiesenen Beträge in der Regel zurückgeholt und ein Schaden vermieden werden.

B.II.c Schadensersatzforderung des Kreditinstitutes gem. § 280 BGB

Hat das Kreditinstitut Geldbeträge auf Konten Dritter überwiesen, ohne dass ein Überweisungsauftrag bestand, kann das Kreditinstitut einen Schadensersatz gegenüber dem Kunden gem. § 280 BGB geltend machen, wenn sich der Kunde sorgfaltswidrig verhalten und damit den Schaden verursacht hat. Der Missbrauch des Online-Bankings durch Phishing ist mit den Fällen des Missbrauchs von ec-Karten vergleichbar. Die Kreditinstitute werden versuchen, sich auf einen Anscheinsbeweis zu stützen, dass der Missbrauch von PIN und TAN nur möglich war, wenn sich der Kunde sorgfaltswidrig verhalten hat.

Der Kunde hat Sorgfaltspflichten beim Online-Banking, die insbesondere das sichere Aufbewahren von Zugangsdaten und von Kennwörtern betrifft (Bankrechts-Handbuch-Schimansky, 2. Aufl., § 49 Rz. 29). Dieses soll ausschließen, dass (unbefugte) Dritte von den Daten Kenntnis erhalten und Überweisungen tätigen. In den Allgemeinen Geschäftsbindungen zum Online-Banking wird der Kunde in der Regel dazu aufgefordert, keine Daten an Dritte weiterzugeben und Kennwörter für das Online-Banking auch nicht gegenüber Mitarbeitern des Kreditinstitutes

zu offenbaren. Ein sorgfältig handelnder Kunde würde sich bei seinem Kreditinstitut telefonisch erkundigen, was die Aufforderung in der E-Mail für eine Bedeutung hat, weil eine Aufforderung des Kreditinstitutes, Zugangsdaten zu versenden, zumindest ungewöhnlich ist. Im Fall des erfolgreichen Phishing hat der Kunde die Zugangsdaten sogar bewusst herausgegeben. Allerdings wurde er über den Empfänger getäuscht, weil er davon ausging, dass es sich um eine Anfrage des Kreditinstituts handelt und nicht um Dritte. Der Link auf die Eingabemaske, der in der Regel der E-Mail beigefügt ist, entspricht oft den Internet-Seiten des Kreditinstitutes. Der Kunde muss nicht merken, dass er nicht auf der Internet-Seite seines Kreditinstitutes ist. Ein Kunde, der seine Daten an Dritte ohne Rückfrage bei seinem Kreditinstitut weitergibt, verletzt daher zwar seine Sorgfaltspflichten. Da der Kunde gewohnt ist, über das Internet Kontakt mit seinem Kreditinstitut aufzunehmen, ist ein vermeintliches „Einloggen" über den Link keine ungewöhnliche Reaktion des Kunden. Fraglich ist, welche rechtlichen Konsequenzen sich daraus ergeben.

Ein Kunde als Laie muss nicht mitbekommen haben, dass diese Art von Datendiebstahl existiert. Das Kreditinstitut dagegen wird über diese Art von Datendiebstahl frühzeitig durch ihre Kunden informiert werden. Ein sorgfältig handelndes Kreditinstitut würde daher als ersten Schritt alle seine Kunden ausdrücklich vor dieser Art von Datendiebstahl warnen und deutlich machen, dass sie als Kreditinstitut unter keinen Umständen derartige Daten abfragen würden. Zwar hat ein Kreditinstitut nur in sehr engen Grenzen Warn- und Schutzpflichten im standardisierten Zahlungsverkehr gegenüber seinen Kunden (Palandt § 676a Rz. 17). Doch begründet die Rechtsprechung dieses vor allem mit dem Massencharakter von Überweisungen. Im Fall des Phishing geht es nicht um eine einzelne Überweisung, sondern um den Versuch, Konten des gesamten Kundenstamms eines Kreditinstitutes für einen Missbrauch zu nutzen. Es geht daher nicht um Einzelbuchungen in einem Massenverkehr. Eine Warnung der Online-Kunden ist für das Kreditinstitut ohne großen Aufwand auf elektronischem Wege möglich. Angesichts dieser Dimension ist davon auszugehen, dass bei einem gezielten Angriff eines Kreditinstitutes dieses gegenüber seinen Kunden bei Kenntnis eine Warn- und Schutzpflicht hat.

Hat ein Kreditinstitut dieses unterlassen, hat sie sich mindestens genauso sorgfaltswidrig verhalten wie die Kunden. Wie die Beispiele der Postbank und der Dresdner Bank zeigen, ist das einzige effektive Mittel, die Datenabfrage für den Zugang zu dem Konto zu verändern, so dass ein Abfischen der Daten erschwert bzw. unmöglich gemacht wird. Ein Kreditinstitut, das ein bekanntermaßen betrugsanfälliges Zugangssystem zum Bankkonto weiterhin betreibt, handelt grob fahrlässig. Das Kreditinstitut, welches seine Kunden nicht unverzüglich vor dem Abfischen der Daten warnt, trifft zumindest eine Mitschuld. Wird das Sicherheitssystem trotz sich häufender Schäden nicht verändert, wiegt die Fahrlässigkeit des Kreditinstitutes so schwer, dass eine Sorgfaltspflichtverletzung des Kunden daneben zurücktritt.

B.II.d Mitverschulden des Kunden bei fehlender zeitnaher Kontrolle der Kontoauszüge

Das Zusenden von Abschlusssalden allein stellt keine Genehmigung der rechtsgeschäftlichen Buchungen durch den Kunden dar (siehe dazu: Bankrechts-Handbuch-Schimansky § 47 Rz. 51). Der Kunde hat jedoch, wie auch in den AGB der Banken und Sparkassen[1] festgelegt, eine Pflicht zur „unverzüglichen" und damit zeitnahen Kontrolle der Kontoauszüge. Ein (Mit-)Verschulden kann sich daher auch ergeben, wenn der Kunde nicht rechtzeitig seine Kontoauszüge kontrolliert.

Die Rechtsprechung erwartet von den Kunden „ein gewisses Maß an Kontrolle" (BGH NJW 1991, 487 (489), Bankrechts-Handbuch-Schimansky § 47 Rz. 49). Einmal im Monat sollte man daher seine Kontoauszüge grundsätzlich durchgehen. Aufgrund von Urlaub, Krankheit etc. kann sich im Einzelfall etwas anderes ergeben. Bei Kenntnis unberechtigter Abbuchungen sollte man unverzüglich sein Kreditinstitut verständigen, also in der Regel sofort bzw. im Laufe des Tages.

B.II.e Weitere Schutzmaßnahmen nach einem Missbrauchsversuch

Hat der Kunde seine Zugangsdaten aufgrund des Abfischens von Daten an Dritte weitergegeben und bemerkt dieses, sollte er sofort seine PIN ändern, herausgegebene TANs aufbrauchen bzw. im Zweifel sein Konto bis zur Klärung des Sachverhaltes sperren lassen, sein Kreditinstitut über das Abfischen eigener Daten und eventuell erfolgte unberechtigte Abbuchungen informieren und sich dieses schriftlich bestätigen lassen. Es ist denkbar, dass die Diebe erst Monate später mit der Abbuchung kleiner Beträge beginnen, so dass man auf jeden Fall als Kunde reagieren sollte, auch wenn noch keine unberechtigten Abbuchungen erfolgt sind. Siehe dazu auch die Ausführungen in dem Schreiben des VZBV.

B.III Fazit

Da die Kreditinstitute selbst die Kunden daran gewöhnt haben, auf dem Internet geheime Zugangsdaten und ihre persönlichen Daten einzugeben, ist eine Verwendung von Zugangsdaten bei einer vermeintlichen Aufforderung durch das Kreditinstitut aus Kundensicht nicht ungewöhnlich. Zeigt sich die Website der Bank selbst und gibt man die Daten dort ein, dann ist es für einen elektronischen Laien schwer verständlich, dass das fremde Seiten sind. Ein Kunde, der seine Daten an Dritte ohne Rückfrage bei seinem Kreditinstitut weitergibt, verletzt daher zwar in der Regel seine Sorgfaltspflichten. Ist der Missbrauchsversuch für den Kunden aber nicht ohne weiteres erkennbar und trifft das Kreditinstitut trotz Kenntnis des Phishings keine geeigneten Gegenmaßnahmen, so verletzt das Kreditinstitut seine Warn- und Schutzpflichten, Eine Sorgfaltspflichtverletzung des Kunden ist in diesem Fall von untergeordneter Bedeutung.

---

[1] Siehe z.B. Nr. 20 (1) g und h AGB-Sparkassen und Nr. 11 (4) Banken

Es ist zu hoffen, dass die Gerichte nicht wie bei der EC-Karte wieder die Fortentwicklung der Internetsicherheit durch die Anbieter dadurch blockieren, dass sie dem Kunden, der keinen Einfluss auf die Sicherheitsstandards hat, das Risiko aufbürden. Dieses setzt ökonomisch betrachtet falsche Anreize und fördert nur den Missbrauch. Immerhin haben ja in der Vergangenheit ein paar mutige Gerichtsentscheidungen dazu geführt, dass die Geldautomaten besser gegen Einblicke gesichert wurden und jetzt auch an jedem Automat das Hinweisschild steht, dass Dritte über die Schulter schauen könnten.

Es ist Aufgabe der Anbieter von Internetadressen und Online-Banking, solchen Missbrauch ihrer Seiten zu verhindern. Nur ein sicheres Internet ist auch für Online-Banking tauglich. Andernfalls werden die Kunden in Zukunft Online-Banking meiden und der Technik kein Vertrauen mehr entgegen bringen. Kurzfristig rechtliche Vorteile für die Kreditinstitute könnten langfristig das gesamte Online-Banking in Verruf bringen.

iff institute for financial services |registered association| Director: Prof. Dr. Udo Reifner

Rödingsmarkt 31/33 Fon +49 (0)40 30 96 91 - 0 www.iff-hamburg.de iff@iff-hamburg.de HaSpa, BLZ 200 505 50
D-20459 Hamburg Fax +49 (0)40 30 96 91 - 22 www.money-advice.net USt-IdNr. DE 17 434 03068 Kto. 1238 122921