

Phishing: Wer haftet wann wofür?

26.11.2006, 16:42 | Handel, Wirtschaft, Finanzen, Banken & Versicherungen

Pressemitteilung von: *Rechtsanwalt Dr. Thomas Schulte*

Als Spielart der Computerkriminalität ist das Phishing längst bekannt. Die juristischen Nachspiele ereignen sich aber zeitversetzt. Das gilt insbesondere, wenn sie bis zur endgültigen Klärung die Instanzen durchlaufen. Bereits vor einigen Monaten haben die Autoren über ein strafrechtliches Urteil des LG Darmstadt berichtet, in dem der „Finanzkurier“ eines Phishing-Täters der gewerbsmäßigen Geldwäsche für schuldig befunden wurde. Inzwischen gibt es auch vereinzelte zivilrechtliche Stellungnahmen, wobei zentrale Zweifelsfragen aber immer noch ungeklärt sind.

Das OLG Hamburg (1 U 75/06 vom 2.8.2006) hatte in zweiter Instanz den geradezu klassischen Phishing-Fall zu entscheiden: Die Klägerin hatte sich über das Internet als „Finanzagentin“ anwerben lassen und bei der beklagten Postbank ein Konto eröffnet. Ein mit der Klägerin kooperierender Phisher hatte das Internetbanking eines Bankkunden manipuliert und so einen Betrag von insgesamt 32.000 Euro auf das eigens hierfür errichtete Konto der Klägerin bei der Beklagten „umgeleitet“. Die Klägerin wiederum hatte das Geld ins Ausland transferiert. Kurze Zeit später stornierte die Postbank die Gutschrift und buchte den Betrag zurück auf das Konto der ausführenden Bank. Die Klägerin erhob Klage auf Rückgutschrift, die Postbank Widerklage auf Zahlung des negativen Saldos (das Konto selbst war inzwischen fristlos gekündigt worden). Das Landgericht Hamburg (334 O 10/06 vom 18.5.2006) hatte der Beklagten Recht gegeben: Sie sei zu dem Rücktransfer berechtigt gewesen, weil die Überweisung fehlerhaft gewesen sei. Der Kontoinhaber bei der ausführenden Bank habe zum einen nie einen Überweisungsauftrag erteilt, zum anderen liege in dem Verhalten der Klägerin ein Verstoß gegen das KWG. Ob die Klägerin außerdem von den illegalen Machenschaften des Phishers wusste und eine strafbare Geldwäsche begangen hatte, ließ das LG offen. Das OLG Hamburg wies die Berufung zurück und bestätigte die landgerichtliche Entscheidung in vollem Umfang. Die in dieser Entscheidung thematisierte Auseinandersetzung zwischen dem „Finanzagenten“ und seiner Bank läßt die eigentlich wichtige und immer noch ungeklärte Frage allerdings offen: Was gilt in solchen Fällen zwischen dem Phishing-Opfer und seiner Bank? Noch liegen hierzu keine Urteile vor; unter anderem, weil die Banken bislang stillschweigend reguliert haben. Dennoch wird diese Frage über kurz oder lang richterlich geklärt werden, denn die AGB für das Internetbanking stellen nur die Regel auf, dass die Weitergabe der PINs und TANs an Dritte nicht fahrlässig ermöglicht werden darf. In welchen Fällen aber von einer solchen Fahrlässigkeit auszugehen ist, dürfte zu Streitfragen führen und die Gerichte werden sie kaum in genereller und abstrakter Form beantworten können. Kaum ein technisches Gebiet unterliegt einer derartigen Dynamik, wie die Internetsicherheit. Um sie herrscht zwischen Saboteuren und Sicherheitstechnikern seit jeher ein permanenter Wettlauf. Aus diesem Grund entstand zum Beispiel das Pharming als Spielart des Phishing. Es ist eine technische Reaktion der Hacker auf die Warnung, den Bank-URL niemals über eine Verlinkung aufzusuchen, sondern ihn direkt in den Browser einzugeben. Kaum hatte sich diese Sicherheitsmaßnahme herumgesprochen, wurden Phishing-Attacken in neuer Form lanciert: Auch wenn der Internetnutzer die URL-Adresse selbst eintippt, muss sein Rechner diese in eine IP-Nummer konvertieren, die ihn zum gewünschten Server führt. Gelingt es einem Hacker, auf dem betreffenden Rechner ein Schadensprogramm zu installieren, kann dieser Konvertierungsvorgang so manipuliert werden, dass der Kunde zwar mit größter Sorgfalt seine Bank-Adresse eingibt und gleichwohl unbemerkt auf einem feindlichen Server landet, wo er Unbefugten seine Daten preisgibt. - Doch wer haftet nun wann und in welchem Umfang? Letztlich werden die Gerichte in jedem Fall eruieren müssen, in wessen Verantwortungsbereich die Schließung einer bestimmten Sicherheitslücke gelegen hätte. Ist also eine bestimmte Bank besonders anfällig, weil ihr Webauftritt leicht fälschbar ist? Ändert sie laufend ihre Bankingseite, so dass man Änderungen schwer erkennen kann? Wendet sie sich häufig per E-Mail an den Kunden, so dass er daran gewöhnt ist, auf diesem Weg mit ihr zu kommunizieren? Hat die Bank ihre Kunden nicht oder nur unzulänglich über eine neue Phishing-Welle informiert? Hat sie es versäumt, eine in einer Phishing-Mail genannte Website sperren zu lassen? Hat sie sich den Erfordernissen erhöhter Sicherheit technisch angepasst (etwa durch die Möglichkeit mehrstufiger Transaktionen)? Zu den Pflichten des Bankkunden dürfte es dagegen gehören, nur sein eigenes Gerät für das Telebanking zu benutzen, regelmäßig das Sicherheitszertifikat der Bankingwebsite zu überprüfen, Wurm- und Virenprüfungen durchzuführen, seine Browsersoftware upzudaten und dergleichen. In Bezug auf die Fahrlässigkeit kann auch die Beweislast zu Zweifeln führen. Muss der Kunde seine Sorgfalt oder die Bank dessen Sorgfaltswidrigkeit beweisen? Für Aufsehen hat in diesem Zusammenhang ein Schlichtungsspruch des Ombudsmanns des Bundesverbandes

der Volks- und Raiffeisenbanken gesorgt. Auch dieser Fall war typisch: Das Geld des Kunden war mithilfe eines Trojaners auf ein Drittkonto transferiert und von dessen Inhaber ins Ausland weitergeleitet worden. Obwohl der Trojaner und die Fälschung des Überweisungsauftrages feststanden, entschied der Ombudsmann zu Ungunsten des Kunden: Der Anscheinsbeweis spreche dafür, dass er entweder selbst die Überweisung angewiesen habe oder mit PIN und TAN nicht sorgfältig umgegangen sei. - Diese Aussage dürfte jedoch nicht verallgemeinerungsfähig sein. Letztlich werden sich die Entscheidungen solcher Fälle auf die einfachen Regeln reduzieren: Jede Partei muss die für Sie günstigen Tatsachen beweisen. Wer dann warum sorgfaltswidrig gehandelt hat, wird vom Einzelfall abhängen. Die ersten Gerichtsurteile bleiben jedenfalls mit Spannung abzuwarten.

Portrait

Unsere Kanzlei mit Sitz am Kurfürstendamm 42, 10719 Berlin, ist wirtschaftsrechtlich orientiert und hauptsächlich im Bank- und Kapitalanlagenrecht sowie auf dem Gebiet des Verbraucherschutz tätig.

News-ID: 109721 • Views: 145 (Stand: 05.08.2026)

Link zur Pressemitteilung:

<https://www.openpr.de/news/109721/Phishing-Wer-haftet-wann-wofuer.html>