Keine Möglichkeit der vollständigen Verhinderung von Attacken mittels Malware, Pharming und DNS-Spoofing durch Verwendung von Virenschutzsoftware, aber Reduzierung dieser Attacken

Gericht

LG Mannheim

Datum

16.05.2008

Aktenzeichen

1 S 189/07

Branche/ Lebenslage

Online-Banking, Schadprogramme, PIN, TAN, Malware, Virenschutzsoftware

Akteure

Bankkonto-Inhaber, Bank

Wer haftet?

Bank

Haftungsart

Schadensersatz

Haftungsumfang

Schadensersatz inkl. Zinsen, Verfahrenskosten

Haftungsbegründendes Verhalten

Tätigung eines nicht durch den tatsächlichen Kontoinhaber veranlassten Zahlungsauftrag

Technische Umstände

Malware Attacke ermöglichte Klau von Zugangsdaten, trotz installiertem Virenschutzprogramm

Persönliche Umstände

Grundsätzlich trägt die Bank das Missbrauchsrisiko, wenn nicht dem Geschädigten ein nachweisbarer Vorwurf zu machen ist; etwa aufgrund unzureichende zumutbarer eigener Schutzmaßnahmen

Möglichkeiten der Haftungsvermeidung

Kunden ist zu raten, zumindest gängige und aktuelle Virenschutzprogramme zu verwenden. Dass diese nicht sämtliche Attacken verhindern, wird dem Kunden von den Gerichten, wie auch hier, nicht zum Vorwurf gemacht

Zitate, Zusammenfassende Würdigung, Strategien zur Haftungsvermeidung

Die Klägerin und Bankkundin nahm ihre Bank in Anspruch eine getätigte Überweisung rückgängig zu machen, welche nicht durch die Kundin selbst, sondern unbefugt durch Dritte initiiert worden war. Wodurch die Dritten an die Zugangsdaten der Bankkundin gelangt waren, ließ sich nachträglich nicht mehr klären.

Das Gericht erkannte einen Anspruch gegen die Bank voll an. Insbesondere lehnte das Gericht einen Anscheinsbeweis zulasten der Klägerin ab, dass aufgrund der korrekten Eingabe von PIN und TAN von einer befugten Überweisung auszugehen sei. Dies wurde mit den umfangreichen Möglichkeiten im Online-Banking begründet, ohne Wissen und Wollen der Bankkunden an deren Zugangsdaten zu gelangen:

> *Die dargestellten Möglichkeiten für Dritte, beim Online-Banking unberechtigt die Legitimationsdaten eines Bankkunden zu Missbrauchszwecken zu erlangen, unter denen sich auch solche befinden, auf die der Bankkunde keinen Einfluss hat und die er nicht ohne weiteres verhindern kann, stehen der Annahme eines Anscheinsbeweises dafür entgegen, dass eine unter Benutzung von TAN und PIN erfolgte unberechtigte Verfügung auf einer Pflichtverletzung des Bankkunden beruht.*

Anders als z.B. beim klassischen Phishing kann der Kunde bei der Benutzung von Malware, Pharming und DNS Spoofing zunächst überhaupt nicht bemerken, dass PIN und TAN von unbefugter Seite erlangt wurden. Auch können derartige Angriffe zwar grundsätzlich durch die regelmäßige Verwendung von Virenschutzprogrammen und der Installation einer Firewall reduziert werden; gänzlich zu verhindern sind sie hierdurch jedoch nicht.

ANMERKUNGEN

Kein Anscheinsbeweis: Die korrekte Eingabe von PIN und TAN im Online-Banking-Verfahren führt nach Ansicht des Gerichts nicht zu einem Anscheinsbeweis, dass der Zahlungsauftrag auf den Kontoinhaber zurückzuführen ist. Ob ein Anscheinsbeweis auch für aktuellere insbesondere sicherere Systeme bei korrekter Eingabe der PIN und TAN ausgeschlossen sein soll ist hieraus nicht zu entnehmen.

Zur Hinweispflicht: Das Gericht ließ die Entscheidung dahinstehen, ob der Kunde bei der Feststellung, dass ein genutzter TAN nicht funktioniert, die Pflicht trägt, diesen TAN zumindest sperren zu lassen. Für den Fall, dass dies für die Entscheidung des Gerichts als entscheidungserheblich eingestuft worden wäre, hätte sich dieses wohl am OLG Karlsruhe orientiert. In der Entscheidung vom 22.01.2008, Az.: 17 U 185/07 lehnte das OLG Karlsruhe bei einem ähnlich gelagerten Fall eine Pflicht ab, dass eine nicht funktionierende TAN gesondert zu sperren sei.

Praxisrelevanz: Es handelte sich hier um eine TAN-Liste in nicht elektronischem Format, bei derer der Bankkunde bereits verwendete TAN üblicherweise durchstreicht. Selbst bei der Annahme, dass das Nicht-Sperren einer TAN eine Pflichtverletzung darstellt, so ließe sich dies nicht ohne Zweifel auf die moderneren TAN-Verfahren übertragen. Bei diesen wird regelmäßig schon keine TAN-Liste vorliegen, sondern nur einzelne TAN angezeigt werden. Im Übrigen wird die Nutzung der TAN-Listen immer weiter durch die moderneren und sicheren TAN-Systeme wie z.B. chip-TAN oder iTAN ersetzt. Sowohl hinsichtlich einer Verpflichtung TAN zu sperren als auch bzgl. des Anscheinsbeweises lassen sich der vorliegenden Entscheidung für die moderneren TAN-Verfahren keine Vermutungen entnehmen.