

Kontoinhaber haften bei Phishing

Gericht: Homebanking erfordert einen Virenschutz

jj. FRANKFURT, 24. Januar. Kontoinhaber, die zu Hause oder im Büro Online-Banking betreiben, müssen selbst für einen ausreichenden Schutz vor Computerbetrügern sorgen. Sonst müssen sie den finanziellen Schaden tragen, der ihnen durch den Diebstahl ihrer Zugangsdaten für elektronische Überweisungen entsteht. Das ergibt sich aus einem Urteil des Landgerichts Köln, das jetzt in der Internetzeitschrift JurPC veröffentlicht worden ist.

Diese Straftaten sind mittlerweile unter dem Namen „Phishing“ (Passwortfischen) bekannt. Das Bundeskriminalamt und das Bundesamt für Sicherheit in der Informationstechnik warnen regelmäßig vor solchen Machenschaften. Meist werden dabei massenhaft Spam-Mails mit der Aufforderung zur Eingabe von Passwörtern verschickt, die vorgeblich von der Hausbank des Kontoinhabers stammen, oder von Straftätern Websites von Geldinstituten vorgetäuscht. Oft werden die erbeuteten Beträge weiter ins Ausland verschoben; der Kontobesitzer kann sich dann sogar wegen Geldwäsche strafbar machen.

Bei dem Rechtsstreit ging es um einen Bankkunden, dessen Kontodaten nebst persönlicher Identifikationsnummer (PIN) sowie der erforderlichen Transaktionsnummer (TAN) von unbekanntem Täter ausspioniert worden waren. Ob dies beispielsweise durch einen Computervirus zustande kam, ließ sich vor Gericht nicht mehr aufklären. Jedenfalls hatten Kriminelle von seinem Konto ebenso wie von den Konten zweier anderer Kunden Geld abgebucht und nach Osteuropa überwiesen. Er bleibt nun auf dem Schaden sitzen und bekommt ihn nicht von seinem Geldinstitut erstattet.

Die Kölner Richter wiesen ihm ein erhebliches Mitverschulden für diese „Phishing-Attacken“ zu (Az.: 9 S 195/07). Dabei stellten sie für die Inhaber von privaten Konten den Maßstab

eines „verständigen, technisch durchschnittlich begabten Anwenders“ auf. Von diesem könne beim Online-Banking gefordert werden, dass er eine aktuelle Virenschutzsoftware verwende. Außerdem müsse er eine Firewall benutzen – also einen Schutzschild gegen Zugriffe von Hackern auf den eigenen Computer.

Doch bei diesen Anforderungen beließen es die Zivilrichter nicht. Ihrem Urteil zufolge müssen Anwender außerdem regelmäßig Sicherheits-Updates für ihr Betriebssystem sowie für die verwendeten Programme (Software) installieren. Darüber hinaus müsse ein Kontoinhaber die Warnungen der Banken beachten, PIN und TAN niemals auf telefonische Anforderung oder auf Anforderung per E-Mail herauszugeben. Das Landgericht hält es sogar für erforderlich, dass der Kunde „deutliche Hinweise auf gefälschte E-Mails und Internetseiten seiner Bank“ erkennt. Als Beispiele dafür nennen die Robenträger sprachliche Mängel, eine „deutlich falsche Internet-Adresse“, ferner Web-Adressen ohne den Vorsatz `https://` sowie das Fehlen des Schlüsselsymbols in der Statusleiste, das eine geschützte Internet-Verbindung signalisiert.

Noch weitergehende Sicherheitsmaßnahmen hält das Landgericht aber nicht für Pflicht. Nicht vorgeschrieben ist demnach ausdrücklich die „Verwendung bestimmter, besonders leistungsfähiger Virenschutzprogramme“ oder spezialisierter Programme zum Schutz gegen bestimmte Schadsoftware. Auch müsse ein Verbraucher nicht die Standard-Sicherheitseinstellungen seines Betriebssystems und seiner Programme verändern; ebenso wenig müsse er ohne Administratorrechte arbeiten. Die Zertifikate der Web-Anbieter muss er gleichfalls nicht überprüfen. „Auch das Erkennen subtiler Abweichungen in der Internetadresse würde die Sorgfaltsanforderungen überspannen“, stellt das Kölner Landgericht fest.