



Internet-Banking: „Die Transaktion muss abgesichert werden, nicht nur das Einloggen.“

Gefährliche Sicherheitslücken

Neue Kriminalitätsformen im weltweiten Datennetz bedrohen das Internet-Banking.
Die Dunkelziffer ist sehr hoch.

Die Internet-Kriminalität sorgt in den obersten Etagen von Finanzinstituten und verwandten Branchen für Kopfzerbrechen: Der britischen *HSBC* sind 180.000 Kundendatensätze abhanden gekommen; der *Bank auf America* wurden Bänder mit Daten von 1,2 Millionen Regierungsmitarbeitern gestohlen, darunter 900.000 Beschäftigte des Verteidigungsministeriums; von *CardSystems Solutions* wurden 40 Millionen Kreditkartendaten von Mastercard- und *VISA*-Kunden widerrechtlich kopiert. Der *IBM-Global Business Security Index* registrierte im ersten Halbjahr 2005 weltweit mehr als 237 Millionen Attacken.

Auch Österreichs Banken und Versicherungen bleiben

von der ausufernden Internet-Kriminalität nicht verschont, obgleich laut Ernst Österreicher vom Bundeskriminalamt wenig Anzeigen registriert werden. „Die Dunkelziffer ist sehr hoch“, betonte Chefinspektor Österreicher beim „Sicherheit 2005-Symposium“, veranstaltet vom Sicherheitskompetenz-Zentrum der *S-Gruppe* in Wien. „Wenig Anzeigen bedeuten wenig Beamte und wenig Geld. Wir drehen uns auch mit den teilweise widersprüchlichen Gesetzen im Kreis.“ Das sind in erster Linie Strafgesetzbuch, Sicherheitspolizei-, Datenschutz-, Telekommunikationsgesetz und Strafprozessordnung.

Phishing. Als drastisches Beispiel führte Ernst Öster-

reicher die rechtliche Situation beim Phishing an: Sammelt der Phisher nur Zugangsdaten, dann sei das nach der Rechtslage grundsätzlich nicht strafbar: „Der Diebstahl von Daten allein ist noch kein Diebstahl im strafrechtlichen Sinn.“ Strafe drohe erst, wenn „der Phisher eine Überweisung vorzunehmen versucht, wenn beispielsweise Passwörter oder TANs abgesendet werden.“ Und selbst dann drohen nicht mehr als sechs Monate Freiheitsstrafe.

IT-Experte Österreicher warnte vor den Bot-Nets, deren Angriffe in den vergangenen sechs Monaten stark zugenommen hätten – laut Statistik des Innenministeriums von 119 auf 927 Fälle. Die heimischen Banken würden

seiner Meinung „einen Beschluss von Bot-Nets auf ihre Internet Banking-Lösungen nicht aushalten“.

Keine Garantie für Vertraulichkeit. Philipp Schumann, Sicherheitsberater der *Bull AG* in Wien, wies darauf hin, dass SSL-Verschlüsselung, wie sie momentan implementiert ist, nicht vor MITM-Attacken schützen: „Es gibt eine ganze Reihe von Techniken dafür.“ Das Grundproblem bestehe darin, dass die Vertraulichkeit von Passwörtern und Accounts nie garantiert werden könne. Der Hebel sei vielmehr bei der Überweisung anzusetzen: „Die Transaktion selbst ist der Schritt, der abgesichert werden muss, und nicht nur das Einloggen“, sagte Schau-



Phishing: „Nicht leicht, eine Internetseite als Fälschung zu erkennen.“

mann. Als Beweis dafür nannte er Kreditkarten: „Die funktionieren praktisch ohne Authentisierung, trotzdem ist der Kreditkartenbetrug im erträglichen Umfang.“

Schaumann zufolge liegt der Schlüssel für technische Lösungen zur Absicherung von Finanztransaktionen bei den Banken. „Denn der Kunde hat es nicht leicht, eine Internetseite als Fälschung zu erkennen.“ MITM-Attacken („Man-in-the-Middle“) seien stark im Kommen. MITM umfasst Angriffsarten, bei dem sich ein Hacker in die Transaktion einloggt, obwohl die Authentifizierung okay war, und beispielsweise Überweisungsdaten verändert. Ebenso möglich ist das Mitlesen und Wiederverwenden von Passwörtern, das Einfügen von Links zu Trojanern in Webseiten oder das Fortsetzen von Sessions nach dem abgefangenen Logout des Anwenders.

MITM-Angriffe erkennt man etwa daran, dass viele Kunden von einer einzigen IP-Adresse kommen bzw. Überweisungen von vielen Kunden an einen einzigen Empfänger geleitet werden. Auch dagegen könne man sich wappnen. Schaumann nannte die verzögerte Durchführung von Überweisungen bei Auffälligkeiten nach vom Kunden zu wählenden Kriterien, zwingende E-Mail-Infos für alle bzw. bestimmte Überweisungen oder das Login über die digitale Signatur. Auch das zweistufige SMS-TAN-Verfahren, das die Erste Bank seit Mai 2005 im Rahmen ihrer Netbanking-Lösung einsetzt, erachtet Schaumann als taugliche Maßnahme.

Internet-Banking. Warum Geldinstitute generell das Internet-Banking favorisieren, liegt an den Kosten: Elektronische Überweisungen kosten die Institute rund zehn Prozent im Vergleich zu manuellen Transaktionen am Schalter – 16 Cent gegenüber 1,5 Euro. Nicht alle Institute geben diese Kostenvorteile an die Kunden weiter, ergab eine Erhebung der AK im September 2005.

„Wir haben 15 Institute getestet. Aber nur neun verrechnen ihren Kunden weniger“, berichtete Harald Glatz, Leiter der Abteilung Konsumentenschutz der AK Wien. Kunden würden das PIN/TAN-Verfahren als zu mühsam finden: „Deswegen mache auch ich es nicht mehr“, sagte Glatz. Auch die Haftung weise „eindeutig eine Schiefelage zu Ungunsten des Kunden auf“. Dagegen seien die Pflichten der Banken „stark herunter gefahren“. Bei Anfragen an die AK würde das Internet-Banking eine untergeordnete Rolle spielen – „90 Prozent betreffen Auktionshäuser, insbesondere Ebay“, betonte der AK-Experte.

Haftung durch die Bank.

Anders beurteilt Harald Krasnigg, Jurist beim Grazer *Evolaris Research Lab*, die Haftungssituation der Finanzinstitute beim Internet Banking: „Bei Schäden, die durch leichte Fahrlässigkeit der Bank entstehen, dürfen diese nach einem Erkenntnis des Obersten Gerichtshofs nicht mehr auf die Bankkunden überwältzt werden“ (OGH-Urteil vom 19. November 2002). Ebenso tragen Banken infolge des OGH-Entscheidens das Haftungsrisiko für Fehlüberweisungen im Internet-Banking, die durch einen mangelnden Abgleich von Kontonummer und Kontowortlaut zustande kommen, „sofern sie kein Kontrollsystem in den automatisierten Ablauf implementieren, die einen Abgleich vornimmt“, erklärte Krasnigg.

Frederick Staufer