Dirk Fox

Online Banking

Hintergrund

Unter Online Banking (auch „Home Banking“ oder „Internet Banking“ genannt) versteht man die Initiierung von Geld-Transaktionen auf einem Bankkonto (wie Überweisungen oder Daueraufträge) über einen Web-Dienst der Bank. Diese Transaktionen werden entweder direkt (‚manuell') im Browser über eine Web-Schnittstelle veranlasst, oder aber über ein lokales Programm, mit dem bspw. ein Kassenbuch geführt und im Hintergrund die Web-Schnittstelle der Bank bedient wird.

Online Banking wurde in Deutschland erstmals im Jahr 1980 – drei Jahre nach den ersten Geldautomaten – über den BTX-Dienst der damaligen Deutschen Bundespost angeboten. Der Dienst wurde von der Deutschen Telekom bis 2007 als „T-Online Classic“ weitergeführt [1]. Inzwischen erledigen 45 % der Deutschen ihre Bankgeschäfte per Online Banking – allen Meldungen über erfolgreiche Betrugsfälle zum Trotz [2].

Sicherheit

Schon beim BTX-System gab es ein Login mit Nutzernamen und (10stelligem) Kennwort. Die Authentizität der Transaktionen wurde durch nur einmal verwendbare „Geldtransaktionsnummern“ sicher gestellt – dem Vorläufer des PIN/TAN-Verfahrens, das für das Internet Banking anfänglich von allen deutschen Banken übernommen wurde. Dadurch war Online Banking in Deutschland von Anfang an erheblich sicherer als bspw. Verfahren einiger amerikanischer oder britischer Banken, die sich – z. T. bis in die jüngste Zeit – auf die initiale Authentisierung mit einer PIN beschränkten und deren Kunden daher für die ersten Trojaner und Phisher leichte Beute waren.

Der Nachteil des PIN/TAN-Verfahrens, das noch heute viele Banken einsetzen, ist, dass die Transaktionsnummer (TAN) von den Daten der Transaktion unabhängig ist. TANs, die dem Kontoinhaber entwendet wurden (z. B. durch Abfangen der Post oder eine Online-Abfrage einzelner TANs durch Phisher oder Trojaner), können daher für beliebige missbräuchliche Transaktionen genutzt werden.

Auf diesen Nachteil reagierte man zunächst durch die Verwendung „indizierter TANs“ (iTAN): Je Transaktion wird dabei genau eine (nummerierte) TAN der TAN-Liste frei geschaltet und der Index dieser einzugebenden TAN an den Kunden übermittelt. Dadurch wird das Risiko eines erfolgreichen PIN/TAN-Angriffs immerhin verringert; vor dem Kopieren eines kompletten TAN-Briefs schützt das Vorgehen jedoch nicht. Schutz gegen diese Angriffe bieten nur TANs, die erst bei Bedarf erzeugt werden und im Idealfall auch noch von den Daten der Transaktion abhängen. Dies gelingt technisch durch die Verwendung von dezentralen und zentralen TAN-Generatoren, die befristet gültige TANs unmittelbar vor der Nutzung erzeugen. Zentrale TAN-Generatoren verwendet beispielsweise das mTAN- oder Mobile TAN-Verfahren, das viele deutsche Banken heute anbieten: Abhängig von den im Online Banking angegebenen Transaktionsdaten (Ziel-Konto, Betrag) und dem Kundenkonto erzeugt die Bank eine TAN mit beschränkter zeitlicher Gültigkeit und schickt diese per SMS an den Kunden. Dabei muss die Bank die Mobilfunknummer des Kunden kennen und sicherstellen, dass diese nur autorisiert geändert werden darf.[1]

Dezentrale TAN-Generatoren sind hingegen eigenständige, Batterie betriebene Geräte im Besitz des Kunden, die auf Knopfdruck eine, nur kurzfristig gültige TAN erzeugen. Einige TAN-Generatoren verwenden dabei neben, einem individuellen geheimen Schlüssel des Kunden oder der EC-Karte die aktuellen Transaktionsdaten, die entweder manuell eingegeben oder über einen am Bildschirm angezeigten 2D- oder 3D-Barcode vom Generator ‚gelesen' werden können. Bankseitig wird auf demselben Weg eine TAN berechnet und mit dem vom Kunden eingegebenen Wert verglichen. TAN-Generatoren realisieren damit eine Zwei-Faktor-Authentisierung: ein Angreifer muss in den Besitz des Generators kommen, um Transaktionen fälschen zu können.

Ein anderer Weg wurde in Deutschland mit dem *Home Banking Computer Interface* (HBCI) eingeschlagen. Es wurde unter Mitwirkung zahlreicher Banken entwickelt und vom Zentralen Kreditausschuss (ZKA) 1996 veröffentlicht. HBCI (2002 in FinTS – *Financial Transaction Service* – umbenannt) ist eine offene Schnittstelle, die Banken unabhängig mehrere Authentifizierungsverfahren unterstützt und sichere Protokolle für die Abwicklung unterschiedlicher Transaktionen spezifiziert [3].

Das höchste Sicherheitsniveau erreicht man mit FinTS mit Chipkarte und einem Chipkartenleser nach Secoder-Standard: Die Autorisierung der Transaktion erfolgt durch kryptographische Verfahren auf der Chipkarte (elektronische Signaturen), die PIN zur Kartenaktivierung wird auf einem PIN-Pad des Lesegeräts eingegeben, und in einem Display des Secoders werden die zu autorisierenden Transaktionsdaten angezeigt.

Referenzen

[1] Heise Online: *Vor 30 Jahren: Online-Banking startet in Deutschland*. 12.11.2010 (https://heise.de/-1135331)
[2] Wikipedia: Electronic Banking. (https://de.wikipedia.org/wiki/Electronic_Banking)
[3] Sparkassen Informatik Zentrum (SIZ): *FinTS*. (http://www.hbci-zka.de/)
[4] Zwissler, Sonja: *HBCI*. Gateway, DuD 1/1999, S. 45.

1 Was nicht einfach ist: So gelang es kürzlich einem Angreifer, beim Mobilfunkprovider seines Opfers telefonisch ein „Auto Forwarding“ für alle eingehenden SMS auf eine angeblich neue Nummer zu veranlassen.