Bankgeschäfte per Klick erledigen

Wie sicher ist Online-Banking?

Online-Banking ermöglicht Privatpersonen und Unternehmen die Abwicklung von alltäglichen Bankgeschäften ohne Medienbruch und über die normalen Öffnungszeiten der Banken hinaus. Die Anzahl an Privatnutzern des Online-Bankings steigt stetig an. Allein 2015 erledigten, laut einer Bitkom-Studie, bereits 40 Millionen Deutsche ihre Bankgeschäfte online [1]. Cyberkriminelle haben hier längst einen interessanten „Geschäftszweig" entdeckt und Verfahren entwickelt, die gängigen Systeme zur Transaktionssicherung auszuhebeln. Wie haben uns diese Sicherungssysteme auf ihre Zuverlässigkeit und Nutzbarkeit hin angesehen. Darüber hinaus geben wir einen Ausblick, was in dieser Angelegenheit künftig noch auf uns zukommen könnte.

Durch kriminelle Aktivitäten wie etwa den nicht autorisierten Zugriff auf Bankkonten oder die schadhafte Manipulation von Online-Überweisungen entstehen den Banken und Endbenutzern immense Schäden. 2014 wurde bei dem Bundeskriminalamt (BKA) ein Schaden von 27,9 Millionen Euro gemeldet (bei 6.984 Fällen - ca. 3.995 Euro Schaden pro Fall) [2]. Die Dunkelziffer, das heißt von den Banken nicht gemeldete Schadensfälle, um die Reputation der Banken nicht zu schädigen, liegt vermutlich deutlich über den offiziellen Angaben des BKA. Abbildung 1 zeigt die Entwicklung der Schadenszahlen im Online-Banking im Zeitraum von 2008 bis 2014. Die Schadenshöhe pro Fall ist auf ca. 4.000 Euro beschränkt, weil die meisten Bankkunden im Online-Banking dies statistisch als maximalen Überweisungsbetrag pro Überweisung zulassen. Betrüger können das gestohlene Geld nicht direkt auf ihr eigenes Konto überweisen, da sie sonst sehr einfach von den Strafverfolgern identifiziert werden können. Daher werden Finanzagenten eingesetzt, die im Namen des Angreifers ein Konto eröffnen. Sobald der Angreifer Geld, durch die Manipulation von Transaktionen, auf dieses Konto überwiesen hat, kontaktiert er den Finanzagenten und lässt sich das Geld von dem Agenten auszahlen. Die Anzahl der Finanzagenten ist, unter anderem aufgrund des hohen Risikos, das die Finanzagenten eingehen, begrenzt. Dies führt zurzeit ebenfalls zu einer Begrenzung der Schadensfälle.

Durch den Missbrauch des Online-Bankings entwickelt sich die Finanzkriminalität derzeit zu einer ernsten Gefahr für die Informationsgesellschaft. Gleichzeitig ist unsere Gesellschaft mit einer Vielzahl neuer Medien konfrontiert, die bei unzureichenden Sicherheitsmechanismen den Schaden noch weiter erhöhen können. Betrüger zielen zum Beispiel vermehrt darauf ab, Online-Banking auf den in der Bevölkerung weit verbreiteten Smartphones zu missbrauchen. Ferner können vermeintlich sichere Transaktionssysteme (zum Beispiel mobileTAN) bereits von Angreifern umgangen werden.

Es ist abzusehen, dass, so lange die aktuelle Generation der etablierten Transaktionssicherungsverfahren eingesetzt wird, die Angriffszahlen weiter ansteigen, da sich die Kriminellen immer weiter auf diese Verfahren einstellen. Banken müssen dabei, um den Anforderungen der Kunden und der Gesellschaft gerecht zu werden, einen Spagat

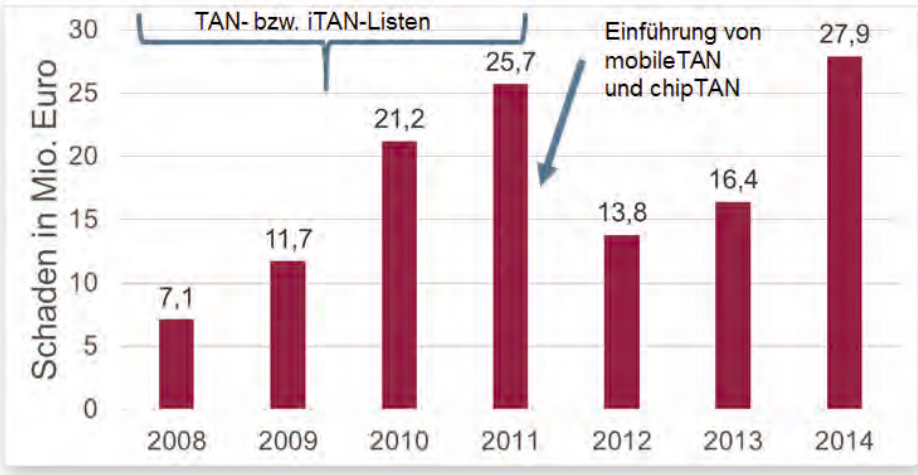

Abbildung 1: Finanzieller Schaden im Online-Banking 2008 bis 2014 [2], Quelle: ifis

zwischen Sicherheit und Nutzbarkeit der Transaktionssicherungsverfahren vollziehen. Letztendlich bleibt den Banken im Hinblick auf Kundenbindung und Aufrechterhaltung des Sicherheitsniveaus nur die Möglichkeit, in periodischen Abständen neue Verfahren zur Transaktionssicherung anzubieten, die aktuellen Sicherheitsrisiken begegnen und den Nutzungsansprüchen der Kunden genügen.

Eine schlechte Alternative wäre, wenn die 40 Millionen Online-Banking-Kunden wieder in die Filialen gingen, um ihre Banktransaktionen zu erledigen. Dies würde sicherlich deutlich mehr Geld kosten, als einen höheren IT-Sicherheitsstandard einzuführen.

Sicherheitskonzepte im Online-Banking

Im Folgenden werden die gängigen Sicherheitskonzepte dargestellt und bewertet.

1. Das chipTAN-Verfahren

Dieses Verfahren nutzt einen TAN-Generator (TAN = Transaktionsnummer) mit Chipkartenleser und optischem Sensor, um die Transaktionsdaten vom Bildschirm über einen optischen Code auf diesen zu übertragen (schwarz flackernder Bereich, sogenannter Flickercode). Der TAN-Generator (Flickercode-Leser) ähnelt dabei einem Taschenrechner mit einem kleinen Display. Bei der Anschaffung des TAN-Generators entstehen möglicherweise Kosten für den Bankkunden, je nach Bankinstitut. Die Transaktionsdurchführung mit Hilfe des chipTAN-Verfahrens beginnt mit der Authentifizierung des Bankkunden gegenüber der Online-Banking-Webseite (1) mittels Nutzername und Passwort und der Übermittlung der Transaktionsdaten an die Webseite des Bankinstituts (2). An diesem Punkt kann der Angreifer die Daten, bevor sie an den sicheren Kanal übergeben werden, manipulieren. Im Folgenden stellt das Bankinstitut auf der Webseite einen optischen Code zur Verfügung, den der Bankkunde über die optische Schnittstelle des TAN-Generators einlesen kann (3). Der optische Code enthält dabei die vom Bankinstitut empfangenen Transaktionsdaten. Zusätzlich zu dem Flickercode werden ebenfalls die Transaktionsdaten auf der Webseite der Bank dargestellt.

Diese Daten können allerdings vom Angreifer mit Hilfe von Banking-Trojaner verändert werden, sodass diese zu der Transaktion passen, die der Bankkunde eigentlich ausführen wollte. Falls im Verlauf eine Manipulation dieser Daten stattgefunden hätte, hat der Bankkunde nun über die sichere Anzeige des TAN-Generators die Möglichkeit, die Bankdaten noch einmal zu verifizieren. Problematisch bei der Verifizierung ist allerdings das kleine Display des Geräts, was zur Folge hat, dass Bankkunden oft unaufmerksam sind und die Daten nicht genau prüfen. Nach erfolgreicher Verifizierung der Transaktionsdaten erzeugt der Bankkunde, mit Hilfe des TAN-Generators und der Bankkarte (typischerweise die EC-Karte), eine TAN für diese Transaktion, mit welcher er diese autorisieren kann (4). Über ein Security-Modul auf Seiten des Bankinstituts hat dieses die Möglichkeit, mit den empfangenen Transaktionsdaten dieselbe TAN zu erzeugen und im letzten Schritt mit der vom Bankkunden generierten TAN zu vergleichen. Stimmen die TANs der Bank und des Bankkunden überein, wird die Transaktion durchgeführt. Der prinzipielle Ablauf des Verfahrens wird in Abbildung 2 dargestellt.

2. Das mobileTAN-Verfahren

Das mobileTAN-Verfahren (auch mTAN oder smsTAN) nutzt das Mobiltelefon des Bankkunden, um eine Transaktion zu autorisieren. Die Sicherheit des Verfahrens liegt darin, dass ein Angreifer die Kontrolle über das Mobiltelefon und das Endgerät des Bankkunden erlangen muss, um Transaktionen erfolgreich manipulieren beziehungsweise eigenständig ausführen zu können. Das mobileTAN-Verfahren benötigt dabei als einziges hier vorgestelltes Verfahren kein zusätzliches Gerät, sondern nur ein in der Regel bereits im Besitz des Bankkunden befindliches Mobiltelefon (oder Ähnliches, zum Beispiel ein Tablet). Kosten entstehen für den Bankkunden, je nach Bankinstitut, für den Versand der SMS bei jeder Transaktion. Nach erfolgreicher Authentifizierung des Bankkunden gegenüber der Bank-Webseite (1) übermittelt dieser die Transaktionsdaten über ein Formular auf der Web-seite an die Bank (2). Wie beim chipTAN-Verfahren hat der Angreifer hier die Möglichkeit, die Daten zu manipulieren, bevor diese an die Bank übermittelt werden. Dem Bankkunden werden die Transaktionsdaten, welche die Bank erhalten hat, nochmals zur Kontrolle angezeigt.

Die Kontrolldaten können ebenfalls vom Angreifer manipuliert werden, sodass der Bankkunde die Manipulation an dieser Stelle nicht bemerken kann. Darauf folgend wird mit einem Security-Modul des Bankinstituts eine TAN für die durchzuführende Transaktion gebildet. Die TAN bezieht sich dabei direkt auf die Transaktion und kann nur für diese genutzt werden. Die TAN wird per SMS an das Mobiltelefon des Bankkunden gesendet (3). Über die Anzeige des mobilen Geräts kann der Bankkunde die Transaktionsdaten nochmals verifizieren. Dieser Schritt ist dabei sicherheitskritischer als beim chipTAN-Verfahren, da die Anzeige des mobilen Geräts deutlich anfälliger gegen Manipulationen eines Angreifers ist. Ein weiteres Problem ist, dass die SMS vom Angreifer gestohlen werden kann und er so selbst in der Lage ist, Transaktionen auszuführen (siehe Abschnitt „Angriff auf das mobileTAN-Verfahren"). Im letzten Schritt übermittelt der Bankkunde die empfangene TAN über ein Formular auf der Online-Banking-Webseite an das Bankinstitut (4). Wenn die vom Bankkunden übermittelte TAN mit der vom Bankinstitut erzeugten übereinstimmt, wird die Transaktion durch-

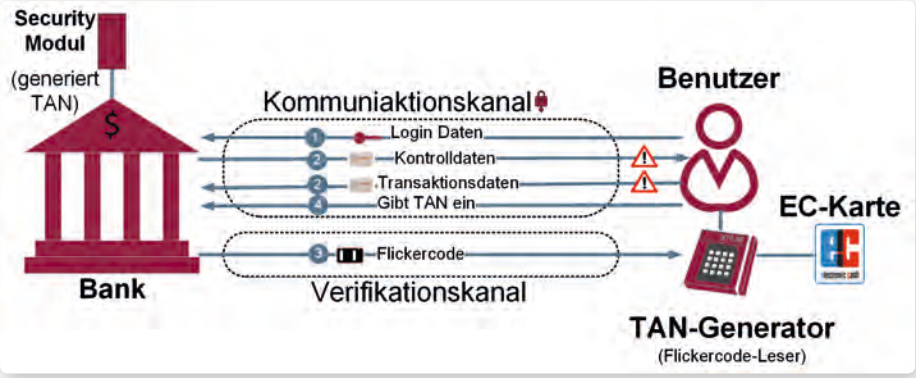

Abbildung 2: Darstellung der logischen Kanäle im Online-Banking mittels chipTAN, Quelle: ifis

geführt, ansonsten verworfen. Der schematische Ablauf des mobileTAN-Verfahren swird in Abbildung 3 deutlich.

3. Das HBCI-Secoder-Verfahren

Das HBCI-Verfahren, nach dem Secoder-Standard, nutzt anstelle einer TAN eine digitale Signatur zur Sicherung der Transaktionsdaten. Dazu werden auf der Kundenseite eine Signaturkarte sowie ein secoderfähiges Kartenlesegerät mit PIN-Pad benötigt. Das Chipkartenlesegerät ist dabei deutlich teurer (ca. 70 Euro) als die günstigen TAN-Generatoren des chipTAN-Verfahrens. Zusätzlich entstehen für den Bankkunden möglicherweise Kosten für die Anschaffung einer speziellen Signaturkarte, da die normale EC-Karte in diesem Fall nicht verwendet wird.

Anders als bei den zweistufigen Challenge-Response-Verfahren chipTAN und mobileTAN, handelt es sich bei dem HBCI-Secoder-Verfahren um ein sogenanntes Ein-Schritt-Verfahren. Das bedeutet, dass alle benötigten Daten sowie Sicherheitsinformationen in einem Schritt an das Bankinstitut gesendet werden. Zunächst authentisiert sich der Bankkunde gegenüber der Bank. Dabei ist es in diesem Schritt schon möglich, das secoderfähige Chipkartenlesegerät und die Signaturkarte, statt eines Passworts, für die Authentifizierung zu nutzen (1). Im nächsten Schritt gibt der Bankkunde die Transaktionsdaten in das Formular der Online-Banking-Webseite ein und übermittelt diese an das Chipkartenlesegerät. Wie bei den bereits vorgestellten Verfahren hat der Angreifer hier die Möglichkeit, die Transaktionsdaten zu manipulieren. Wie auch bei den beiden vorherigen Verfahren kann der Angreifer die Kontrolldaten, die im Browser angezeigt werden, manipulieren, ohne dass der Bankkunde dies bemerkt. Über das Display des Chipkartenlesegeräts kann der Bankkunde die Transaktionsdaten nochmals verifizieren. Wie auch beim chipTAN-Verfahren besteht die Problematik, dass die Bankkunden, aufgrund des kleinen Displays, unachtsam bei der Verifikation agieren. Nach der Verifikation und einer PIN-Abfrage, die der Bankkunde über das PIN-Pad des Chipkartenlesegeräts eingeben muss, werden die Transaktionsdaten dem Chip der Signaturkarte zugeführt, digital signiert und nachfolgend an das Bankinstitut übermittelt (2). Das Bankinstitut kann, anhand der digitalen Signatur, die Integrität der Transaktionsdaten prüfen und im Erfolgsfall die Transaktion durchführen. Der schematische Ablauf des HBCI-Secoder-Verfahrens wird in Abbildung 4 dargestellt.

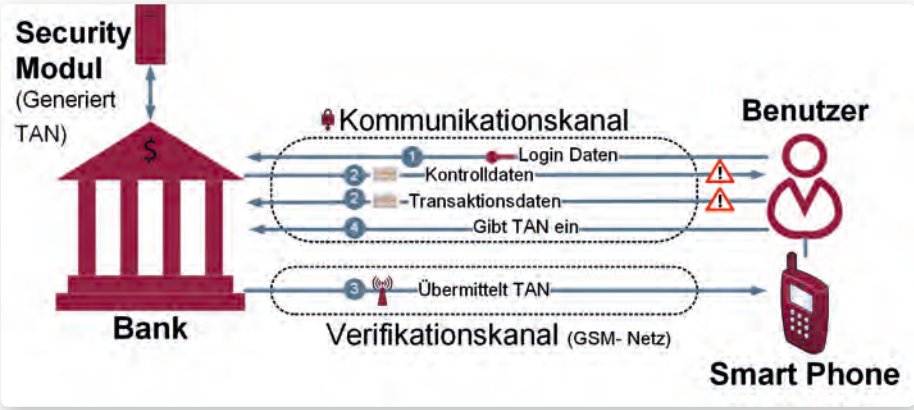

Abbildung 3: Darstellung der Kanäle im Online-Banking mittels mobileTAN, Quelle: ifis

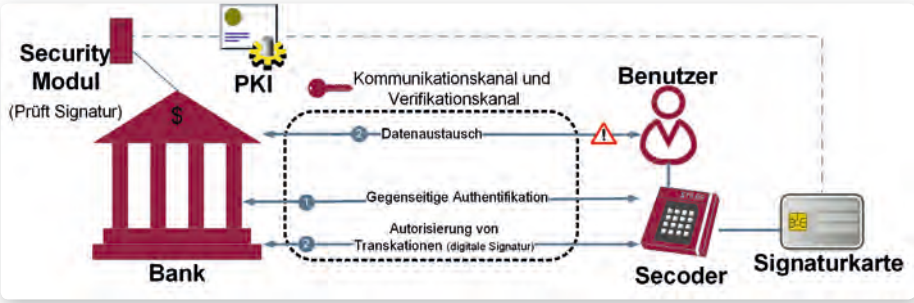

Abbildung 4: Darstellung der Kanäle im Online-Banking mittels HBCI Secoder, Quelle: ifis

Angriffsflächen im Online-Banking

Ein großes Problem, das aktuell im Online-Banking vorliegt, ist die Manipulation der Darstellung der Banken-Webseiten durch Banking-Trojaner auf dem Endgerät des Bankkunden. Die Banking-Trojaner haben durch Man-in-the-Browser-Angriffe die Möglichkeiten, clientseitig die lokale Darstellung der Bank-Webseiten zu manipulieren. Die gesicherte Verbindung (in der Regel ein TLS-gesicherter Kanal) zur Bank wird dadurch nicht beeinflusst, da die Manipulation nach beziehungsweise vor der Einspeisung in den Kanal zwischen Kunde und Bank, erfolgt. Der Bankkunde kann eine Manipulation der lokalen Darstellung aus diesem Grund nur sehr schwer erkennen. Eine Sicherheitsmaßnahme zur Erkennung dieser Angriffe, die in der Regel auf die Manipulation der Transaktionsdaten abzielen, bietet die Verifikation der Transaktionsdaten über eine sichere Anzeige auf Seiten des Bankkunden. Sichere Anzeigen werden sowohl durch das chipTAN- als auch durch das HBCI-Secoder-Verfahren in Form des Displays auf den obligatorischen Chipkartenlesegeräten umgesetzt.

Durch den Einsatz von Man-in-the-Browser-Angriffen kann ein Angreifer aber auch äußerst wirkungsvolle Social-Engineering-Angriffe durchführen, die durch die technischen Möglichkeiten der Transaktionssicherungsverfahren nicht erkannt werden können. Der Bankkunde, der sich auf der Webseite der Bank befindet, sieht sich dabei dahingehend getäuscht, dass er unberechtigterweise eine Überweisung erhalten hat (siehe Abbildung 5). Um die Illusion vollständig zu machen, wird der aktuelle Kontostand verändert und die Transaktion wird in die Transaktionshistorie aufgenommen. In diesem Fall überweist der Kunde dem Angreifer also „freiwillig" den dargestellten Betrag.

Qualitätsübersicht der betrachteten Verfahren

In Abbildung 6 werden die heutzutage gängigsten TAN-Verfahren und das signaturba-

sierte HBCI-Secoder-Verfahren abschließend miteinander verglichen.

Aus Sicht der IT-Sicherheit schneiden das HBCI-Secoder-Verfahren und das chipTAN-Verfahren, aufgrund der sicheren Anzeige der Transaktionsdaten auf dem Chipkartenlesegerät vor Transaktionsautorisierung, am besten ab. Allerdings ist bei beiden Verfahren ein Chipkartenlesegerät obligatorisch, was die Mobilität dieser Verfahren und damit deren Nutzbarkeit negativ beeinflusst. Beim HBCI-Secoder-Verfahren wird zusätzlich eine spezielle Signaturkarte zur Transaktionsdurchführung benötigt. Letztlich kann nur das mobileTAN-Verfahren effektiv mobil einsetzt werden, da der Bankkunde sein Mobiltelefon immer mit sich führt. Dieser Komfortgewinn für den Kunden wird durch eine größere Angriffsfläche für einen Angreifer erkauft.

Dies liegt daran, dass heutige mobile Geräte (Smartphones) anfällig für Mobile Malware sind, die beispielsweise die Anzeige auf dem mobilen Gerät manipuliert, um den Bankkunden zu täuschen. Durch die manipulierbare Anzeige entsteht auch die erhöhte Anfälligkeit gegenüben Man-in-the-Browser-Angriffen, die auf die Manipulation der Transaktionsdaten abzielen. Durch die Möglichkeit des chipTAN- und HBCI-Secoder-Verfahrens, die Transaktionsdaten vor Transaktionsdurchführung noch einmal auf einer sicheren Anzeige, das heißt dem Display des Chipkartenlesegeräts, verifizieren zu können, entsteht eine geringere Gefahr bezüglich Man-in-the-Browser-Angriffen. In diesem Fall hat der Angreifer zwar weiterhin die Möglichkeit, die Anzeige des Browsers des Opfers zu manipulieren, dieses ist dann aber im Nachhinein durch die Verifikation über das Display des Chipkartenlesegeräts erkennbar.

Im Gegensatz zu den früher häufig eingesetzten TAN-Listen, deren TANs nicht an die aktuelle Transaktion gebunden waren, bieten die aktuellen TAN-Verfahren, mobile- und chipTAN, einen sicheren Schutz gegen Phishing-Angriffe, da die TANs an eine spezielle Transaktion gebunden sind. Die entstehenden Kosten des mobileTANs und chipTAN-Verfahren sind ähnlich zu bewerten. So fallen beim chipTAN-Verfahren einmalige Anschaffungskosten von ca. zehn Euro (abhängig vom jeweiligen Bankinstitut) an und beim mobileTAN-Verfahren Kosten von ca. neun Cent pro SMS (ebenfalls abhängig von dem Bankinstitut). Das HBCI-Verfahren schließt, aufgrund der sehr hohen Anschaffungskosten (ca. 70 Euro für den Kartenleser und ca. 15 Euro für die Signaturkarte), deutlich schlechter bei den Kosten ab, als die beiden anderen Verfahren.

Angriff auf das mobileTAN-Verfahren

Es gibt unterschiedliche Varianten, das mobileTAN-Verfahren anzugreifen. Zum einen kann ein Angreifer versuchen, das Mobiltelefon und den Computer des Opfers zu infizieren, um so Transaktionen zu autorisieren, zum anderen eine zweite SIM-Karte für die Rufnummer des Opfers zu erstellen, damit die Bestätigungs-SMS auf dem eigenen Mobiltelefon empfangen werden kann. In Abbildung 7 wird

Sehr geehrter Kunde, am 22.02.2016 wurde auf Ihr Konto 123456 eine Summe in einer Höhe von 50,00 EUR gutgeschrieben. Laut unseren Informationen wurde das Geld versehentlich auf Ihr Konto überwiesen, daher ist Ihr Konto vorübergehend gesperrt. Wir empfehlen Ihnen die Summe an den Absender zurück zu überweisen. Ihr Konto wird dann automatisch wieder freigeschaltet. Bitte drücken Sie auf **"ERSTATTEN"** um das Geld zurück zu überweisen. Bitte entschuldigen Sie die Unannehmlichkeiten.

Abbildung 5: Beispiel einer Manipulation auf einer Bank-Webseite, Quelle: ifis

	mobileTAN	chipTAN	HBCI-Secoder
Sicherheitsaspekte	+	+ +	+ + +
Nutzbarkeit	+ + +	+ +	+
Kosten	−	−	− − −

Abbildung 6: Qualitätsübersicht der dargestellten Sicherheitsverfahren im Online-Banking, Quelle: ifis

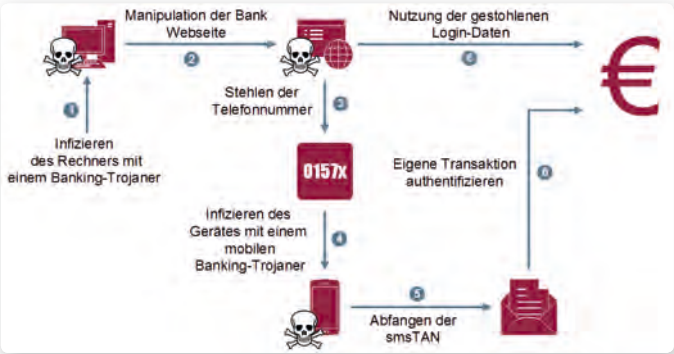

Abbildung 7: Schematischer Angriff auf das mobileTAN-Verfahren: Quelle: ifis

Anzeige

der schematische Ablauf zur Infektion beider Geräte erläutert. Durch die Infektion beider Geräte mit einem speziellen Banking-Trojaner ist der Angreifer in der Lage, selber Transaktionen zu erstellen und diese mit der gestohlenen TAN zu autorisieren:

1. Durch unterschiedliche Infektionsvektoren (zum Beispiel Drive-by-Download, Phishing-Mail o.Ä.) wird ein Banking-Trojaner auf dem Rechner des Opfers installiert.
2. und **3.** Der Trojaner manipuliert die Webseite der Bank (mittels eines „Man-in-the-Browser"-Angriffs), um die Telefonnummer und die Anmeldedaten des Opfers zu ermitteln. Dazu fügt der Angreifer clientseitig ein Feld in die Webseite der Bank ein, über welches er die Telefonnummer abfragt.
4. Das Opfer erhält eine SMS, die beispielsweise dazu auffordert, ein neues „Sicherheitszertifikat" zu installieren. Hinter dem „Sicherheitszertifikat" verbirgt sich ein Trojaner des Angreifers. Sobald das Opfer die Installation startet, wird der Trojaner auf das Mobiltelefon aufgespielt.
5. Der Trojaner überwacht die eingehenden SMS, um enthaltene TANs zu ermitteln und an den Angreifer weiterzuleiten.
6. Mit den in Schritt 3 gestohlenen Anmeldeinformationen loggt sich der Angreifer auf der Webseite der Bank ein. Dort erstellt der Angreifer eine gefälschte Transaktion auf ein beliebiges Konto. Durch den in Schritt 4 installierten Banking-Trojaner erhält der Angreifer die TAN für seine Transaktion. Somit ist der Angreifer in der Lage, das mobileTAN-Verfahren zu brechen.

Banken im Cyberwar?

Neben dem Angriff auf Privat- und Geschäftskunden von Banken, in dem der Angreifer rein monetäre Motivationsgründe hat, könnten andere Staaten, kriminelle Hackergruppen des organisierten Verbrechens und vor allem Terroristen versuchen, den Bankensektor an sich anzugreifen und so das Bankgeschäft zumindest für einen gewissen Zeitraum lahmzulegen. Der Angreifer hat in diesem Szenario kein monetäres Interesse, sondern zielt auf einen gesellschaftlichen Schaden ab, um politische Ziele durchzusetzen. Finanzagenten sind hier nicht nötig. So könnte das Vertrauen der Bankkunden in das Online-Banking stark beeinträchtigt werden, wenn im Online-Banking bei vielen Kunden gleichzeitig stark manipulierte Werte angezeigt werden oder der Banking-Service komplett lahmgelegt wird. Da das Vertrauen der Kunden ein wichtiges Gut der Banken ist, würde die Reputation der Banken und damit auch die des Online-Bankings hierdurch nachhaltig geschädigt werden. Neben dem gesellschaftlichen Schaden würde ein solcher Angriff, wenn er großflächig angelegt ist, in einer Gesellschaft, die weitgehend auf elektronische Zahlungen setzt, die Wirtschaft empfindlich treffen. Der Schaden, den die Banken hiermit erleiden, würde den bislang anfallenden Schaden um ein Vielfaches übersteigen.

Neue Lösungsansätze

Trotz der erhöhten Sicherheit, die das mobileTAN-Verfahren und besonders das chipTAN-Verfahren und HBCI-Secoder-Verfahren gegenüber alten Verfahren wie beispielsweise iTAN heutzutage noch bieten, ist davon auszugehen, dass diese Varianten in Zukunft durch neue, moderne Varianten zur Transaktionssicherung abgelöst werden müssen. Dies ist vor allem durch die Zunahme von Mikro-Transaktionen und das Bezahlen mit Kreditkarte erforderlich geworden. Erste Unternehmen haben bereits innovative Verfahren vorgestellt, um das Bezahlen per Kreditkarte in Zukunft abzusichern. Die prominentesten Beispiele hierfür sind: „Pay By Selfie", das von MasterCard eingeführt wird und „Smile to Pay", das von Alibaba entwickelt wird. Beide Verfahren nutzen biometrische Eigenschaften eines Menschen, um eine Transaktion zu autorisieren. Dabei wird das Gesicht des Kunden gescannt, wenn dieser eine Transaktion durchführen will. Zur Autorisierung wird also kein Passwort (PIN) mehr benötigt.

Ein nicht so innovatives Konzept setzen deutsche Kreditinstitute für das Online-Banking mit dem Namen „pushTAN" um. Dabei wird die TAN, ähnlich wie bei mobileTAN, an das Smartphone des Bankkunden gesendet. Allerdings benötigt der Bankkunde eine spezielle App auf seinem Endgerät, welche die TAN empfängt. Die Kreditinstitute erhöhen somit die Schwierigkeit, die TAN abzugreifen deutlich, da die App die Nachrichten verschlüsseln kann (anders als bei einer SMS). Ebenfalls kann der Zugriff auf die App geschützt werden.

Vor allem bei der Authentifizierung der Bankkunden gegenüber der Online-Banking-Webseite bestehen, wie bei den meisten Applikationen, einfache Möglichkeiten, die Sicherheit zu erhöhen. So setzen alle Banken noch Nutzernamen und Passwörter zur Authentifizierung der Bankkunden ein. Einige Banken limitieren das Passwort sogar auf lediglich fünf Zeichen. Dabei könnten die Banken die Verfahren, die zur Autorisierung einer Transaktion genutzt werden, auch zur Authentifizierung am Online-Banking-Konto nutzen (zum Beispiel ein One-Time-Passwort per SMS an den Kunden bei mobileTAN, eine Authentifizierung über den Flickercode beim chipTAN-Verfahren beziehungsweise eine Authentifizierung mittels Signaturkarte beim HBCI-Secoder-Verfahren).

Eine weitere Möglichkeit stellt die Nutzung digitaler Identitäten wie des neuen Personalausweises (nPA) dar. Der nPA bietet die Möglichkeit, eine gesicherte Online-Identifikation, die sogenannte eID-Funktion, mittels des nPA und einer 6-stelligen PIN durchzuführen. Zusätzlich bietet der nPA die Möglichkeit, qualifizierte elektronische Signaturen (QES) zu erzeugen. QES sind dabei rechtlich einer Unterschrift per Hand gleichgestellt. Die QES könnte dazu genutzt werden, die Transaktionsdaten vor unbemerkter Manipulation zu schützen. Diese Verfahren sind aber für den Bankkunden umständlich zu bedienen.

Ein weiteres Beispiel für eine digitale Identität, starke Authentifikation und Signaturen stellt das XignQR-System dar. XignQR basiert auf PKI-Technologien, nutzt die Fernsignatur aus der eIDAS-Verordnung (elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt) und ist sehr einfach zu handhaben. Damit kann beim Online-Banking, neben einer starken Zwei-Faktor-Authentifizierung, auch eine sehr sichere und europaweite anerkannte Sicherung der Transaktionsdaten benutzerfreundlich und sicher umgesetzt werden [3].

Neben der Entwicklung neuartiger Verfahren, um den Betrug im Online-Banking zu erschweren, ist es ebenso wichtig, Bankkunden auf aktuelle Gefahren hinzuweisen. Oft ist erst durch ein ‚Fehlverhalten' des Bankkunden ein Angriff möglich. Daher muss der Bankkunde eine zentrale Rolle im gesamten Sicherheitskontext einnehmen. Es werden Systeme benötigt, die basierend auf der aktuellen Gefahrenlage im Internet einschätzen können, ob eine besondere Gefahr im Online-Banking besteht. Ein solches

Alarmierungssystem würde den Bankkunden auf besondere Gefahrensituationen hinweisen und diesen so für gewisse Gefahrensituationen sensibilisieren. Das Institut für Internet-Sicherheit – if(is) erforscht daher im Rahmen eines Forschungsprojekts, das sich mit dem Betrugsschutz im Online-Banking befasst, Mechanismen, die Bankkunden vor aktuellen Gefahren warnen. Beispielsweise wurde ein System entwickelt, welches mittels kollektiver Intelligenz Manipulationen auf Webseiten erkennt und den Bankkunden warnt, sobald er eine manipulierte Webseite betrachtet [4].

Fazit

Angreifern ist es zurzeit möglich, die gängigen TAN-Verfahren erfolgreich anzugreifen. Allerdings ist eine Monetisierung relativ schwierig durchzuführen, insbesondere weil die Angreifer auf Finanzagenten angewiesen sind. Das führt dazu, dass sich der offiziell angegebene Schaden noch in Grenzen hält. Trotzdem werden die Banken die technischen Abwehrmechanismen für die Angriffe weiter verbessern, um den Schaden gering und insbesondere die Reputation aufrechtzuerhalten.

Der wirtschaftliche Schaden, den die Banken zurzeit durch Betrugsfälle im Online-Banking erleiden, ist vernachlässigbar im Vergleich zu dem Schaden, der durch einen großflächig ausgelegten Angriff zum Beispiel im „Cyberwar" entstehen würde. Für beide Szenarien werden moderne Verteidigungsmechanismen benötigt, die zum einen eine hohe Nutzbarkeit für den Bankkunden bieten und zum anderen die Sicherheit der Online-Banking Systeme deutlich verbessern. Dies betrifft bankenseitige sowie nutzerseitige Schutzmaßnahmen. ■

Quellenangaben

[1] *Bitkom, Online-Banking ist bequem und sicher. [Online] Available: https://www.bitkom.org/Presse/Presseinformation/Online-Banking-ist-bequem-und-sicher.html. Accessed on: Aug. 10 2016.*

[2] *Bundeskriminalamt, „Cybercrime: Bundeslagebild 2014", 2015. [Online] Available: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2014.html. Accessed on: Aug. 14 2016.*

[3] *M. Hertlein, P. Manaras, and N. Pohlmann, „Abschied vom Passwort – Authentifikation für ein gereiftes Internet", DATAKONTEXT-Fachverlag, 2015.*

[4] *T. Urban and N. Pohlmann, „Sehen heißt glauben! Aufdeckung von Webseiten Manipulation", in Proceedings der DACH Security 2016 Konferenz.*

TOBIAS URBAN,
wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen; er leitet den Forschungsbereich Zahlungssysteme und Banktransaktionen.

RICK WIDDERMANN,
wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen; er ist im Forschungsbereich Zahlungssysteme und Banktransaktionen tätig.

PROF. DR. NORBERT POHLMANN,
Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT

otris privacy
Konzerndatenschutz

40. DAFTA
17.-18. November, Köln
40 Jahre DAFTA und otris ist dabei!

otris software
vereinfacht Verantwortung.

www.otris.de