TRUST IN GERMAN SICHERHEIT

G DATA WHITEPAPER

DIE GEFAHREN BEI ONLINE-BANKING UND -SHOPPING

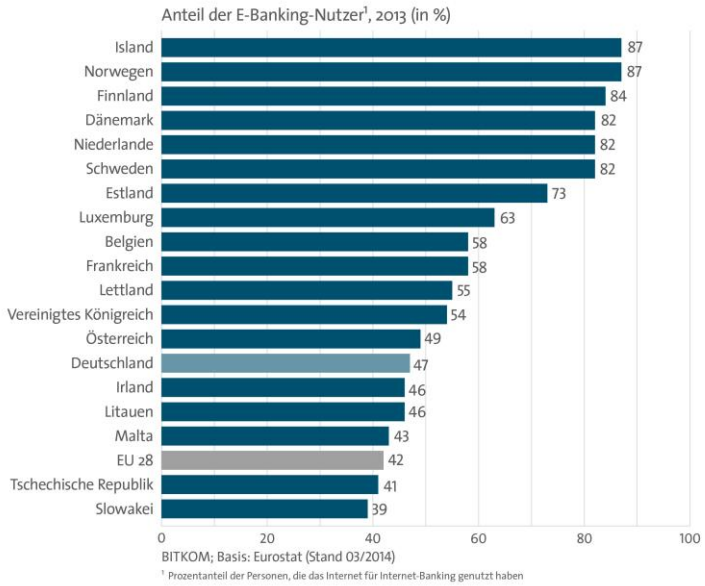
TRUST IN GERMAN SICHERHEIT

INHALT

MOTIVATION

Finanzieller Gewinn ist schon seit langem der zentrale Beweggrund von hochprofessionellen Cyberkriminellen und weltweit organisierten Hackerbanden. Vor diesem Hintergrund kann es nicht überraschen, dass die wachsende Zahl von Online-Banking-Nutzern nach wie vor eines der wichtigsten Angriffsziele darstellt. Was kann mehr Gewinn versprechen, als per Internet bewegtes Geld direkt an der Quelle abzuschöpfen?

Laut Branchenverband BITKOM ist die Zahl der Online-Banking-Nutzer in Deutschland von 27 Millionen im Jahr 2011 auf 37 Millionen im Jahr 2014 angestiegen. Das entspricht 47 Prozent aller Internetnutzer zwischen 14 und 74 Jahren. Bei den 14- bis 29-jährigen Nutzern beträgt der Anteil 70 Prozent, bei den 30- bis 49-jährigen sind es sogar 71 Prozent. [1][2]



Deutschland liegt beim Anteil der Online-Banking-Nutzer im europäischen Mittelfeld. (Quelle: BITKOM)

Demgegenüber stehen 16,4 Millionen Euro Beute, die Cyberkriminelle in Deutschland laut Bundeskriminalamt im Jahr 2013 aus Attacken auf diese Nutzergruppe erbeutet haben. Das BKA schätzt den tatsächlichen Schaden mit 180 Millionen Euro jedoch erheblich höher ein, weil nur etwa 10 Prozent aller erfolgreichen Cyber-Angriffe überhaupt zur Anzeige kommen. Pro Fall erbeuten die Diebe im Schnitt 4.000 Euro. Das Landeskriminalamt in Bayern schätzt die Höhe der durchschnittlichen Beute mit 5.000 Euro sogar noch höher ein. [3]

Die Studie „Online-Banking 2014 – Sicherheit zählt!“, erstellt von TNS Infratest im Auftrag des IT-Dienstleisters Fiducia und der Initiative D21, hat ergeben, dass rund zwei Prozent der Befragten Anwender schon einmal einen Schaden beim Online-Banking erlitten haben. Drüber hinaus haben 17 Prozent davon berichtet, dass in ihrem direkten Umfeld ein solcher Schadensfall eingetreten ist. [4] [5]

Trotz neuer Sicherheitsverfahren beim Online-Banking besteht also nach wie vor eine relativ große Wahrscheinlichkeit, Opfer eines Angriffs zu werden und dabei viel Geld zu verlieren. Die Angriffsmethoden haben sich in den letzten Jahren jedoch grundlegend verändert: Ursprünglich waren „Social Engineering“-Ansätze wie Phishing, mit denen Anwendern die benötigten Zugangsdaten und TAN-Nummern für Kontotransaktionen entlockt wurden. Weil aktuelle Sicherheitsverfahren immer eine Zweiwege-Autorisierung und eine Kontrolle des Anwenders mit einschließen, sind kompliziertere Angriffsverfahren erforderlich. [6] Diese setzen ohne Ausnahme

auf den Einsatz von hochspezialisierten Schadprogrammen und erfordern – neben der Wachsamkeit des Anwenders - ebenso spezialisierte Sicherheitslösungen zu deren Abwehr. Dabei sind in zunehmendem Maß sowohl Windows-PCs als auch Mobilgeräte betroffen, die immer stärker für Online-Banking oder die Zweiwege-Autorisierung genutzt werden. [7]

AKTUELLE AUTORISIERUNGS-VERFAHREN FÜR ONLINE-BANKING

Grundsätzlich existieren zwei vollkommen unterschiedliche Wege für Online-Banking: über das HBCI/FinTS-Protokoll und eine zugehörige Client-Software oder über den Internet-Browser und die Nutzung eines Web-Portals. Da der Anteil von Angriffen auf HBCI/FinTS-Clients verschwindend gering ist und die weitaus meisten Anwender ihre Bankgeschäfte mit dem Internet-Browser erledigen, soll dieses Verfahren in dieser Betrachtung außen vor gelassen werden.

Grundlage aller Autorisierungsverfahren für webbasiertes Online-Banking ist die Aufteilung des Kontozugangs in eine Nutzer-Identifizierung per Zugangspasswort/PIN und die Freigabe von Konto-Transaktionen durch Transaktionsnummern (TANs). Diese Transaktionsnummern wurden ursprünglich als Liste per Post an den Anwender verschickt und konnten in beliebiger Reihenfolge zur Freigabe von Überweisungen usw. verbraucht werden. Kannte ein Angreifer neben den Zugangsdaten auch nur eine der gültigen (also noch nicht verwendeten) TANs, hatte er alle Daten zur Durchführung einer betrügerischen Überweisung in der Hand. Aktuelle Verfahren setzen deshalb auf verschärfte Kriterien für die Gültigkeit einer Transaktionsnummer.

iTAN

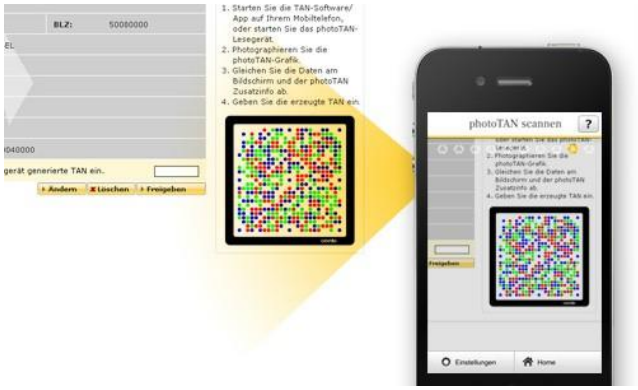
Beim iTAN-Verfahren ist nicht mehr eine beliebige TAN aus der verschickten Liste gültig, sondern lediglich die TAN an einer zufällig festgelegten Position. Ohne Kenntnis der gesamten Liste – oder großer Teile davon - ist in der Praxis keine Autorisierung durchführbar. Nachteil: Durch geschicktes Phishing mehrerer TANs oder Diebstahl der Liste kann ein Angreifer die nötigen Kenntnisse zur Freigabe von Überweisungen erlangen.

SMS-TAN/M-TAN

Das SMS-TAN/M-TAN-Verfahren kommt ohne vorher festgelegte Liste aus und führt zusätzlich einen zweiten Übertragungsweg bei der Erzeugung einer gültigen TAN ein: Der Anwender legt im Internet eine Überweisung oder eine andere Kontobewegung an, daraufhin schickt die Bank eine nur für diesen Vorgang gültige TAN sowie die Zielkontonummer und den Betrag per SMS auf das Mobiltelefon des Kunden. Die Verknüpfung von Betrag, Zielkonto und TAN und die Kontrollmöglichkeit der Übertragungsdaten durch den Kunden erschweren das Abschöpfen einer gültigen TAN gegenüber dem iTAN-Verfahren. Allerdings besteht die Gefahr, dass die verschickten SMS-Nachrichten abgefangen oder durch Schadsoftware auf dem Mobiltelefon weitergeleitet werden.

Photo-TAN/Push-TAN

Anders als beim SMS-TAN-Verfahren kommen Photo-TAN und Push-TAN ohne SMS-Nachrichten aus. Beim Photo-TAN-Verfahren wird nach dem Anlegen einer Transaktion eine farbige Grafik auf dem Bildschirm des PCs angezeigt, die mit der Kamera des Mobiltelefons abfotografiert und durch eine Banking-App auf dem Telefon in eine TAN umgewandelt wird. Wahlweise kann auch ein Lesegerät die Grafik interpretieren, was wegen der geringeren Gefahr einer Manipulation die sicherere Alternative ist.



Beim PhotoTAN-Verfahren erfolgt die Erzeugung einer TAN durch Auslesen einer verschlüsselten Grafik auf dem PC-Bildschirm. (Quelle: Commerzbank)

Das Push-TAN-Verfahren schickt die online angelegten Transaktionsdaten per Internet an die Banking-App auf dem Mobiltelefon des Anwenders. Dort können diese überprüft und eine TAN-Nummer daraus erzeugt werden. Sowohl Photo-TAN als auch Push-TAN versperren Angreifern den Weg, die durch Abschöpfen von SMS-Nachrichten an gültige TANs gelangen wollen. Die eingesetzten Banking-Apps auf dem Mobiltelefon können jedoch ebenfalls Ziel von Angriffen werden.

Chip-TAN/e-TAN/smartTAN

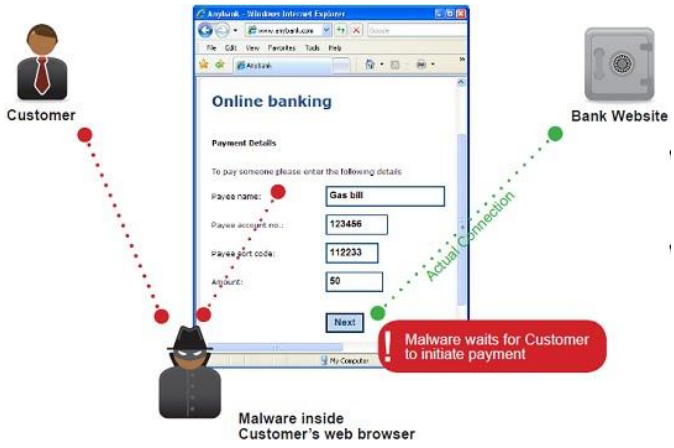
Das allgemein als Chip-TAN bezeichnete Autorisierungs-Verfahren nutzt nicht das Mobiltelefon, sondern einen elektronischer TAN-Generator zur Erzeugung einer gültigen Transaktionsnummer. Je nach Ausprägung unterscheidet sich die Methode, mit der die TAN erzeugt wird:

- Beim smartTAN-Verfahren genügt es, eine zum Konto gehörende Kundenkarte (Maestro-/ec-/V-Pay-Karte) in den TAN-Generator einzuschieben, um dann auf Knopfdruck gültige TANs erzeugen zu können. Schwachstelle: Der Diebstahl der Kundenkarte ermöglicht es einem Angreifer, gültige TANs zu erzeugen. Die Sperrung der Karte kann den Angriffsversuch jedoch vereiteln.
- Ein eTAN-Generator ist für den Kunden personalisiert und erzeugt die TAN-Nummer unter Verwendung eines geheimen Schlüssels, der Uhrzeit und der Kontonummer des Überweisungs-Empfängers. Die wird vom Kunden auf der Zehner-Tastatur des Geräts eingetippt. Bei manchen Bankinstituten findet statt der Empfänger-Kontonummer auch eine vom Internet-Portal generierte Kontrollnummer Verwendung. Die ist jedoch anfällig für Manipulationen.
- Beim chipTAN-Verfahren kommt ein elektronischer TAN-Generator mit Karteneinschub und Zehnertastatur zum Einsatz. Zunächst wird die Kundenkarte in das Gerät eingeschoben, danach erfolgt die Erzeugung der TAN je nach Institut auf unterschiedliche Weise: Bei einigen Banken gibt der Kunde über die Tastatur einen Startcode, die Kontonummer des Empfängers sowie den Betrag ein (chipTAN manuell). Bei vielen Sparkassen und Volksbanken wird dagegen eine Grafik aus fünf schwarz-weiß flackernden Balken („Flicker-Code“) am Bildschirm des Computers angezeigt, die der TAN-Generator mit optischen Sensoren einliest. Auf diese Weise werden ebenfalls die Ziel-Kontonummer und der Betrag übertragen, die der Kunde vor der Erzeugung der TAN am Gerät kontrollieren kann. Dieses Verfahren gilt derzeit als das sicherste. [7]

ANGRIFFSMETHODEN

Die Verknüpfung von Transaktionsdaten und TAN sowie die Nutzung eines zweiten, vom PC entkoppelten Übertragungswegs zur Erzeugung von gültigen TANs hat es Hackern und Cyberkriminellen viel schwerer gemacht, an die Daten zur Durchführung einer Überweisung zu kommen. Es genügt nicht mehr, die Konto-Zugangsdaten und eine unverbrauchte TAN oder die TAN-Liste in die Hände zu bekommen. Die Online-Diebe benötigen eine TAN, die zu ihrer unrechtmäßigen Überweisung passt. Gemeinsamer Ansatzpunkt aller wirksamen Angriffsmethoden ist deshalb die Manipulation der Überweisungsdaten schon vor der Erzeugung der TAN.

Cyberkriminelle greifen zu diesem Zweck auf hochspezialisierte Trojaner zurück, die zu den fortgeschrittensten Schadprogrammen überhaupt gehören. In der Regel lassen sich die Trojaner durch Erweiterungen, sogenannte Web-Injects, exakt an eine Vielzahl internationaler Online-Banking-Portale anpassen. Diese Erweiterungen greifen die gängigen Webbrowser (Internet Explorer, Firefox, Google Chrome, Opera) an und manipulieren die Kommunikation zwischen PC und Bankrechner. Die verschlüsselte Kommunikation zwischen dem Computer des Anwenders und dem Server der Bank wird dabei ausgehebelt, weil sämtliche verschickte Daten schon vor bzw. nach der Verschlüsselung im Browser verändert werden. Aus dem „Man-in-the-Middle"-Angriff, der die Kommunikationskette unterbricht und manipuliert, wird so ein „Man-in-the-Browser"-Angriff, der die Hürde verschlüsselter Kommunikation elegant unterläuft. [3]



Aktuelle Schadprogramme klinken sich in den Browser des Opfers ein und manipulieren die Bankdaten vor bzw. nach der Verschlüsselung. (Quelle: securityaffairs.co)

Der Angriff selbst kann in unterschiedlichen Komplexitätsstufen erfolgen:

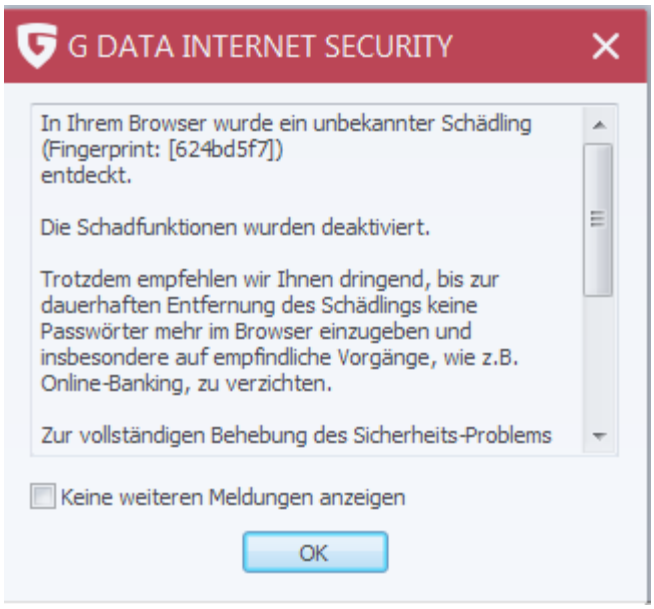
- Im einfachsten Fall spiegelt das Schadprogramm dem Anwender eine vorgebliche „Rücküberweisung", „Testüberweisung", „Sicherheitsüberprüfung", „Umstellung auf das IBAN-Verfahren" oder ähnliches vor. Dazu soll der Anwender eine TAN erzeugen und eingeben. Die erzeugte TAN passt zu einer im Hintergrund ablaufenden Überweisung auf das Konto der Kriminellen. Der Vorteil dieses Verfahrens: Durch die vorgebliche Legitimität und die Freigabe der Überweisung durch den Kunden werden alle gängigen Autorisierungsverfahren einschließlich ChipTAN ausgehebelt. Nachteil: Ein informierter Kunde erkennt sofort den Betrugsversuch.

- Durch Einblenden eines zusätzlichen Textfelds auf der Login-Seite der Bank werden die Handynummer des Kunden und das Betriebssystem seines Mobiltelefons abgefragt. Ein Link zum Download einer vorgeblichen Sicherheitssoftware veranlasst ihn, sein Mobiltelefon mit einem weiteren Schadprogramm zu infizieren. Ist dies geschehen, kontrollieren die Angreifer den Zugang zum Bankkonto und können die per SMS zugeschickten TAN-Nummern abgreifen. Das versetzt sie dazu in die Lage, eigene Überweisungen durchzuführen. Je nach Autorisierungsverfahren sind auch Schadprogramme zur Abfrage/Weiterleitung von PhotoTANs oder PushTANs denkbar.
- Das Schadprogramm manipuliert die Überweisungsdaten im Hintergrund und vom Kunden unbemerkt, sodass die veränderten Daten zur Erzeugung einer gültigen TAN zum Einsatz kommen. Der Betrug fliegt nur dann auf, wenn der Anwender die Zieldaten der Überweisung vor Eingabe der TAN noch einmal überprüft.
- Mithilfe der per Schadprogramm abgefragten persönlichen Daten bestellen die Angreifer beim Mobilfunkanbieter des Kunden eine zweite SIM-Karte. Damit können sie die SMS zur Übermittlung von Transaktionsnummern auf einem eigenen Mobiltelefon empfangen und eigene Überweisungen vornehmen.
- Besonders gut organisierte Banden haben sogar schon die Nummer der Bank-Hotline manipuliert, um die Anrufe misstrauischer Kunden in einem eigenen Callcenter abzufangen. Die dortigen „Bank-Mitarbeiter“ erklärten den Opfern die Einblendungen der Schadsoftware als unbedenklich und ermunterten sie, den Anweisungen auf dem Bildschirm zu folgen. [3]

SO SCHÜTZT G DATA BANKGUARD VOR „MAN-IN-THE-BROWSER“-ANGRIFFEN

Natürlich erfolgt der erste Schutz vor einem Banking-Trojaner durch die Virenerkennung der installierten Sicherheitslösung. Ist die Signatur des Schadprogramms bekannt, wird es schon beim Download identifiziert und unschädlich gemacht.

Sollte die Erkennung bei einem noch unbekannten Schadprogramm scheitern, schützt G DATA BankGuard den Browser vor einer Manipulation durch Web-Injects. Beim Online-Banking – so wie auch beim verschlüsselten Zugriff auf einen Online-Shop - wird die Verbindung zum Bankrechner über eine im Arbeitsspeicher befindliche Browser-Bibliothek eingerichtet. Hier findet die Entschlüsselung der Daten aus der verschlüsselten SSL-Verbindung statt. G DATA BankGuard vergleicht die aktuell in den Arbeitsspeicher geladene Version der Bibliothek mit einer von BankGuard selbst erstellten, vertrauenswürdigen Kopie. Wird eine Abweichung erkannt, weist eine eingeblendete Warnmeldung den Anwender auf die Gefahr hin. Der Browser wird zwangsweise sofort beendet und vom erkannten Banking-Trojaner bereinigt. So wird eine Manipulation der Daten durch das Schadprogramm wirkungsvoll verhindert.



G DATA BankGuard ist Teil aller G DATA-Sicherheitslösungen für Windows (ANTIVIRUS, INTERNET SECURITY, TOTAL PROTECION) und lässt sich über eine Option in den Programmeinstellungen ganz einfach ein- und ausschalten.

G DATA INTERNET SECURITY FÜR ANDROID sichert zusätzlich die Übertragung von Transaktionsnummern

G DATA INTERNET SECURITY FÜR ANDROID kann den Schutz wirkungsvoll ergänzen, wenn der Bankkunde eines der Autorisierungs-Verfahren für Mobiltelefone verwendet. Das Programm analysiert die Berechtigungen aller installierten Apps und erkennt auf diese Weise auch bislang unbekannte Phishing-Apps. Darüber hinaus identifiziert der zuverlässige Malware-Scanner die Signaturen bekannter Schadprogramme unter den Downloads und den Apps im Gerätespeicher. Auf diese Weise bleibt bei einem Online-Banking-Angriff das Abgreifen von SMS-Nachrichten oder durch Apps erzeugten TANs verwehrt.

LITERATURVERZEICHNIS

1. BITKOM: Eurostat-Statistik E-Banking-Nutzung
   http://www.bitkom.org/de/markt_statistik/64034_65226.aspx
2. BITKOM: 37 Millionen Deutsche nutzen Online-Banking
   http://www.bitkom.org/de/markt_statistik/64034_80365.aspx
3. Uli Ries: Bankraub Digital, c't Ausgabe 25/2014, Seite 76
   http://www.heise.de/ct/ausgabe/2014-25-Millionenschaeden-durch-Angriffe-aufs-Online-Banking-2450695.html
4. Kurt Sagatz: Angriffe auf den digitalen Geldbeutel nehmen zu
   http://www.tagesspiegel.de/medien/digitale-welt/online-banking-angriffe-auf-den-digitalen-geldbeutel-nehmen-zu/10034102.html
5. Studie der Initiative 21: „Online Banking – Sicherheit zählt"
   http://www.initiatived21.de/wp-content/uploads/2014/07/d21_fiducia_studie_onlinebanking_2014.pdf
6. Sara Zinnecker: Vorsicht beim Online-Banking
   http://www.handelsblatt.com/finanzen/steuern-recht/recht/ratgeber-hintergrund/sicherheitsluecken-vorsicht-beim-online-banking/9434420.html
7. BITKOM: Leitfaden Online-Banking
   http://www.bitkom.org/de/publikationen/38337_81169.aspx