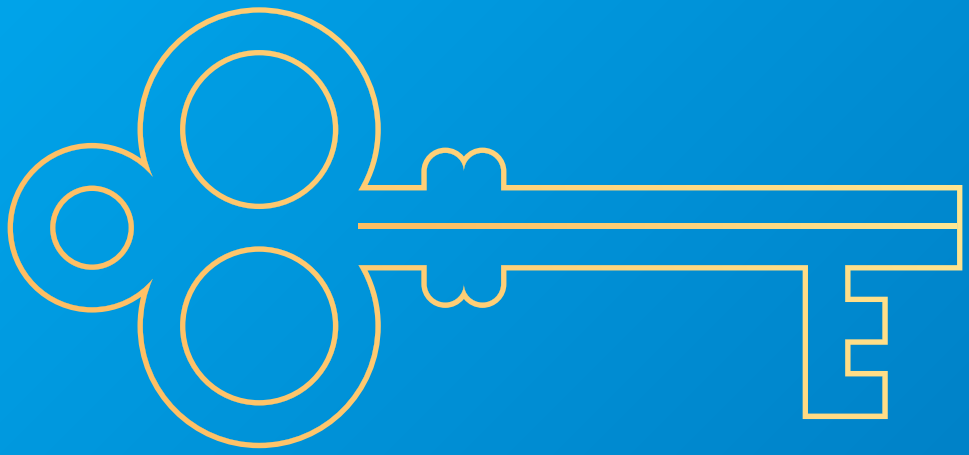
Outbank



Von Zertifikaten und Verschlüsselungen

Ein Guide zu sicherem Online- und Mobile-Banking

Inhalt

1. Executive Summary

Mobile Banking ist bequem, schnell und effizient, doch häuften sich in den letzten Jahren die Bedenken deutscher Nutzer, wie sicher mobiles Banking wirklich ist. Bisher wurde wenig Aufklärung betrieben, die dem Nutzer detailliert aufzeigt, mit welchen Technologien und Möglichkeiten die Privatheit und der Schutz seiner Daten gewährleistet werden können. Wer sich um die Integrität seiner Daten sorgt, kann beispielsweise nach Anbietern Ausschau halten, die auf externe Datenspeicherung verzichtet und die Daten direkt auf dem Telefon verschlüsselt speichert. Wer Bedenken hat, dass Transaktionen abgefangen und umgeleitet werden könnten, kann sich an die Banking-Apps halten, die Wert auf die kontinuierliche Überprüfung der Sicherheitszertifikate der Banken legt. Wer Sorgen hat, dass Unbefugte über das Smartphone Überweisungen tätigen könnten (z.B. im Fall des Telefonverlustes) sollte sich einen Anbieter aussuchen, der besonders auf lokale Verschlüsselung der Daten achtet und dafür besonders hohe Passwort-Sicherheitsmaßnahmen verwendet.

Die Generalisierung „Mobiles Banking ist unsicher“ entspricht schon lange nicht mehr der Wahrheit und unterschätzt die technischen Möglichkeiten, Banking-Applikationen umfassend zu schützen. Im folgenden Whitepaper werden diese Technologien detailliert vorgestellt und dahin gehend erläutert, wie sie potenzielle Gefahren vorbeugen oder verhindern. Zudem befindet sich am Ende des Whitepapers ein Glossar zum Thema Sicherheit. Dies dient nicht nur zum besseren Verständnis der Sicherheitsarchitektur im Banking, sondern soll den interessierten Mobile Banker unterstützen, eine wirklich sichere Applikation zu finden. Wer Banking-Anbieter auf diese Begrifflichkeiten untersucht, ist auf der sicheren Banking-Seite.

2. Wie steht Outbank zur Banking-Sicherheit?

Die Finanzlage entscheidet darüber, wie man den Alltag gestaltet. Geld erlaubt die monatliche Miete, das tägliche Mittagessen oder auch ein neues Auto zu bezahlen. Deshalb sind alle Daten rund um Geld und Finanzen nicht nur sehr persönlich, sondern auch besonders sensibel. Diese Daten sollen nur die Menschen sehen, denen man absolutes Vertrauen schenkt.

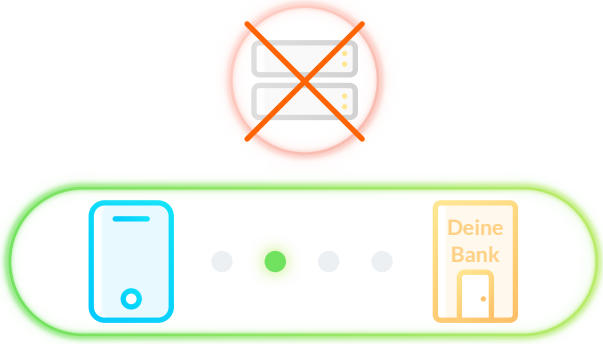
Genau deshalb unterstützt Outbank den Ansatz der absoluten Data Privacy und verschlüsselt, speichert und sichert die Daten mit den modernsten Verschlüsselungsstandards auf dem persönlichen Gerät des Nutzers. Um höchstmögliche Sicherheit auf dem Endgerät und während der Kommunikation mit Banken, z.B. im Fall einer Überweisung, zu schaffen, hat Outbank folgende Sicherheitsmaßnahmen implementiert:

- **Lokale Datenspeicherung**

Outbank speichert alle Finanzdaten verschlüsselt auf dem Endgerät des Nutzers. Die Daten sind somit wirklich nur vom Nutzer und weder von Outbank noch anderen Drittparteien einsehbar. Man spricht in diesem Fall auch vom Zero-Knowledge-Prinzip. Auch große Unternehmen, wie Apple, stellen derzeit mehr und mehr auf absolute Data Privacy durch Zero-Knowledge um und speichern Nutzerdaten nur noch auf deren Endgeräten, ohne selbst Zugriff darauf zu haben.

- **Modernste Datenverschlüsselung**

Wenn Daten verschlüsselt werden, entsteht beispielsweise aus dem Verwendungszweck „Autoversicherung“ ein langer Block an zusammengewürfelten Zeichen- und Zahlenkombinationen - auch Chiffretext genannt. Für Menschen und Computer ergeben diese Zeichenkombinationen keinen Sinn und sind de facto unlesbar. Doch selbstverständlich gibt es in der Schwierigkeitsstufe dieser Kombinationen auch starke Unterschiede. Outbank nutzt zur Verschlüsselung der sensiblen Finanzdaten den weltweit sichersten Standard - die symmetrische AES-Verschlüsselung. Sie wird u.a. auch zur Sicherung von Regierungsdokumenten der höchsten Klassifizierungsstufe genutzt. Um die Daten zu entschlüsseln und damit für den Menschen wieder verständlich und lesbar zu machen, ist ein Schlüssel notwendig. Dieser Schlüssel wird bei Outbank aus dem Master-Passwort des Nutzers erzeugt. Nur der Nutzer kann mit diesem Passwort seine Daten wieder lesbar und nutzbar machen. Niemand außer dem Besitzer des Master-Passwortes hat somit Zugang zum verschlüsselten Inhalt.



- **Direkte Bank-Device-Kommunikation**

Wie im Fall der lokalen Datenspeicherung sind auch in der Kommunikation zwischen Bank und der Outbank App keine Proxy-Server zwischengeschalten. Sie erfolgt direkt zwischen Kreditinstitut und Endgerät. Ein Proxy-Server übernimmt die Kommunikation mit der Bank des Kunden und muss dazu die Zugangsdaten des Kunden in unverschlüsselter Form kennen. Somit kennt dieser Server die Zugangsdaten aller seiner Kunden und natürlich auch alle Finanzdaten, die zum Kunden übermittelt werden. Somit stellt dieser Server ein sehr lohnendes Ziel dar. Outbank eliminiert diese Gefahr vollständig, da die App immer direkt mit der Bank kommuniziert.

- **Sichere Bankzertifikate**

Jede Bank verfügt über ein Sicherheitszertifikat, dem sogenannten SSL- bzw. TLS-Zertifikat. Damit zertifiziert das Kreditinstitut, dass die Verbindung zu den Bankdienstleistungen nicht kompromittiert und damit vertrauenswürdig ist. Die meisten Banking-Anbieter überprüfen dieses Zertifikat in der Regel nicht explizit, da sie der Verantwortung dafür dem Betriebssystemhersteller überlassen. Die explizite Überprüfung der Zertifikate vor dem Verbindungsaufbau nennt man Certificate Pinning. Outbank verwendet Certificate Pinning für jede Verbindung. Zusätzlich überprüfen wir automatisiert die Sicherheit aller verwendeten Gegenstelle. Dies mehrmals stündlich von verschiedenen Orten (unterschiedliche autonome Zonen). Sobald eine Unregelmäßigkeit auftritt, wird eine Verbindung zur Bank von der App aus gesperrt. Im Falle eines Hackerangriffs auf die Kommunikation mit der Bank findet daher weder eine Verbindung noch Kommunikation zwischen App und Bank statt. Die damit verbundene erhöhte Sicherheit ist daher auch nur in Outbank und keiner anderen Banking-App gegeben.

- **Geschützte Datensynchronisierung**

Eine weitere Besonderheit der Outbank App ist die geschützte Synchronisierung der Daten auf allen Endgeräten. Dazu nutzt Outbank ebenfalls die AES-Verschlüsselung. Anonymisiert und als unlesbare Kryptogramme werden die

Daten über einen in Deutschland platzierten AWS-Server auf allen Endgeräten aktualisiert. Alle Information, die sich auf diesem Server befinden, sind mit dem individuellen Master-Passwort des Nutzers verschlüsselt, abgelegt und können somit nicht eingesehen werden.

Zusammengefasst schützt Outbank die Data Privacy, indem alle Daten auf dem Telefon nach höchsten Sicherheitsstandards verschlüsselt sind. Selbst wenn der Nutzer unsere Infrastruktur zur Datensynchronisierung nutzt, werden die Daten zunächst auf dem Telefon verschlüsselt und erst dann an den Server versandt. Dieser ist zur Synchronisierung der Daten notwendig. Zudem sichert Outbank die Kommunikation zwischen App und Bank mit einer kontinuierlichen Überprüfung des Sicherheitszertifikats des Kreditinstituts. Wie diese Sicherheitstechnologien konkret die Sorgen der Nutzer lösen und die Cyberbedrohungen abwehren, zeigt Kapitel vier.

3. Der gläserne Bürger - auch im Mobile Banking?

Wenn ich meine Daten an eine Banking-App abgebe, weiß das Unternehmen dahinter dann, wenn ich mal ein Minus auf dem Konto habe? Berichten sie das vielleicht sogar? Wie weiß ich, ob sie meine Daten nicht an Versicherungen und andere Finanzanbieter verkaufen, die mich dann mit Angeboten bedrängen? Alles berechtigte Fragen, die Outbank in einem Wort beantworten kann: Nein.

Nein, Outbank weiß zu keinem Zeitpunkt über den Kontostand des Nutzers Bescheid. Ob verschuldet oder Milliardär, Outbank hat keine Einsicht in die Finanzdaten. Sie werden verschlüsselt auf dem Telefon des Nutzers gespeichert, wo sie einzig und allein vom User per Eingabe des Master-Passworts eingesehen werden können.

Nein, es werden keine Kontostände an andere Finanzdienstleister weitergegeben. Da Outbank weder auf die Daten zugreifen, noch sie einsehen kann, ist die Weitergabe und der Verkauf von Finanzdetails unmöglich. In Outbank wissen nur die Bank und der Nutzer über dessen Finanzsituation Bescheid.

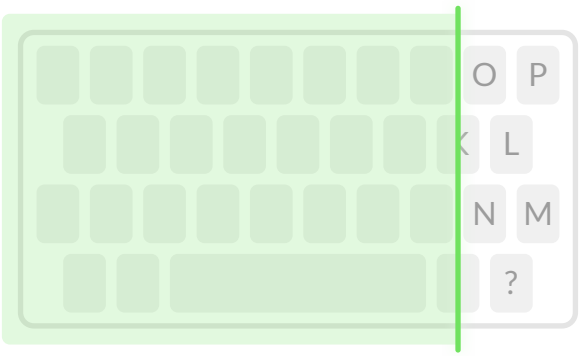
4. Wie überwindet man mit Outbank Banking-Gefahren?

Seit 2001 beobachtet Outbank den Mobile-Banking-Markt und entwickelte die App von Kategorisierung bis Touch ID je nach aktuellem Kundenwunsch weiter. Gleichzeitig observierte Outbank, welche Gefahrenpotenziale im Mobile Banking bestehen und die Sicherheitsbedenken unter den Nutzern steigern. Diese Gefahrenpotenziale beantwortet Outbank mit vier, über mehrere Jahre und mit viel Erfahrung, entwickelten Sicherheitstechnologien.

- **Gefahr #1: Telefonverlust**

Wenn ich mein Telefon verliere, was passiert dann mit meiner Banking-App? Kann der Dieb oder Finder meine Konten leer räumen?

Selbstverständlich nicht. Outbank speichert keine Passwörter. Der Finder des Telefons oder Laptops kann deshalb weder anhand eines Reset-Buttons, noch per E-Mail das Passwort erfragen oder abändern. Wer das Master-Passwort nicht kennt oder vergessen hat, dem bleibt die App verschlossen. Das heißt, ist der Finder oder Dieb im Besitz des Telefons kann er die App weder bedienen noch die Finanzdaten einsehen. Er müsste dafür zusätzlich das Passwort knacken. Doch das ist, wie im nächsten Schritt beschrieben, in der Outbank App kaum möglich.



- **Gefahr #2: Passwortdiebstahl**

Wer versucht das Passwort eines Outbank-Nutzers zu knacken, wird sich daran die Zähne ausbeißen. Da Outbank keine Passwörter speichert, gibt es keine Datenbank mit Passwörtern zu knacken, sondern der Betrüger muss zunächst ein höchst komplexes Verschlüsselungssystem aufdecken.

Schnelle Computer können heute bereits in wenigen Sekunden so viele Zahlenkombinationen berechnen, dass selbst richtig komplizierte Passwörter in kürzester Zeit geknackt werden können. Outbank schützt jedoch jeden Nutzer, egal wie schwer oder einfach er sein Master-Passwort wählt. Um dies zu ermöglichen, wird das Master-Passwort noch einmal zusätzlich verändert. Früher nutzte man dazu z.B. MD5 Hashes, doch auch diese Hashes können heutzutage durch schnelle Computersysteme mühelos geknackt werden.

Die bisher sicherste und in Outbank angewandte Methode sind Schlüsselableitungsfunktionen, im Englischen Key Derivation Function genannt. Aus einem Passwort wird mithilfe einer solchen Funktion ein neuer Schlüssel fester Länge erzeugt. Die Berechnung dieses Schlüssels kostet Zeit und erhöht den Zeitaufwand einer Brute-Force (Herausfinden des Passworts durch Ausprobieren) für einen Angreifer immens.

- **Gefahr #3: Viren & Trojaner**

Viren und Trojaner verstecken sich in allen Ecken des Internets. Wer sich Apps auch mal aus dem World Wide Web herunterlädt und nicht aus dem offiziellen App Store oder Play Store, läuft Gefahr sich einen dieser Viren auf das Smartphone oder den Computer zu laden. Warum Gefahr? Trojaner beinhalten heutzutage oft einen Key-Logger, der unbemerkt im Hintergrund die Finger-Tabs und Tastatureingaben aufzeichnet. Damit stehlen Hacker bevorzugt Passwörter.

In der Android-App sichert Outbank die Eingaben der Bankzugangsdaten gegen den Key-Logger mit einer höchst komplexen Technologie ab. Die Tastatur in Outbank ist nicht wie jede andere. Es handelt sich hierbei um ein Secure Keyboard. Diese Sicherheitstechnologie funktioniert wie eine Schutzschicht. Das Aufzeichnen von Benutzereingaben durch Trojaner wird damit deutlich erschwert.

- **Gefahr #4: Banken-Hack**

In den letzten Jahren häuften sich die Nachrichten zu möglichen Hackerangriffen auf Bankinstitute, sei es die britische Tesco-Bank, die russische Central Bank oder die Bangladesh Central Bank. Während Outbank selbstverständlich nicht den Angriff auf eine Bank verhindern kann, werden die Outbank Nutzer der jeweiligen Bank jedoch im Ernstfall geschützt. Liegt eine Kompromittierung des Sicherheitszertifikats vor, blockiert Outbank den Zugang zur Bank und verhindert so, dass die Nutzer in einem ungesicherten Bankenumfeld Transaktionen tätigen.

Möglich wird dieser Schutz durch aktives Certificate Pinning. Konkret bedeutet dieser Begriff, dass die Sicherheitszertifikate der Bank kontinuierlich auf ihre Unversehrtheit überprüft werden. Als vertrauenswürdige Banking-Applikation liegt Outbank der höchste Sicherheitsstandard am Herzen. Die Sicherheit aller Banken verifiziert Outbank deshalb für alle Nutzer in einem fünfzehn-minütigen Rhythmus.

5. Wie schützt man sich allgemein besser im Netz?

Sicherheit im Netz ist immer ein zweiseitiges Schwert. Ein beliebtes Sprichwort besagt dazu: „Sicherheit ist nur so sicher, wie sein schwächstes Glied." Während Outbank alle notwendig Schritte unternimmt, um den Nutzer nahezu 100%ige Sicherheit zu gewährleisten, bedarf es auch dem verantwortungsbewussten Zutun der Nutzer. Wie User zu noch mehr Sicherheit im Banking beitragen können, erläutern wir in den folgenden drei Punkten:

- **E-Mailanhänge prüfen**

Häufig schleusen sich Viren durch infizierte E-Mailanhänge auf den Computer oder das Smartphone. Daher raten wir allen Nutzern, keine Anhänge zu öffnen, deren Absender sie nicht kennen.

Spoofing-Mails sind jedoch mittlerweile bereits so ausgereift, dass sie sich an den Nutzer angleichen und als Absender einen bekannten Namen oder eine Institution angeben, mit der der Nutzer häufig in Kontakt steht. In dem Fall lohnt es sich, eine kurze Google-Suche mit der Betreffzeile der E-Mail zu machen. Sollte es sich um eine infizierte Spam-Mail handeln, weisen meist schon die ersten Suchergebnisse darauf hin.

Auf ähnliche Weise versuchen Phishing-Mails den Nutzer auf infizierte Seiten zu locken. Meist mit dem Namen eines bekannten Unternehmens getarnt, enthalten Phishing-Mails einen infizierten Link. Wer in den letzten 2-3 Wochen keinen Kontakt mit dem jeweiligen Unternehmen hatte, sollte diese Mails am besten direkt löschen. Wer sich doch lieber versichern möchte und die Mail öffnet, sollte jedoch nicht direkt auf den enthaltenen Link klicken. Per Mouse-Over wird üblicherweise die Linkadresse angezeigt. Führt diese Adresse nicht direkt zur Webseite des Unternehmens, handelt es sich um eine Umleitung auf eine infizierte Webseite.

- **Offizielle App Stores nutzen**

Die Problematik bezüglich externer Download-Plattformen besteht nicht erst seit dem Vorfall der infizierten Pokémon-Go-Vorversion, hat dadurch aber das Interesse der Öffentlichkeit geweckt. Und zwar bieten vereinzelte Webseiten immer wieder Download-Links zu sehr beliebten oder heiß erwarteten Apps an. Da diese Webseiten aber nicht den Sicherheitsbestimmungen der offiziellen App Stores unterliegen, kommt es häufig vor, dass diese Apps mit Viren infiziert sind.

Wir raten deshalb allen Nutzern, nur Apps aus dem Apple App Store oder Google Play Store herunterzuladen. Alle Apps, die dort gelistet sind, werden von den jeweiligen Plattformen zuvor geprüft und können deshalb bedenkenlos heruntergeladen werden.

- **Authentifizierung mit 2 Geräten durchführen**

Im Herbst 2016 sorgte eine Sicherheitslücke im photo-TAN-Verfahren deutschlandweit für großes Aufsehen. Grund der Sicherheitslücke war die TAN-Authentifizierung über nur ein Endgerät. Üblicherweise werden in sicheren TAN-Verfahren zwei, voneinander unabhängige Geräte benutzt, damit der Vorgang nur von dem durchgeführt werden kann, der im Besitz beider Geräte ist. Da die TAN im photoTAN-Verfahren nicht mehr auf einem zweiten Gerät generiert wird, haben Hacker leichtes Spiel. Sie nisten sich über ein Schlupfloch im Smartphone ein und hacken die TAN-Generator-App und können die TAN-Generierung somit manipulieren, aufzeichnen, abfangen oder die Überweisung so abändern, dass das Geld mit diesem TAN auf ein anderes Konto geleitet wird.

Aus diesem Grund raten wir unseren Usern, wenn möglich zwei verschiedene Geräte zu verwenden. Also z.B. eine Überweisung auf dem Mac auszuführen und die mobileTAN für die Transaktion auf dem Telefon/Smartphone zu empfangen. Dadurch ist sowohl die Generierung als auch Anwendung einer TAN sicher.

- **Webseiten ohne Schloss vermeiden**

Besitzt eine Webseite ein SSL-Zertifikat, ist das für jeden Nutzer sofort an einem kleinen Vorhängeschloss-Icon in der URL-Leiste ersichtlich. Dank des SSL- bzw. TLS-Zertifikats werden Datenströme verschlüsselt. Jede vertrauenswürdige Webseite, die Nutzerdaten abfragt oder speichert, sollte deshalb immer über ein SSL-Zertifikat verfügen. Liegt das Zertifikat nicht vor, können die Daten unter Umständen frei eingesehen werden und bieten Hackern ein einfaches Ziel. Wir raten allen Nutzern deshalb immer vor der Registrierung auf einer Webseite einen kurzen Blick auf die URL-Leiste zu werfen. Erscheint dort ein Schloss? Wenn ja, ist eine Grundsicherheit geschaffen.

6. Glossar

2-Faktor-Authentifizierung

Bei der 2-Faktor-Authentifizierung geht es ganz grundsätzlich darum, den Nutzer in vor digitalem Identitätsdiebstahl zu schützen. Heißt, indem der Nutzer seine Identität über zwei, voneinander unabhängige Faktoren bestätigt (z.B. einem Passwort und einer Information die bei der Anmeldung via SMS verschickt wird), können sich Hacker nur dann als der Nutzer ausgeben, wenn sie Zugang zu beiden Faktoren (Passwort und Mobiltelefon) haben.

In Bezug auf TAN-Verfahren spricht man auch von einer 2-Geräte-Authentifizierung. Hierbei wird ein Endgerät zur TAN-Generierung und eines für die TAN-Anwendung genutzt. Das Szenario lässt sich gut am Beispiel der smsTAN erläutern. Der Nutzer bereitet eine Überweisung vom Laptop vor, im TAN-Fenster kann er dann die TAN anfordern. Diese wird ihm als SMS auf das Smartphone geschickt. Dort liest er den sechsstelligen Code ab und gibt ihn auf dem Computer ein. Die Transaktion kann dann abgeschickt werden.

AES-Verschlüsselung

Die Verschlüsselung nach Advanced Encryption Standard (AES) ist die bisher sicherste Form der Datenverschlüsselung. Es handelt sich dabei um ein Verschlüsselungsverfahren, das aus einem Klartext bestimmter Länge einen hieroglyphen-ähnlichen Chiffretext erstellt. AES ist eine Blockchiffre und verwendet eine Blockgröße von 128 Bit. Die Transformation von Klar- zu Chiffretext wird mit einem Schlüssel abgesichert. Der Schlüssel hat eine Länge von 128, 192 oder 256 Bit. Bei Eingabe des gleichen Schlüssels wird die Transformation wieder rückgängig gemacht und der Klartext erscheint in leserlicher Form. Wird der gleiche Schlüssel zum Ver- und Entschlüsseln benutzt, wird in der Fachsprache von einer symmetrischen Verschlüsselung gesprochen. Die asymmetrische Verschlüsselung wiederum nutzt zwei unterschiedliche Schlüssel. Dieses Verfahren wird auch Public-Key-Verschlüsselung genannt. Anhand eines öffentlichen Schlüssels kann jeder Informationen für eine spezielle Person verschlüsseln. Entschlüsselt und gelesen werden können diese Informationen aber nur von der Person, an die sie gerichtet sind. Diese Person verfügt über einen separaten, nicht-öffentlichen Schlüssel.

Wie die AES-Verschlüsselung bei Outbank Nutzen findet, könnt ihr in Kapitel drei nachlesen.

Key-Logger

Bei einem Key-Logger handelt es sich um eine Software, die alle Eingaben in eine Computertastatur aufzeichnen. Key-Logger-Viren werden oftmals beim Besuch einer infizierten Webseite unbemerkt im Hintergrund heruntergeladen und protokollieren ab dem Zeitpunkt alle Aktivitäten eines Touchpads oder einer externen Tastatur. Key-Logger werden meist verbreitet, um an Passwörter wichtiger Accountzugänge zu gelangen.

Key Derivation Function

Outbank verwendet PBKDF2 - näheres unter https://de.m.wikipedia.org/wiki/PBKDF2

Kompromittierung

Kompromittierung im technologischen Sinn bedeutet, die mögliche Einsicht oder Manipulierung von Daten.

MD5 Hashes

Der MD5 Hash wurde lange Zeit verwendet, um Passwörter in eine definierte Zeichenkette zu konvertieren. Dadurch müssen nicht die Original-Passwörter übertragen und gespeichert werden. Die Konvertierung funktioniert folgendermaßen: Sätze, egal welcher Länge, werden in eine 32 Zeichen lange Kette verwandelt. Wird nur ein Buchstabe im Text abgeändert, entsteht eine komplett andere Zeichenkette. Damit wird der Vergleich von Daten erleichtert. Nur wenn die Hashes zweier Datenpakete übereinstimmen, ist die Integrität der Daten bestätigt. Mittlerweile ist diese Methode nicht mehr sicher genug um Passwörter damit sicher zu speichern. Outbank nutzt deshalb PBKDF2.

Man-In-The-Middle-Attacke

Outbank-Nutzer sind gegen MITM-Attacken mehrfach geschützt. Wie, wird in Kapitel zwei näher erläutert.

Phishing-Mails

Phishing-Mails sind auf Zugangsdaten aus. Sie tarnen sich meist mit einem bekannten Absender, wie etwa großen Banken, Bezahlsystemen, Versandhäusern, Logistikdienstleistern oder Packstationen und lotsen den Empfänger auf eine manipulierte Webseite, die dem Layout des Absender-Unternehmens gleicht. Der Nutzer wird daraufhin beispielsweise aufgefordert sich einzuloggen, ausstehende Beträge zu bezahlen oder sich Gutscheine überweisen zu lassen. Diese Webseiten zeichnen die Login- und Passworteingaben auf, sodass der Hacker die Zugangsdaten zu seinem eigenen Vorteil nutzen kann.

Sicherheitszertifikat

Ein Sicherheitszertifikat wird von sog. Certificate Authorities ausgestellt. Dazu gehören z.B. Comodo, VeriSign oder Symantec. Diese Zertifikate bestätigen, dass die Kommunikation mit der, im Zertifikat angegeben Person/Firma, stattfindet.

Spam-Mail

Der Begriff Spam steht für unerwünschte, oftmals mit Viren infizierte E-Mails. Jeder vertrauenswürdige E-Mailanbieter hat heutzutage einen Spam-Ordner integriert. Anhand intelligenter Algorithmen werden auffällige E-Mails aussortiert und automatisch in dem Spam-Ordner abgelegt. Der Nutzer hat dann die freie Wahl, welche Mails er öffnen oder löschen möchte.

TAN-Verfahren

Tan/iTAN
Die TAN-Liste ist die Urversion der TAN-Verfahren. Als gedruckte Liste enthält sie eine bestimmte Anzahl an TAN-Codes. Sobald die Liste aufgebraucht ist, erhält der Nutzer eine neue Liste. Dieses Verfahren ist nicht mehr im Einsatz. Das iTAN-Verfahren enthält für jede TAN eine zusätzliche Nummerierung. Die Bank fordert für eine Transaktion dann eine vorgegebene Nummer aus der Liste an. Dieses Verfahren ist noch im Einsatz.

mobile TAN (SMS-TAN)
Im mobileTAN-Verfahren wird die TAN von der Bank via SMS an eine hinterlegte Mobilrufnummer des Kunden gesendet.

optisches chipTAN-Verfahren
Für das chipTAN-Verfahren erhalten Nutzer einen TAN-Generator von ihrer Bank. In diesen Generator wird die Bankkarte eingesteckt. Bevor eine Überweisung ausgeführt wird, erscheint auf dem Bildschirm (Computer oder Smartphone) fünf flackernde Balken. Der Nutzer muss den Generator daraufhin an den vorgegebenen Bereich des Flickercodes halten. Dadurch wird die Erzeugung der TAN gestartet. Bei erfolgreicher Erzeugung erscheint die TAN im Fenster des Generators. Der Nutzer muss diese TAN danach wiederum im Überweisungsfenster eingeben.

manuelles chipTAN-Verfahren
Im manuellen chipTAN-Verfahren haben Nutzer ebenfalls den TAN-Generator mit Karteneinschub zur Hand. Bevor eine Transaktion angestoßen wird, erscheint auf dem Computerbildschirm ein Startcode. Dieser Code muss im TAN-Generator eingegeben werden. Anschließend gibt der Nutzer die Empfängerkontonummer und den Überweisungsbetrag ein. Aus diesen Informationen wird schlussendlich die TAN generiert, die der Nutzer in das TAN-Fenster der Überweisung eingibt.

photoTAN
Das photoTAN-Verfahren wird nur über ein Endgerät abgewickelt. Die Daten der jeweiligen Transaktion werden als bunte Pixel-Grafik angezeigt. Zur Entschlüsselung und Generierung der TAN muss der Nutzer eine App der Bank oder einen Photo-TAN Leser nutzen. Diese TAN muss dann im Überweisungsformular an entsprechender Stelle eingegeben werden.

pushTAN
Auch für das pushTAN-Verfahren wird eine separate App benötigt. Bevor die Transaktion freigegeben werden kann, erhält der Nutzer eine Benachrichtigung in der pushTAN-App, muss die darin enthaltenen Informationen verifizieren, und sobald er sie bestätigt, wird die TAN generiert. Die TAN muss im TAN-Feld der Überweisung eingetragen werden.

Zero-Knowledge-Prinzip

Der Begriff Zero Knowledge wurde von Edward Snowden geprägt. Er definiert das Zero-Knowledge-Prinzip als Maßnahme, die es weder dem Daten verarbeitenden Unternehmen, Datentransfer- noch Cloudspeicher-Anbietern möglich ist, persönliche Nutzerdaten einzusehen. Ermöglicht wird dies indem die Daten auf dem Endgerät des Nutzers nach höchstem Standard verschlüsselt werden und erst dann das Gerät in Richtung Cloudspeicher verlassen. Die Daten können dadurch von keinem der beteiligten Unternehmen eingesehen werden.

Outbank wendet das Zero-Knowledge-Prinzip an, um höchste Datensicherheit zu gewährleisten.