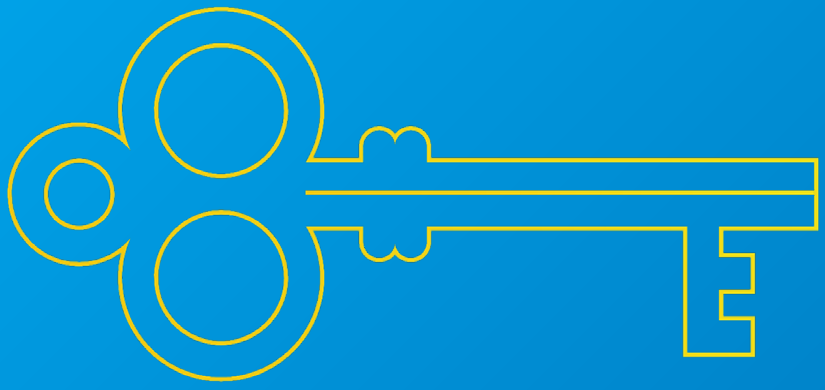
Outbank



Von Zertifikaten und Verschlüsselungen

Ein Guide zu sicherem Online und Mobile Banking

Inhalt

1. Executive Summary

Mobile Banking ist bequem, schnell, effizient und von überall aus möglich. Trotz all der Einfachheit häufen sich aber Bedenken, ob Banking Apps tatsächlich sicher sind. Laut einem Test der Stiftung Warentest im Herbst 2018 ist Mobile Banking zwar genauso sicher wie Online Banking – gleichzeitig hält jedoch mehr als die Hälfte der Deutschen das Online Banking für unsicher, wie eine Umfrage der Gesellschaft für Konsumforschung GfK im selben Jahr herausfand. Die Ungewissheit und Angst vor Datenpannen und Sicherheitslücken ist groß. Die gefühlte Unsicherheit wird dadurch verstärkt, dass immer noch wenig Aufklärung darüber stattfindet, welche Möglichkeiten für den Schutz der persönlichen Daten existieren.

Tatsächlich gibt es zahlreiche Sicherheitsmechanismen und Methoden, die das Banking auf dem Smartphone sicher machen und umfassend schützen. Wer sich um die Integrität seiner Daten sorgt, kann beispielsweise nach Anbietern Ausschau halten, die auf externe Datenspeicherung verzichten und die Daten direkt auf dem Smartphone verschlüsselt speichern. Wer Bedenken hat, dass Transaktionen abgefangen und umgeleitet werden könnten, kann sich an Banking-Apps halten, die Wert auf eine kontinuierliche Überprüfung der Sicherheitszertifikate der Banken legen. Wer Sorge hat, dass Unbefugte über das Smartphone Überweisungen tätigen könnten (z.B. im Fall eines Telefonverlustes oder -diebstahls), sollte sich einen Anbieter aussuchen, der auf lokale Verschlüsselung der Daten achtet und besonders hohe Sicherheitsmaßnahmen bei Passwörtern anwendet.

Dieses Whitepaper zeigt auf, welche Maßnahmen Outbank zum Schutz der Privatsphäre seiner Nutzer unternimmt. Es stellt diese Technologien detailliert vor und erläutert, wie sie potenziellen Gefahren vorbeugen oder diese verhindern. Ein Glossar zum Thema Sicherheit am Ende des Whitepapers dient zum besseren Verständnis der Sicherheitsarchitektur im Banking und erklärt häufige Angriffsmethoden. Zudem soll es den interessierten Mobile Banker unterstützen, eine wirklich sichere Applikation zu finden. Wer Banking-Anbieter auf diese Begriffe untersucht, ist auf der sicheren (Banking-) Seite.

2. Wie steht Outbank zur Banking-Sicherheit?

Die Finanzlage entscheidet darüber, wie sich der eigene Alltag gestalten lässt. Geld erlaubt die monatliche Miete zu begleichen, das tägliche Mittagessen zu bezahlen oder auch eine Reise zu unternehmen. Deshalb sind alle Daten rund um Geld und Finanzen nicht nur sehr persönlich, sondern auch besonders sensibel. Diese Daten sollen nur die Menschen sehen, welchen man absolutes Vertrauen schenkt.

Genau deshalb unterstützt Outbank den Ansatz der absoluten Datensicherheit. Outbank verschlüsselt, speichert und sichert die sensiblen Daten des Nutzers mit modernsten Verschlüsselungsstandards auf dem persönlichen Gerät des Nutzers. Um höchstmögliche Sicherheit auf dem Endgerät und während der Kommunikation mit Banken zu schaffen, hat Outbank folgende Sicherheitsmaßnahmen implementiert:

- **Lokale Datenspeicherung**

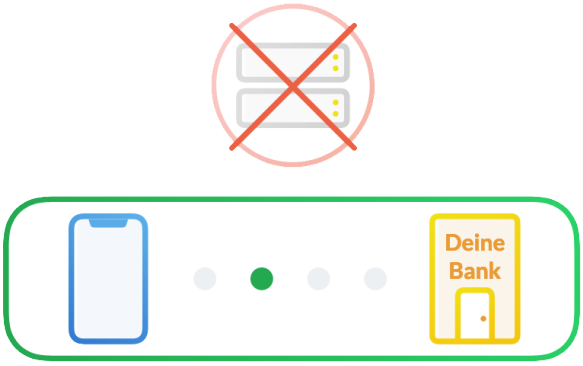
Outbank speichert alle Finanzdaten verschlüsselt auf dem Endgerät des Nutzers. Die Daten sind somit wirklich nur vom Nutzer einsehbar – weder von Outbank noch anderen Drittparteien. Das dahinterstehende Verfahren ist das Zero-Knowledge-Prinzip. Auch große Unternehmen wie Apple stellen aktuell immer mehr auf absolute Datensicherheit durch Zero Knowledge um und speichern Nutzerdaten nur noch auf deren Endgeräten, ohne selbst Zugriff darauf zu haben.

- **Moderne 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 unlesbar. Natürlich gibt es starke Unterschiede in der Schwierigkeitsstufe dieser Kombinationen. Outbank nutzt zur Verschlüsselung der sensiblen Finanzdaten den weltweit sichersten Standard: die symmetrische AES-Verschlüsselung. Diese Verschlüsselung wird auch zur Sicherung von Regierungsdokumenten der höchsten Klassifizierungsstufe genutzt. Um die Daten zu entschlüsseln und damit für den Menschen wieder 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-Passworts hat somit Zugang zum verschlüsselten Inhalt.

- **Direkte Bank-Device-Kommunikation**

Jegliche Kommunikation von der Bank und der Outbank App findet direkt zwischen Finanzinstitut und Endgerät statt.



Wie im Fall der lokalen Datenspeicherung sind auch hier keine Server zwischengeschaltet. Bei anderen Anbietern übernehmen häufig Proxy-Server die Kommunikation mit der Bank des Nutzers. Dazu müssen sie die Zugangsdaten des Nutzers in unverschlüsselter Form kennen. Die Server wissen somit nicht nur über die Zugangsdaten all ihrer Nutzer Bescheid, sondern auch über alle Finanzdaten, die zum Nutzer übermittelt werden – ein sehr lohnendes Ziel für Angreifer. Outbank eliminiert diese Gefahr vollständig, da die App direkt mit der Bank kommuniziert und keine Server zwischengeschaltet sind.

- **Sichere Bankzertifikate**

Jede Bank verfügt über ein Sicherheitszertifikat, das sogenannte TLS- bzw. SSL-Zertifikat. Damit bescheinigt das Kreditinstitut, dass die Verbindung zu ihren Servern nicht kompromittiert und damit vertrauenswürdig ist. Die meisten Banking-App-Anbieter überprüfen dieses Zertifikat in der Regel nicht explizit, da sie der Verantwortung dafür dem Betriebssystemhersteller überlassen. Outbank hingegen überprüft bei jeder Verbindung vor dem Verbindungsaufbau, ob das Zertifikat gültig ist. Dieser Prozess heißt Certificate Pinning. Zusätzlich prüft Outbank automatisiert die Sicherheit aller verwendeten Server der Anbieter mehrmals stündlich von verschiedenen Orten (unterschiedliche Autonome Systeme). Sobald eine Unregelmäßigkeit auftritt, bricht Outbank die Verbindung zur Bank sofort ab. Im Falle eines Cyber-Angriffs auf die Kommunikation mit der Bank findet daher weder eine Verbindung noch Kommunikation zwischen App und Bank statt. Outbank ist aktuell eine der wenigen Banking-Apps, die diese erhöhte Sicherheit anbieten.

- **Geschützte Datensynchronisierung**

Eine weitere Besonderheit der Outbank App ist die geschützte Synchronisierung der Daten auf allen Endgeräten beim Secure Sync. Dafür nutzt Outbank ebenfalls die AES-Verschlüsselung. Vor dem Versand werden die Daten zunächst verschlüsselt und anonymisiert – und erst dann als unlesbare Kryptogramme über einen AWS-Server in Deutschland geschickt. Der Weg über den Server ist notwendig, um die Daten auf allen Endgeräten zu synchronisieren. Alle Informationen, die sich auf dem Server befinden, sind mit dem

individuellen Master-Passwort des Nutzers verschlüsselt abgelegt. Sie können somit nicht eingesehen werden.

Zusammengefasst schützt Outbank die sensiblen Nutzerdaten, indem alle Daten auf dem Endgerät des Nutzers nach höchsten Sicherheitsstandards verschlüsselt sind. Selbst wenn ein Nutzer die Outbank Infrastruktur zur Datensynchronisierung nutzt, sind die Daten sicher, da sie vor dem Versand verschlüsselt und erst dann an den Server geschickt werden. Zudem sichert Outbank die Kommunikation zwischen App und Bank mit einer kontinuierlichen Überprüfung des Zertifikats des Kreditinstituts. Wie diese Sicherheitstechnologien konkret die Sorgen der Nutzer lösen und Cyber-Bedrohungen abwehren, zeigt Kapitel vier.

3. Der gläserne Bürger – auch im Mobile Banking?

Wenn ich meine Daten mit einer Banking-App verwalte, weiß das Unternehmen dann, wenn ich ein Minus auf dem Konto habe? Berichtet es das sogar? Muss ich Angst haben, dass meine Daten an Versicherungen und Finanzanbieter verkauft werden, die mich dann mit Angeboten bedrängen? Und muss Outbank nicht über meine Finanzsituation Bescheid wissen, um meine Verträge kategorisieren zu können?

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 Endgerät des Nutzers gespeichert, wo sie einzig und allein vom Nutzer per Eingabe des Master-Passworts eingesehen werden können.

Nein, es werden keine Finanzdaten oder 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.

Nein, auch bei Funktionen wie der Vertragserkennung erhält Outbank keinen Einblick in die Finanzdaten des Nutzers. Dafür kommen Algorithmen zum Einsatz, die ausschließlich auf dem Gerät des Nutzers ausgeführt werden.

4. Wie lassen sich mit Outbank Banking-Gefahren überwinden?

Seit 2001 beobachtet Outbank den Mobile-Banking-Markt und entwickelt die App von Kategorisierung bis Touch ID je nach Kundenwunsch und Neuerungen in der Branche weiter. Gleichzeitig verfolgt Outbank, welche Gefahrenpotenziale im Mobile Banking bestehen und wie diese die Sicherheitsbedenken unter den Nutzern steigern. Auf diese Gefahrenpotenziale antwortet Outbank mit Sicherheitstechnologien, die die Outbank Entwickler über mehrere Jahre und mit viel Erfahrung erstellt haben.

- **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 auf Servern. Der Finder des Smartphones 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. Ist

der Finder oder Dieb im Besitz des Smartphones, kann er die App weder bedienen noch Finanzdaten einsehen. Er müsste dafür zusätzlich das Passwort knacken. Doch das ist, wie im nächsten Schritt beschrieben, in der Outbank App praktisch unmöglich.

- **Gefahr #2: Passwortdiebstahl**

Wer versucht, das Passwort eines Outbank Nutzers zu knacken, wird sich daran die Zähne ausbeißen. Der Betrüger müsste dafür ein höchst komplexes Verschlüsselungssystem aufdecken.

Da Outbank keine Nutzerdaten und somit auch keine Passwörter zentral speichert, gibt es auch keine Server-Datenbanken, die geknackt werden könnten. Risiken durch Angriffe auf Passwort-Datenbanken fallen somit von vornherein schon einmal weg. Mittlerweile können schnelle Computer bereits in

wenigen Sekunden so viele Zahlen- und Zeichenkombinationen berechnen, dass selbst komplizierteste Passwörter in kürzester Zeit geknackt werden können. Auch hier schützt Outbank jeden Nutzer – unabhängig davon, wie schwer oder einfach er sein Master-Passwort wählt. Jedes einzelne Master-Passwort wird dafür in einen neuen, kryptischen Schlüssel einer festen Länge umgewandelt und somit unleserlich verändert. Diese Umwandlung erfolgt über die Schlüsselableitungsfunktion Key Derivation Function PBKDF2.

Früher kamen dafür auch Hashes wie MD5 Hashes zum Einsatz; inzwischen können schnelle Computersysteme diese aber ebenfalls mühelos knacken. Die Key Derivation Function PBKDF2 ist eine der sichersten Methoden, um kryptographische Schlüssel aus Passwörtern zu erzeugen. Die Berechnung dieses Schlüssels kostet viel Zeit und erhöht den Aufwand immens, den ein Angreifer für das Erraten des Passworts bspw. mittels Brute Force aufbringen muss.

- **Gefahr #3: Banken-Hack**

In den letzten Jahren häufen sich Nachrichten zu Cyber-Angriffen auf Bankinstitute wie die britische Tesco-Bank, die russische Central Bank oder die Bangladesh Central Bank. Oftmals ist dabei auch die Rede von Man-in-the-Middle-Attacken. Ein Angreifer schaltet sich dabei zwischen Nutzer und Bank und fängt somit die Datenströme ab.

Natürlich kann Outbank nicht den Angriff auf eine Bank verhindern. Im Ernstfall sind die Outbank Nutzer der jeweiligen Bank jedoch geschützt. Wurde das Sicherheitszertifikat der Bank kompromittiert oder manipuliert, blockiert Outbank den Zugang zur Bank. Das verhindert, dass die Nutzer in einem ungesicherten Bankenumfeld Transaktionen tätigen. Dazu überprüft Outbank im 15-Minuten-Takt, ob die Sicherheitszertifikate einer Bank unversehrt sind. Dieses Sicherheitsverfahren heißt auch aktives Certificate Pinning.

- **Gefahr #4: Smartphone-Hack**

Neben Banken haben Angreifer auch Smartphones zum Ziel. Dafür nutzen sie Sicherheitslücken auf den Geräten aus, schleusen sich über infizierte Spam-Mails ein oder fälschen WiFi-Verbindungen. Darüber manipulieren sie dann häufig die TAN-Generator-App oder fangen smsTAN ab – und können dadurch beispielsweise bei einer Transaktion den Überweisungsempfänger ändern.

Outbank-Nutzer sind auch in dem Fall eines Smartphone-Hacks oder Man-in-the-Middle-Angriffs auf das Gerät geschützt. Grund dafür ist abermals Certificate Pinning: Ein Angreifer kann zwar weiterhin bspw. die smsTAN abfangen, er kann jedoch keine Empfängerdaten oder Überweisungsbeträge ändern. Wenn er gefälschte Daten für die Transaktion an Outbank senden möchte, erkennt Outbank die Manipulation anhand des kompromittierten SSL-Zertifikats – und bricht sofort die Verbindung ab.

5. Wie kann ich mich als Nutzer allgemein besser im Netz schützen?

Im Netz ist Sicherheit immer ein zweischneidiges Schwert, denn: „Sicherheit ist nur so sicher, wie sein schwächstes Glied." Während Outbank alle notwendigen Schritte unternimmt, um seinen Nutzern nahezu 100 %ige Sicherheit zu gewährleisten, stehen auch die Nutzer selbst in der Verantwortung. An dieser Stelle deshalb einige Tipps, wie jeder selbst zu noch mehr Sicherheit im Banking beitragen kann:

- **Links und Anhänge von E-Mails prüfen**

Häufig schleusen sich Viren durch infizierte E-Mail-Anhänge oder -Links auf den PC oder das Smartphone. Daher sollten Nutzer keine Anhänge öffnen, deren Absender sie nicht kennen.

Spoofing Mails sind mittlerweile stark ausgereift. Sie passen sich an den Nutzer an und tarnen sich mit einem bekannten Namen oder einer Institution, mit der der Nutzer häufig in Kontakt steht. Wer sich unsicher ist, kann eine kurze Google-Suche mit der Betreffzeile der E-Mail durchführen. Sollte es sich um eine infizierte Spam-Mail handeln, weisen meist die ersten Suchergebnisse bereits darauf hin.

Auf ähnliche Weise versuchen Phishing-Mails, den Nutzer auf infizierte Webseiten zu locken. Häufig mit dem Namen eines bekannten Unternehmens getarnt, enthalten Phishing-Mails einen infizierten Link. Teilweise geben Angreifer als Absender dieser E-Mails auch den Namen einer Person im eigenen Unternehmen an, um noch mehr Vertrauen zu erwecken (CEO Fraud). Bestand in den letzten zwei bis drei Wochen kein Kontakt zum jeweiligen Unternehmen oder der Person, sollten diese E-Mails am besten direkt gelöscht werden. Wer sich versichern möchte und die E-Mail öffnet, sollte nicht direkt auf den enthaltenen Link klicken. Per Mouse-Over lässt sich üblicherweise die Linkadresse anzeigen. Führt diese Adresse nicht direkt zur Webseite des Unternehmens, handelt es sich vermutlich um eine Umleitung auf eine infizierte Webseite.

- **Offizielle App Stores nutzen**

Wer Apps nicht aus den offiziellen App Stores von Google oder Apple herunterlädt, läuft Gefahr, sein Gerät mit Viren zu infizieren. Gerade bei sehr beliebten oder heiß erwarteten Apps besteht die Gefahr, dass vereinzelt Webseiten Downloads von diesen Versionen anbieten. Da diese Webseiten aber nicht den Sicherheitsbestimmungen der offiziellen App Stores unterliegen, sind diese Apps häufig mit Trojanern infiziert.

Nutzer sollten deshalb Apps ausschließlich aus dem Apple App Store oder Google Play Store herunterladen. Alle Apps, die dort gelistet sind, werden von den jeweiligen Plattformen zuvor geprüft. Sie können deshalb in der Regel bedenkenlos heruntergeladen werden.

- **Authentifizierung mit 2 Geräten durchführen**

Im Herbst 2016 sorgte eine Sicherheitslücke im photoTAN-Verfahren deutschlandweit für großes Aufsehen. Grund der Sicherheitslücke war die TAN-Authentifizierung über nur ein Endgerät. Üblicherweise kommen beim sicheren TAN-Verfahren zwei, voneinander unabhängige Geräte zum Einsatz für die Zwei-Faktor-Authentisierung. Dadurch kann nur derjenige den Vorgang durchführen, der im Besitz beider Geräte ist. Im photoTAN-Verfahren wird die TAN jedoch nicht auf einem zweiten Gerät generiert. Angreifer haben somit leichtes Spiel: Sie nisten sich über ein Schlupfloch im Smartphone ein und hacken die TAN-Generator-App. So können sie die TAN-Generierung manipulieren, aufzeichnen, abfangen oder die Überweisung so abändern, dass das Geld auf ein anderes Konto geleitet wird.

Aus diesem Grund sollten Nutzer stets zwei verschiedene Geräte für TAN-Verfahren verwenden. Bei einer Überweisung macht es beispielsweise Sinn, die mobile TAN für die Transaktion auf dem Smartphone zu empfangen und den Vorgang selbst am Mac oder PC durchzuführen. Dadurch ist sowohl die Generierung als auch Anwendung einer TAN sicher.

- **Webseiten ohne Schloss vermeiden**

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

- **Auf Banking in öffentlichen Netzen verzichten**

Im Gegensatz zum heimischen Privat-WLAN sind öffentliche WLAN-Verbindungen in den wenigsten Fällen verschlüsselt. Wer sich hier einloggt, läuft Gefahr, dass seine Daten abgefangen oder manipuliert werden. Teilweise richten Kriminelle sogar eigene “Free Wifi”-Verbindungen ein, nur um anschließend die verbundenen Geräte zu hacken und die Daten mitzulesen. In einem öffentlichen, freien Netz seine Bankgeschäfte zu erledigen, ist deshalb schon beinahe fahrlässig.

Im öffentlichen WLAN sollten Nutzer deshalb keine persönlichen oder vertraulichen Daten abrufen oder gar Mobile Banking nutzen. Wer häufig fremde Rechner zum Surfen oder für das Banking gebraucht, sollte anschließend immer den Cache des Browsers löschen. In diesem Zwischenspeicher legen Browser die Daten der letzten Verbindungen ab. Werden diese Informationen nicht gelöscht, könnten Kriminelle diese später auslesen und missbrauchen. Im besten Fall sollten Nutzer auch hier ganz darauf verzichten, fremde Rechner für ihr Banking zu nutzen.

6. Glossar

AES-Verschlüsselung

Die Verschlüsselung nach Advanced Encryption Standard (AES) ist die bisher sicherste Form der Datenverschlüsselung. Dieses Verschlüsselungsverfahren erstellt aus einem Klartext wie dem **Master-Passwort** einen hieroglyphen-ähnlichen Chiffretext einer bestimmten Länge (128 Bit bzw. eine Zahl mit 39 Stellen). Die Umwandlung von Klar- zu Chiffretext wird mit einem weiteren Schlüssel abgesichert. Dieser besitzt eine Länge von 128, 192 oder 256 Bit. Das entspricht einer Zahl mit jeweils 39, 58 oder 78 Stellen. Bei Eingabe des Schlüssels wird die Transformation wieder rückgängig gemacht und der Klartext (das Master-Passwort) leserlich. Ist der Schlüssel zum Ver- und Entschlüsseln identisch, liegt eine symmetrische Verschlüsselung vor.

Autonomes System

Als Autonomes System (AS) wird ein Verbund von Netzwerken bezeichnet, die miteinander über ein Protokoll kommunizieren. Jeder große Internetdienstanbieter wie beispielsweise Telekom oder Vodafone besitzt ein eigenes AS. Alle AS sind untereinander verbunden und bilden so gemeinsam das Internet. Outbank nutzt beim **Certificate Pinning** unterschiedliche AS, um die **Sicherheitszertifikate** der Banken zu überprüfen. Sollten die Zertifikate einer Bank in den einzelnen AS unterschiedlich sein, deutet das auf eine Manipulation hin. Da Outbank die Zertifikate in unterschiedlichen AS abfragt, würde es diese Manipulation sofort erkennen und kann seine Nutzer somit vor dieser Gefahr schützen.

Brute Force

Generell werden bei der Brute-Force-Methode in der Informatik alle potenziellen Lösungen ausprobiert, bis die richtige gefunden ist. Kriminelle wenden dieses Vorgehen beispielsweise an, wenn sie Passwörter erraten möchten. In Outbank sind Nutzer davor geschützt, da aus den **Master-Passwörtern** kryptographische Schlüssel über die **Key Derivation Function PBKDF2** erzeugt werden.

CEO Fraud

Der CEO Fraud kommt vielfach bei **Phishing-Mails** zum Einsatz. Diese Betrugsmasche zielt darauf ab, Nutzer zu Geldüberweisungen zu bewegen. Angreifer fälschen dafür E-Mails, die sie beispielsweise im Namen von Geschäftsführern (CEO) oder Kollegen aus dem Unternehmen der Empfänger versenden. Darin fordern sie den Nutzer zum Überweisen von Geldbeträgen auf.

Certificate Pinning

Wie jede vertrauenswürdige Webseite besitzt auch jede Bank ein **Sicherheitszertifikat**. Damit bestätigt sie ihre Identität und verspricht eine unmanipulierte Bankverbindung. Bei einem Cyber-Angriff auf die Bank beispielsweise durch **Man in the Middle** ist das Sicherheitszertifikat **kompromittiert** und damit nicht mehr vertrauenswürdig. Der Angreifer könnte so die Verbindung zwischen Bank und Nutzer manipulieren. Outbank schützt seine Nutzer davor, indem es alle 15 Minuten das Sicherheitszertifikat mittels Certificate Pinning überprüft. Stellt Outbank fest, dass das Zertifikat nicht gültig ist, wird die Verbindung im Vorfeld blockiert.

Ende-zu-Ende-Verschlüsselung

Eine Ende-zu-Ende-Verschlüsselung stellt sicher, dass Daten während ihrer Übertragung ständig verschlüsselt und somit geschützt sind. In Outbank kommt diese Verschlüsselungsart zusammen mit dem **Zero-Knowledge-Prinzip** bei der sicheren Datenübertragung (**Secure Sync**) zum Einsatz. Hier werden die Daten zunächst auf dem Endgerät des Nutzers nach höchstem Standard (**AES-Verschlüsselung**) verschlüsselt. Erst dann verlassen sie das Gerät in Richtung Cloud-Speicher. Die Daten können dadurch von keinem der beteiligten Unternehmen zu keiner Zeit eingesehen werden. Nur der Nutzer kann die Daten mit seinem **Master-Passwort** entschlüsseln.

Key Derivation Function PBKDF2

Um Passwörter in einen kryptischen Schlüssel zu verwandeln, werden Key Derivation Functions bzw. Schlüsselableitungsfunktionen angewandt. Dabei wird eine bestimmte Funktion mehrmals hintereinander auf das selbe Passwort angewandt. Diese Iterationen stellen sicher, dass nicht mehr auf das ursprüngliche Passwort geschlossen werden kann. Das macht es Angreifern sehr schwer, Passwörter bspw. mittels der **Brute-Force-Methode** herauszufinden. Outbank verwendet den Standard PBKDF2: Password-Based Key Derivation Function 2.

Kompromittierung

Ist ein System kompromittiert, ist die Sicherheit der Daten nicht mehr gewährleistet. Angreifer könnten unberechtigt eindringen, Daten einsehen oder manipulieren. Häufig kompromittieren Angreifer die Verbindung zwischen Bank und Nutzer, um Daten abzufangen (**Man-in-the-Middle-Angriff**). Verfahren wie das **Certificate Pinning** schützen Nutzer in Outbank vor den Folgen manipulierter Verbindungen.

MD5 Hashes

Der Message-Digest Algorithm 5 (MD5) ist eine Funktion, der einen Text in eine 32 Zeichen lange Kette umwandelt – egal wie lang oder kurz der Text ist. Ändert sich nur ein Buchstabe im Text, entsteht eine komplett andere Zeichenkette. Nur wenn die Zeichenketten (Hashes) zweier Datenpakete übereinstimmen, ist die Unversehrtheit der Daten bestätigt. Durch dieses Vorgehen ist es einfacher, Daten zu vergleichen. Lange Zeit wurden MD5 Hashes verwendet, damit Passwörter nicht im Klartext übertragen oder gespeichert werden mussten. Mittlerweile können schnelle Computersysteme MD5 Hashes mühelos knacken. Deshalb ist diese Methode nicht mehr sicher genug, um damit kryptographische Schlüssel zu erzeugen. Outbank nutzt deshalb die **Key Derivation Function PBKDF2**.

Man In The Middle

Bei einer Man-in-the-Middle-Attacke (MITM) stellt sich ein Angreifer zwischen zwei Systeme, bspw. den Nutzer und seine Bank. Er kann damit den Datenaustausch zwischen den beiden abfangen, kontrollieren und manipulieren. Outbank Nutzer sind gegen MITM-Attacken mehrfach geschützt, beispielsweise durch kontinuierliches Überprüfen des Sicherheitszertifikats beim **Certificate Pinning**.

Master-Passwort

Das Master-Passwort ist ein vom Nutzer selbst vergebenes Passwort, das er bei der ersten Einrichtung von Outbank erstellt. Mit diesem Passwort entsperrt der Nutzer die Outbank App. Um die Daten nach einer Synchronisierung über **Secure Sync** wieder zu entschlüsseln, muss der Nutzer ebenfalls sein Master-Passwort eingeben. Dieses Passwort wird nicht gespeichert und kann deshalb nicht zurückgesetzt werden. Wer das Master-Passwort nicht kennt, dem bleibt die App verschlossen. Das Nicht-Speichern des Passworts erhöht die Sicherheit: Werden keine Passwörter gespeichert, können sie auch nicht gestohlen werden. Vergisst der Nutzer sein Passwort, sind alle in Outbank gespeicherten Daten verloren und er muss die App erneut einrichten.

Phishing-Mails

Phishing-Mails sind darauf aus, Zugangsdaten abzufangen. Sie tarnen sich meist mit einem bekannten Absender, wie etwa großen Banken, Bezahlsystemen, Versandhäusern, Logistikdienstleistern oder Packstationen. Dadurch lotsen sie den Nutzer auf eine manipulierte Webseite, die dem Layout des Absender-Unternehmens gleicht. Der Nutzer wird beispielsweise aufgefordert sich einzuloggen, um ausstehende Beträge zu bezahlen oder sich Gutscheine überweisen zu lassen. Die Webseite zeichnet die Login- und Passworteingaben des Nutzers auf. Der Angreifer kann die Zugangsdaten so zu seinem eigenen Vorteil nutzen. Bekannte Phishing-Methoden sind **CEO Fraud** und **Mail-Spoofing**.

Secure Sync

Der Secure Sync ist die sichere Datenübertragung in Outbank über mehrere Endgeräte. Verwendet ein Nutzer den Secure Sync, sind seine Daten automatisch auf mehreren Geräten auf dem selben Stand. Zahlreiche Sicherheitstechnologien schützen die Datenübertragung bspw. **AES-Verschlüsselung**, **Ende-zu-Ende-Verschlüsselung**, **Key Derivation Function PBKDF2** und **Certificate Pinning**. Vor dem Versand der Daten werden diese auf dem Gerät des Nutzers verschlüsselt. Weder Outbank noch der Cloud-Anbieter Amazon können die Daten vor, während oder nach der Übertragung einsehen. Die Daten bleiben während des gesamten Prozesses vollständig verschlüsselt. Erst wenn der Nutzer sein **Master-Passwort** eingibt, sind die Daten wieder lesbar. Aktuell ist die sichere Datenübertragung für iOS- und macOS-Geräte möglich.

Sicherheitszertifikat (SSL, TLS)

Ein Sicherheitszertifikat bescheinigt, ob eine Webseite Daten sicher und verschlüsselt überträgt. Gerade bei Webseiten, die persönliche und sensible Nutzerdaten übertragen, sind diese Zertifikate unumgänglich. Übertragen werden sie über das Protokoll Transport Layer Security (TLS), weshalb sie auch **TLS-Zertifikate** genannt werden. Früher wurden sie über das Protokoll Secure Sockets Layer (SSL) übermittelt und heißen dementsprechend **SSL-Zertifikate**. Ausgestellt werden die Zertifikate von Certificate Authorities wie Comodo, VeriSign oder Symantec. Diese überprüfen, ob der Antragsteller (z.B. der Betreiber einer Webseite oder eine Bank) auch berechtigt ist, für eine bestimmte Internetadresse ein Zertifikat zu erhalten. Je nach Sicherheitsstufe muss der Antragsteller dabei unterschiedliche komplexe Anforderungen erfüllen.

Spam-Mail

Der Begriff Spam steht für unerwünschte, oftmals mit Viren infizierte E-Mails. Jeder vertrauenswürdige E-Mail-Anbieter hat heutzutage einen Spam-Ordner integriert. Anhand intelligenter Algorithmen werden auffällige E-Mails aussortiert und automatisch im Spam-Ordner abgelegt. Der Nutzer kann dann entscheiden, ob er diese E-Mails öffnen oder löschen möchte.

Spoofing-Mail / Mail-Spoofing

Beim Mail-Spoofing täuschen Angreifer eine andere Identität vor. Dabei erscheint beispielsweise als Absender ein Name, der dem E-Mail-Empfänger bekannt ist. Die tatsächliche E-Mail-Adresse ist jedoch eine gefälschte. Wie andere **Phishing-Mails** ist auch eine Spoofing-Mail darauf aus, an

geheime Nutzerdaten zu gelangen oder den Nutzer zum Überweisen von Geldbeträgen zu bewegen.

TAN-Verfahren

Mit einer **Transaktionsnummer (TAN)** lassen sich im Mobile und Online Banking bestimmte Vorgänge wie Überweisungen freigeben. Um dieses Einmalkennwort zu erzeugen, kommen unterschiedliche Verfahren zum Einsatz.

Tan/iTAN
Die TAN-Liste ist die Urversion der TAN-Verfahren. Die gedruckte Liste enthält eine bestimmte Anzahl an TAN-Codes, die der Nutzer in beliebiger Reihenfolge verwenden kann. Ist die Liste aufgebraucht, erhält der Nutzer eine neue. Mittlerweile ist dieses Verfahren nicht mehr im Einsatz, da es zu unsicher ist. Die indizierte TAN-Liste (iTAN) enthält für jede TAN zusätzlich eine Nummerierung. Für eine Transaktion fordert die Bank eine bestimmte Nummer aus der Liste an. Dieses Verfahren wird im September 2019 aufgrund von Sicherheitsproblemen ebenfalls eingestellt.

SMS-TAN (mobileTAN, mTAN, smsTAN)
Im SMS-TAN-Verfahren wird die TAN von der Bank via SMS an eine hinterlegte Mobilrufnummer des Nutzers gesendet.

optisches chipTAN-Verfahren
Für das optische chipTAN-Verfahren erhält der Nutzer einen TAN-Generator seiner Bank. In diesen Generator steckt er seine Bankkarte. Bevor eine Überweisung ausgeführt wird, erscheinen auf dem Bildschirm (PC oder Smartphone) fünf flackernde Balken. Hält der Nutzer den Generator an den vorgegebenen Bereich des Flickercodes, wird die TAN erzeugt. Anschließend erscheint auf dem Display des Generators die benötigte TAN.

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 PC-Bildschirm ein Startcode. Diesen Code muss der Nutzer in den TAN-Generator eingeben. Anschließend gibt er die Empfängerkontonummer und den Überweisungsbetrag ein. Aus diesen Informationen wird schließlich die TAN generiert.

photoTAN
Das photoTAN-Verfahren wird über ein einzelnes Endgerät abgewickelt. Die Daten der jeweiligen Transaktion erscheinen als bunte Pixel-Grafik. Zur Entschlüsselung und Generierung der TAN nutzt der Nutzer eine App der Bank oder einen photoTAN-Leser. Wenn bei diesem Verfahren nur ein Gerät zum Einsatz kommt, gilt es als nicht sicher. In Outbank ist dieses Verfahren aktuell deshalb nur mit einem zusätzlichen Gerät möglich.

pushTAN
Beim pushTAN-Verfahren benötigt der Nutzer ebenfalls eine separate App. Bevor er die Transaktion freigeben kann, erhält er eine Benachrichtigung in der pushTAN-App. Nachdem er die darin enthaltenen Informationen verifiziert und bestätigt hat, wird die TAN generiert.

Zero-Knowledge-Prinzip

Der Begriff Zero Knowledge wurde von Edward Snowden geprägt. Das Zero-Knowledge-Prinzip soll sicherstellen, dass persönliche Daten auch beim Transfer über Cloud-Anbieter ständig geschützt sind. Die Daten werden deshalb verschlüsselt übertragen. So können weder das Daten verarbeitende Unternehmen noch der Datentransfer- oder Cloudspeicher-Anbieter persönliche Nutzerdaten einsehen. Outbank wendet Zero Knowledge in Verbindung mit **Ende-zu-Ende-Verschlüsselung** beim **Secure Sync** an.

Zwei-Faktor-Authentisierung / Zwei-Geräte-Authentisierung

Die Zwei-Faktor-Authentisierung (2FA) soll Nutzer vor digitalem Identitätsdiebstahl schützen. Dazu muss der Nutzer seine Identität über zwei, voneinander unabhängige Faktoren bestätigen. Das geschieht beispielsweise über ein Passwort und eine zusätzliche Information, die bei der Anmeldung via SMS verschickt wird. Angreifer können sich nur dann als Nutzer ausgeben, wenn sie Zugang zu beiden Faktoren haben – in diesem Fall Passwort und Mobiltelefon.

Im Zusammenhang mit TAN-Verfahren heißt dieses Vorgehen auch Zwei-Geräte-Authentisierung. Dabei wird jeweils ein Endgerät zur TAN-Generierung und eines für die TAN-Anwendung genutzt. Bei der **SMS-TAN** beispielsweise bereitet der Nutzer eine Überweisung am PC oder Mac vor und fordert im TAN-Fenster die TAN an. Diese wird ihm als SMS auf sein Smartphone geschickt. Den darin enthaltenen Code gibt er auf dem PC oder Mac ein und schickt dadurch den Auftrag für die Transaktion ab.