Dirk Fox

Social Engineering im Online-Banking und E-Commerce

Seit Jahren liefern sich die Anbieter von Online-Banking-Systemen und E-Commerce-Angeboten mit Angreifern ein Katz-und-Maus-Spiel, das den Eindruck erweckt, es gehe lediglich um technische Schutzmaßnahmen und clevere Umgehungstricks. Tatsächlich liegt die Ursache für die Erfolge der Angreifer tiefer – nämlich in der Art, wie Menschen Vertrauen schenken.

1 Einleitung

In wachsendem Umfang unterstützen heute Web-basierte Anwendungen auch Geschäftsprozesse, die Transaktionen von nicht vernachlässigbaren Werten ermöglichen – von Auktionsplattformen bis zum Online-Trading. In vielen Fällen haben dabei die beteiligten Geschäftspartner (Plattformanbieter und Kunde) keinen persönlichen Kontakt miteinander.

Die Nutzung von Web-basierten Anwendungen in diesen Geschäftsprozessen sorgt dabei für eine oft erhebliche Vereinfachung und Beschleunigung sowie eine spürbare Senkung der Transaktionskosten. Allerdings schafft sie auch zusätzliche, gänzlich neue Ansatzpunkte für Betrug, da nicht mehr nur die Systeme des Anbieters angegriffen werden können, sondern die vom Kunden genutzten IT-Systeme die ‚Angriffsfläche' vergrößern. Diese stehen zudem in der Regel nicht unter der Kontrolle des Anbieters und sind oft unzureichend geschützt. Durch das Fehlen eines persönlichen Kontakts zwischen Anbieter und Kunde entfallen zudem Kontrollmöglichkeiten, die im Betrugsfall eine Identifikation des Täters erleichtern können. Schließlich ist die Möglichkeit zur (Teil-) Automatisierung solcher Angriffe eine Verlockung für Online-Betrüger (‚schnelles Geld').

Viele dieser Web-basierten Anwendungen, die sich im weitesten Sinne unter den Sammelbegriffen ‚E-Commerce' und ‚Online-Banking' zusammenfassen lassen, werden daher seit einigen Jahren von mehr oder weniger erfolgreichen, gezielten Angriffen bedroht. Der Umgang mit diesen Angriffen ähnelt bis heute meist einem ‚Katz-und-Maus-Spiel': Wird ein konkreter Angriff bekannt, reagieren die Anbieter mehr oder weniger zügig mit mehr oder weniger geeigneten Gegenmaßnahmen – bis zum Bekanntwerden der nächsten erfolgreichen Angriffsmethode. Dabei ist allen Angriffen auf E-Commerce- und Online-Banking-Lösungen gemeinsam, dass sie – zumindest als ein Teilelement, zunehmend aber als primäre Komponente – Techniken verwenden, die unter dem Begriff ‚Social Engineering' zusammengefasst werden können, meist kombiniert mit Schadsoftware, die auf dem System des Kunden ‚installiert' wird.

Im Folgenden wird ein systematischer Zugang zur Erfassung der ‚erfolgs'-kritischen Ursachen solcher Social Engineering-Angriffe versucht und aufgezeigt, welche Maßnahmen zu deren Abwehr erforderlich sind – und wo deren Grenzen liegen.

Dirk Fox

Geschäftsführer der Secorvo Security Consulting GmbH und Herausgeber der DuD.

E-Mail: dirk.fox@secorvo.de

2 Was ist ‚Social Engineering'?

Unter ‚Social Engineering' werden Techniken zur Beeinflussung von Menschen verstanden, die insbesondere dafür eingesetzt werden, unberechtigt an Daten oder Informationen zu gelangen oder ein regelwidriges Verhalten zu bewirken. ‚Social Engineers' täuschen eine falsche Identität und einen falschen Kontext vor, versuchen ihre Opfer unter Druck zu setzen oder sie durch Charme für sich zu gewinnen [1]. Sie bedienen sich unterschiedlicher Kommunikationsmedien – Telefon, E-Mail –, scheuen aber meist den direkten persönlichen Kontakt, um das Entdeckungsrisiko gering zu halten.

Zentral für alle Arten von Angriffen durch Social Engineering ist, dass eine in der Regel dem Angegriffenen nicht persönlich bekannte Person versucht, das Vertrauen des Opfers zu gewinnen. Social Engineering nutzt dabei typische menschliche Verhaltensmuster, die im Zusammenhang mit der Entwicklung sozialen Vertrauens greifen. Zu diesen zählen insbesondere die folgenden [1, 2]:

- *Gemeinsamkeiten*: Ähnliche Erfahrungen, gemeinsame Erlebnisse oder gleiche Bekannte sorgen für einen Vertrauensvorschuss. Das gilt besonders für emotional positiv besetzte Gemeinsamkeiten wie gute Freunde, ein geliebtes Hobby oder eine glückliche Erinnerung.
- *Sympathie*: Einem sympathischen Menschen werden ungewöhnliche Wünsche eher erfüllt und eigenartige Begründungen eher geglaubt als einem unsympathischen. Sympathie kann

auch durch höfliche Formulierungen oder entgegenkommende Reaktionen geweckt werden.

- *Kontext*: Menschen schließen in definierten Umgebungen meist vom Kontext auf die Personen – Anwesende auf einer Party sind Freunde des Gastgebers, ein Fremder im Unternehmen mit Logo des IT-Dienstleisters auf dem Hemd ist ein berechtigter Administrator und eine Person mit Kittel und Reinigungsgerät gehört zum Putzpersonal.
- *Autoritäten*: Anordnungen von (vermeintlichen) Autoritätspersonen werden von den meisten Menschen über geltende Regeln gestellt – sogar, wenn die Regeln von eben diesen Autoritäten aufgestellt wurden. Menschen neigen dazu, die Behauptung eines Dritten, im Auftrag einer (gemeinsamen) Autorität zu handeln, eher für wahr zu halten – und sei es nur, weil sie die Sanktionierung eines ‚ungehorsamen' Verhaltens eher scheuen als die eines Regelverstoßes.
- *Verpflichtung*: Ist man jemandem einen Gefallen schuldig, steigt die Bereitschaft, bestehende Regeln zu überschreiten, um sich zu revanchieren.
- *Erfahrung*: Tritt nach einem riskanten oder ungewohnten, als möglicherweise riskant empfundenen Verhalten wiederholt keine negative Konsequenz ein, sinkt die Vermeidungshemmung. Der Effekt wird verstärkt, wenn man erfährt, dass auch andere (insbesondere als kompetenter oder erfahrener geltende oder hierarchisch ‚höher' stehende) Personen sich ebenso verhalten.

Aber auch wünschenswerte menschliche Eigenschaften wie Hilfsbereitschaft, Höflichkeit oder Freundlichkeit begünstigen Social Engineering-Angriffe: Viele Menschen geben Anrufern und Fremden in der Regel einen Vertrauensvorschuss, glauben das, was diese ihnen mitteilen, ohne nähere Überprüfung. Vor allem unter Zeitdruck und bei erhöhter Dringlichkeit eines wichtigen Vorgangs erscheint ‚unbürokratisches' Handeln gefragt – und etwaige Bedenken werden zurückgestellt.

Für einen Social Engineer kommt es daher darauf an, durch eine – mehr oder weniger glaubwürdige – ‚Legende' eine Ausnahmesituation vorzutäuschen, die ein Abweichen von den gewohnten Abläufen oder auch einen Regelverstoß rechtfertigt. Ist das Vertrauen einmal gewonnen, sind Betroffene sogar oft bereit, schier unglaubliche Legenden, die ihnen aufgetischt werden, bereitwillig zu glauben.

Und noch ein Faktor spielt Social Engineers in die Hände: die wachsende Komplexität von Prozessen erschwert es den Beteiligten, die Voraussetzungen für die Vertrauenswürdigkeit eines Prozessschrittes zu erkennen – und selbst einschätzen zu können, welches Vorgehen in einer mutmaßlichen Ausnahmesituation angemessen ist.

Social Engineering ist eine akute Bedrohung in modernen Gesellschaften, in denen durch die zunehmende Vernetzung über unterschiedliche Kommunikationsmedien nicht-persönliche, mehr oder minder anonyme Kontakte zur Regel werden.

3 Social Engineering in E-Commerce und Online-Banking

Methoden des Social Engineering erfordern die Kontaktaufnahme mit einem (potentiellen) Opfer. Beschränkt auf ‚klassische' Kommunikationsmittel wie das Telefon stellen Social Engineering-Angriffe meist eine lokal begrenzte Gefahr dar (man denke z. B. an den verbreiteten ‚Enkeltrick'), denn sie erfordern einerseits relativ genaue Recherchen über die (Lebens-) Umstände des Opfers, andererseits meist die physische Nähe (z. B. zur Geldübergabe) und bergen daher ein relativ hohes Entdeckungsrisiko, vor allem für Wiederholungstäter.

Im Internet hingegen skalieren Social Engineering-Angriffe durch die Verwendung von Massen-E-Mailings (Spam) und bergen zugleich geringere Risiken für den Angreifer. Als Legende wird hier in der Regel die Vorspiegelung eines ‚Ausnahmefalls' verwendet, der ein Abweichen vom üblichen Prozedere erforderlich macht, wie z. B. ein Funktionstest, eine Sicherheitsüberprüfung, ein Update oder eine erforderliche Neu-Registrierung. Zu den Internet-spezifischen Social Engineering-Angriffen zählen u. a.

- *Phishing-E-Mails* zur Abfrage von Identifikations- und Authentifkationsdaten (Login-IDs, Passworte, PINs, Kontodaten, TANs, Kreditkartennummern, …)
- *Spam-E-Mails mit Schadsoftware* enthaltenden Anhängen oder Links auf mit Schadsoftware versetzte Seiten zur Infektion eines Anwendersystems
- *Manipulation gut besuchter Webseiten* zur Installation von Schadsoftware auf Systemen zufälliger Besucher der Seite (‚drive by infection')
- *Verfälschung des Erscheinungsbilds von Webseiten* als ‚Man-in-the-Browser', um dem Nutzer einen abweichenden Vorgang vorzuspielen, der ihn zur Preisgabe von Transaktionsdaten bewegt

Dabei nutzen viele Angreifer die Grundelemente der Entwicklung sozialen Vertrauens auch bei Angriffen auf E-Commerce- und Online-Banking-Lösungen:

- *Gemeinsamkeiten*: Ganz wesentlich für die Glaubwürdigkeit der Legende, die der Angreifer auftischt, ist die verwendete Sprache. Wird sie nicht in der Muttersprache des Nutzers erzählt, sinkt die Wahrscheinlichkeit, dass dieser darauf hereinfällt, rapide. Aber auch ein Anknüpfen an aktuelle Vorkommnisse oder Nachrichten, die dem Nutzer bekannt sind, erhöht die Glaubwürdigkeit erheblich. Die Vortäuschung von Bedürftigkeit oder einem Notfall wird eher von Menschen geglaubt, die etwas Ähnliches bereits erleben mussten.
- *Sympathie*: Ein höflicher, hilfsbereiter Ton und Stil des Textes der E-Mail oder der Aufforderung auf einer manipulierten Webseite sorgt eher dafür, dass er gelesen und dem Inhalt geglaubt wird. Auch eine personalisierte Ansprache erhöht die Akzeptanz beim Empfänger.
- *Kontext*: Das ‚Look & Feel' (Aufbau, Layout, Logo, …) einer E-Mail oder einer manipulierten Webseite, ein falscher aber ähnlich lautender Domainname oder eine Bezugnahme auf eine frühere (authentische) Kontaktaufnahme („siehe unsere E-Mail vom ….") kann beim Nutzer den Eindruck erwecken, dass der Vorgang oder die Abfrage nicht ungewöhnlich ist – und die Wahrscheinlichkeit steigern, dass der Angriff nicht bemerkt wird. Wird eine Legende, die der Angreifer dem Benutzer auftischt, an aktuelle Ereignisse geknüpft und z. B. mit Hinweisen auf (echte) Nachrichten versehen, akzeptiert ein Nutzer auch eher ungewohnte Vorgänge. Auch fehlerfreie Rechtschreibung und Grammatik sind wichtig, da man das von einem professionellen Absender erwartet.
- *Autoritäten*: Phishing- oder Spam-E-Mails mit Schadsoftware, die sich als Nachricht einer als Autorität empfundenen Behörde (BND, Finanzamt, …) ausgeben, werden von vielen Empfängern spontan eher als glaubwürdig empfunden, selbst wenn

die jeweilige Behörde die betroffene E-Mail-Adresse gar nicht kennen kann.
- *Verpflichtung*: Wird vom Angreifer glaubhaft ein Gefallen vorgetäuscht (z. B. „Wir haben eine unrechtmäßige Abbuchung von Ihrem Konto gestoppt"), kann er anschließend leichter eine ‚Gegenleistung' einfordern („Bitte geben Sie im untenstehenden Feld die TAN Nr. 36 ein."). Auch durch explizite Sicherheitshinweise („Geben Sie niemals Ihre PIN oder TAN am Telefon preis" o. ä.), die signalisieren, dass man sich um die Sicherheit des Nutzers sorgt, kann die Glaubwürdigkeit wirksam gesteigert werden.

Diese Angriffsformen können mit ‚klassischen' Social Engineering-Methoden kombiniert werden, wie beispielsweise Anrufe bei Nutzern (Kunden), bei denen sich der Social Engineer als Mitarbeiter des Anbieters ausgibt, oder Schreiben (natürlich mit passendem gefälschten Briefkopf, um den beabsichtigten Kontext herzustellen), die vermeintlich vom Anbieter stammen.

4 Kernelement erfolgreicher Angriffe

Wesentliche Voraussetzung für einen erfolgreichen Social Engineering-Angriff ist es, dass das Opfer einem objektiv nicht vertrauenswürdigen Vorgang subjektiv Vertrauen schenkt. Dabei zielt ein Angriff üblicherweise auf das schwächere Glied in der Prozesskette. In der Regel ist das der Nutzer eines Dienstes, da die Anbieter von für einen Angreifer besonders interessanten Diensten meist für eine möglichst sichere Gestaltung Sorge tragen. Verstärkt wird die ‚Schwachstelle Nutzer' dadurch, dass die meisten Online-Dienste ihre Sicherheit in erster Linie aus ihrer eigenen Perspektive als Anbieter konzipieren.

Für die Sicherheit des Dienstes ist dabei vor allem die Authentizität eines Prozessschritts, genauer: die Sender- bzw. Empfängerauthentizität, relevant; die Vertraulichkeit (verschlüsselte Verbindung) ist dabei meist sekundär. So will der Anbieter sicher sein, dass die in einem Prozessschritt der Transaktion übermittelten Daten tatsächlich von dem vorgeblichen Nutzer oder Kunden stammen bzw. diesen erreicht haben:
- Bei jeder von einem Nutzer (Kunden) ausgelösten Transaktion (z. B. Bestellvorgang, Zahlungsvorgang) will der Anbieter sicher sein, dass tatsächlich der vorgebliche Kunde diese Transaktion ausgelöst hat (Senderauthentizität), und dass er dies im Streitfall nachweisen (bzw. der Kunde es nicht erfolgreich abstreiten) kann.
- Bei jeder vom Anbieter ausgelösten Transaktion muss der Anbieter sicher sein, dass seine Transaktion (z. B. TAN-Übermittlung via SMS, Warenversand) tatsächlich den Kunden erreicht (Empfängerauthentizität) – oder ihm (dem Anbieter) ein Fehler im Streitfall nicht zuzurechnen ist.

Zur Erreichung dieser beiden Sicherheitsziele ergreift ein Anbieter in der Regel verschiedene Maßnahmen, wie bspw. ein kennwortgeschütztes Login, Transaktionsnummern oder der Versand mit Paketverfolgung oder Versicherung. Dabei wird oft jedoch dreierlei übersehen:
- **Erstens**: Auch der Anwender (Kunde) hat Sicherheitsanforderungen – insbesondere die Erwartung, dass die von ihm ausgelösten Prozessschritte den Anbieter erreichen, und alle vorgeblich vom Anbieter stammenden Daten auch tatsächlich von diesem übermittelt wurden. Berücksichtigt man diese Sicherheitsperspektive des Nutzers (Kunden) nicht, hat ein Social Engineer u. U. leichtes Spiel, weil er die Sender- oder Empfängerauthentizität einer Transaktion des (vermeintlichen) Anbieters gegenüber dem Nutzer manipulieren kann.
- **Zweitens**: Sicherheitskonzepte, die sich auf die im System vorgesehenen Kommunikationskanäle (z. B. nur auf Online-Transaktionen) beschränken, schützen nicht vor Social Engineering-Angriffen, die andere Kommunikationskanäle (wie Telefon, SMS, E-Mail, persönlicher Kontakt) verwenden.
- **Drittens**: Die Sender- und die Empfängerauthentizität einer Transaktion leitet sich bei Online-Diensten meist aus der Authentizität bestimmter vorab registrierter Informationen ab. Social Engineering-Angriffe zielen daher oft nicht direkt auf die vom Anbieter zur Erreichung seiner oben genannten Sicherheitsziele ergriffenen Schutzmaßnahmen, sondern auf deren Voraussetzungen (bspw. die für eine mTAN/SMS-TAN verwendete Mobilfunknummer oder die im System hinterlegte Empfängeradresse), indem sie diese mit einer überzeugenden Legende modifizieren. Denn eine Warensendung kann nur dann den Besteller erreichen, wenn die angegebene Adresse stimmt; eine SMS nur dann beim Nutzer ankommen, wenn die hinterlegte Mobilfunknummer korrekt ist. Kann ein Angreifer diese Information (sei es durch einen Social Engineering-Angriff via Telefon oder als ‚Man-in-the-Browser') manipulieren, stimmen die Sicherheitsannahmen des Anbieters nicht mehr.

Ziel des Angreifers ist es, den Nutzer zur Auslösung einer Transaktion zu bewegen, die vermeintlich die Sicherheitserwartungen des Nutzers (Kunden) erfüllt, dabei aber tatsächlich die für eine nicht autorisierte, ge- oder verfälschte Transaktion erforderlichen Daten (PIN, TAN, …) dem Angreifer preisgibt.

Social Engineers machen sich dabei zu Nutze, dass ihre Opfer in der Regel die Senderauthentizität einer Nachricht des Anbieters nicht konsequent überprüfen, sondern aus der subjektiv empfundenen Vertrauenswürdigkeit der Nachricht auf deren Authentizität schließen.

5 Identifikation von Sicherheitslücken

Zur Identifikation von Sicherheitslücken, die von einem Social Engineer genutzt werden können, sind vor allem vier Fragestellungen zu analysieren:
- Gibt es aus der Perspektive des Anbieters Authentizitätsannahmen im Bezug auf den Nutzer (Korrektheit der Anschrift, Korrektheit der Mobilfunknummer, …), deren Voraussetzungen von einem Angreifer manipuliert werden können?
- An welchen beteiligten IT-Systemen kann ein Angreifer mit Hilfe einer geeigneten Legende eine Manipulation der Software (‚Man-in-the-Browser', ‚Man-in-the-Smartphone', …) erreichen, die dann als Basis für weitere Angriffsschritte dienen kann?
- Welche Kommunikationskanäle (SMS, Brief, persönlicher Kontakt, E-Mail, Online-Portal, Telefon, …) können von einem Angreifer zur Kontaktaufnahme mit dem Nutzer (Kunden) eingesetzt werden, um sich hinreichend glaubhaft als Anbieter auszugeben?
- Welche Authentizitätserwartungen des Nutzers (Kunden) können von einem Social Engineer durch die Vorspiegelung von Vertrauenswürdigkeit glaubwürdig erfüllt werden?

Die Antworten auf die beiden ersten Fragen liefern Ansatzpunkte für Sicherheitslücken innerhalb des Protokolls, mit denen die

Authentizitätserwartungen des Anbieters getäuscht werden können. So sollten Protokollschritte auch dann noch authentisch sein, wenn davon ausgegangen werden muss, dass die IT-Systeme des Nutzers – und damit insbesondere das, was ihm am Bildschirm angezeigt wird – durch einen Trojaner kontrolliert werden.

Die Antworten auf die beiden letzten Fragen zeigen Möglichkeiten auf, über die ein Angreifer eine Social Engineering-Attacke auf den Nutzer (Kunden) durchführen kann, die der Anbieter zwar grundsätzlich nicht verhindern, aber zumindest durch geeignete Ausgestaltung seiner Prozesse und Information des Kunden deutlich erschweren kann.

6 Gegenmaßnahmen

Ist die Sender- und Empfänger-Authentizität der Transaktionsschritte aus der Perspektive des oder der Anbieter durch geeignete Maßnahmen sichergestellt, lässt sich ein höheres Maß an Sicherheit nur dadurch erreichen, dass die Nutzer des Dienstes für nicht authentische Kontaktaufnahmen sensibilisiert werden.

Dabei sind vor allem auch Kommunikationskanäle (wie Telefon, SMS, E-Mail etc.) zu betrachten, die in den Prozessen des Anbieters gar nicht vorgesehen sind: Wie kann man z. B. erreichen, dass sich kein Unberechtigter gegenüber dem Nutzer am Telefon glaubwürdig als Bankmitarbeiter ausgeben kann? Dass eine gefälschte E-Mail vom Nutzer als Angriffsversuch enttarnt wird? Dass eine ungewöhnliche Aufforderung auf der (vermeintlichen) Webseite des Anbieters beim Nutzer Verdacht erregt?

Will man bestimmte Kommunikationskanäle nicht grundsätzlich ausschließen (wenn doch, könnte man davor wirksam öffentlich warnen), kommt es darauf an, die Nutzer mit einem ‚typischen' Ablauf vertraut zu machen und an diesen so zu gewöhnen, dass Abweichungen sofort auffallen. Zugleich muss man ihnen einprägsam vermitteln, dass sie bei Auffälligkeiten bspw. eine vorgegebene Telefonnummer zur Verifikation anrufen sollen.

Aber auch bei hoch sensibilisierten Kunden lässt sich ein erfolgreicher, gut konzipierter und damit erfolgreicher Angriff nicht vollständig ausschließen. Daher genügt Prävention allein nicht – Angriffe müssen auch durch permanente Analysen und Konsistenzprüfungen aufgedeckt (Detektion), gestoppt (Schadensbegrenzung) und konsequent verfolgt werden.

7 Fazit

Das weniger erfreuliche Fazit aus den obenstehenden Überlegungen ist: Jedes Online-Banking- und jedes E-Commerce-System muss mit Social Engineering-Angriffen rechnen, die sich nicht oder nur eingeschränkt präventiv bekämpfen lassen. Etwas erfreulicher ist immerhin die Erkenntnis, dass alles sicherlich noch viel schlimmer wäre, hätten Social Engineering-Angriffe nicht durch schlechtes Englisch und noch schlechteres Deutsch Nutzer unfreiwillig erst für Angriffe dieser Art sensibilisiert.

Und noch ein Aspekt begrenzte bisher den Erfolg von Social Engineering-Angriffen: Mehrere besonders erfolgreiche Angriffs-‚Serien' konnten in den vergangenen Jahren dadurch beendet werden, dass die Drahtzieher gefasst wurden. Da in der ‚Szene' Kenntnisse über erfolgreiche Angriffstechniken und Vorgehensweisen selten gestreut werden, um die Entdeckungsgefahr nicht zu vergrößern und die eigene ‚Goldader' zu schützen, mussten neue Angreifergruppen immer wieder das eine oder andere Rad neu erfinden.

Dennoch bleibt die ernüchternde Einsicht, dass die sozialen Regeln zwischenmenschlicher Vertrauensbildung in weitgehend anonymen Online-Diensten hemmungslos zur Schädigung von Nutzern missbraucht werden. Was in unserem täglichen Leben vernünftiges und bewährtes Verhalten ist, kann im Internet naive Gutgläubigkeit sein.

Referenzen

[1] Mitnick, Kevin: Die Kunst der Täuschung. Mitp Verlag, 2003.
[2] Weßelmann, Bettina: Maßnahmen gegen Social Engineering. DuD 9/2008, S. 601-604.