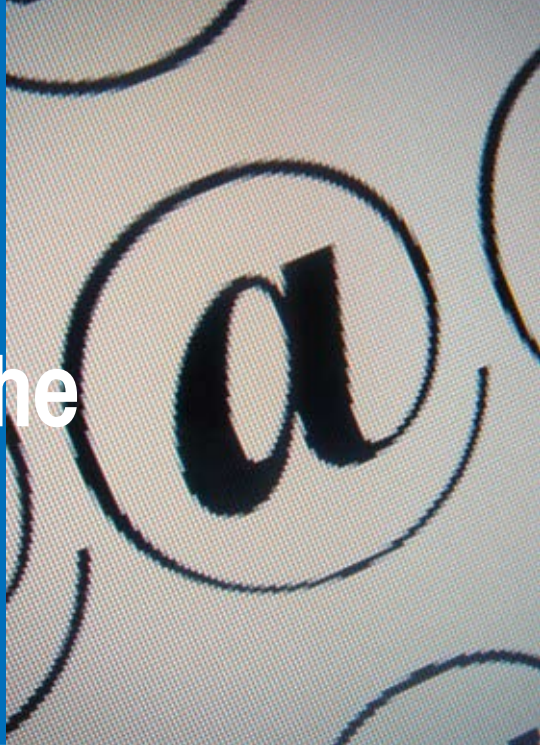
Aspekte sicheren Onlinebankings: **psychologische** Faktoren beachten

Von Eduard Heindl



Technisch gesehen ist der reine Übertragungsweg von Daten beim Onlinebanking durchaus sicher, meint Eduard Heindl. Doch die psychologischen Seiten des Prozesses werden zu oft vernachlässigt, sodass beispielsweise die sichere Erkennung des Kommunikationspartners nicht immer gegeben ist, warnt der Autor. Sein Fazit: Die Internetpräsenz einer Bank muss dieselbe Wiedererkennbarkeit und Seriosität ausstrahlen wie eine reale Bankfiliale. Red.

Für Banken ist Onlinebanking eine optimale Ergänzung ihrer Geschäftsprozesse, da der Medienbruch klassischer, überweisungsträgergebundener Bankgeschäfte wegfällt. Daher gibt es von Seiten der Banken einen starken Druck in Richtung Onlinebanking und auch einen frühen Markteintritt, der teilweise bis in die achtziger Jahre des letzten Jahrhunderts mit BTX zurückreicht. Wenig verstanden ist aber immer noch das Nutzerverhalten, vor allem unter Sicherheitsaspekten. Dies soll hier näher diskutiert werden.

Komponenten der Sicherheit

Jedes sichere System besteht aus Einzelkomponenten, die eine Kette bilden. Das schwächste Glied in der Kette wird zumeist von Angreifern genutzt, um das System zu missbrauchen. Im heutigen Onlinebanking über Internet mit verschlüsseltem TSL (oft als SSL bezeichnet) kann praktisch ein kryptologisches Niveau erreicht werden, das einen direkten Angriff auf den Transportkanal aussichtslos macht. Die wesentlichen Komponenten sind dabei die öffentlichen und privaten Schlüssel der beiden Teilnehmer, Kunde und Bank, sowie ein Sitzungsschlüssel, der heute standardmäßig 128 Bit Länge hat und damit nicht mit verfügbaren Ressourcen entschlüsselt werden kann.

Betrachtet man den TLS-Prozess genauer, gibt es das Problem der sicheren Erkennung des Kommunikationspartners. Das Problem ist dabei asymmetrisch, jede Bank besitzt sicherlich einen digital signierten öffentlichen Schlüssel, kaum ein Kunde in Deutschland hat seinen Browser jedoch mit einem signierten öffentlichen Schlüssel ausgestattet. Weiterhin ist auch das Wissen über die Abläufe bei der Verschlüsselung sehr ungleich verteilt, im Rechenzentrum der Bank ist ausreichend Kompetenz für die optimale Konfiguration des Systems vorhanden, auf Kundenseite kann von völliger Ignoranz bis Perfektion alles gefunden werden. In diesem Spannungsfeld muss es nun gelingen, die Sicherheit auf der Kundenseite zu erhöhen, ohne unnötige und unrealistische Forderungen an die Kunden zu stellen.

Zum Autor

Prof. Dr. Eduard Heindl, Hochschule Furtwangen, Fakultät Wirtschaftsinformatik, Furtwangen.

Architektur des Bankgebäudes strahlt Stetigkeit aus

Sicherheit ist neben der Kette aus sicheren Komponenten auch ein psychologisches Phänomen. Banken leben vom Vertrauen der Kunden, da diese ihr Bestes, ihr Geld, an die Bank zur Aufbewahrung übergeben. Im klassischen Modell ist das Interface das Bankgebäude mit seriös wirkenden Mitarbeitern. Daneben natürlich alles was in der Öffentlichkeit über die Bank bekannt ist.

Sieht der Kunde die Bank, strahlt bereits die Architektur des Gebäudes Stetigkeit aus. Betritt ein Kunde eine Bank, öffnet sich die Tür automatisch, so findet er sorgfältig ausgestattetes Interieur vor, das ihm Vertrauen in die Geschäftsprozesse vermittelt. Jeder Mitarbeiter ist korrekt gekleidet und höflich. Alle Bereiche der Bank sind beschildert oder durch ihr Aussehen leicht den Aufgaben zuzuordnen, die Kasse liegt hinter einer dicken Glasscheibe, die Beratung ist von Pflanzen umrankt. Private Angelegenheiten können in separaten Räumen besprochen werden. Was ist das Spiegelbild dieser Situation im Internet?

Die Homepage auf der Domain der Bank sollte die gleiche Ausstrahlung haben wie das Gebäude, die vielen Unterseiten entsprechen dem Interieur und die Texte den höflichen korrekten Mitarbeitern.

Sicherheitsproblem Domainwechsel

Besucht ein Kunde eine Bank online, so wird er die Internetadresse der Bank in seinen Browser eingeben oder von Google dorthin vermittelt. Bereits diese Adresse ist nicht immer aussagekräftig, so findet man sich schnell auf einer Seite mit einem Namen ähnlich wie „vr-networld.de/c51/default.html" wieder, was auch immer das bedeuten mag, aussagekräftig ist es jedenfalls nicht.

Geht er dann zum sicheren Onlinebanking findet er sich auf Seiten mit so kryptischen Namen wie „https://finanzportal.fiducia.de/ebpp08/entry?rzid=XC&rzbk=0418" wieder, wobei selbst für Internetexperten nicht sofort zu erkennen ist, dass es sich hier um eine Webseite der Volksbank handelt. Aus Sicht des Internetprotokolls ist es ein Domainwechsel, der immer eine Domainserveranfrage erfordert. Mit geeigneten Manipulationen im Bereich der Domainserver könnte hier leicht auf eine „andere" Adresse umgelenkt werden. Dies ist ein bekanntes Sicherheitsproblem im Internet-Protokoll.

Zertifikat des Websitebesitzers prüfen

Auch der Sicherheitshinweis „Geben Sie die Internet-Adresse Ihrer Bank per Hand ein" wird hier sehr fragwürdig. Man stelle sich vor, eine Bank würde ihren Postverkehr über die Adresse einer anderen Firma abwickeln. Besonders problematisch ist aber, dass gerade Angreifer oft unter einer Subdomain arbeiten, die ähnlich aufgebaut ist, etwa „Volksbank.secure2000.de" ist noch frei im Internet verfügbar. Technisch ist es ein leichtes, die Adressen kundenfreundlich und fälschungssicherer aufzubauen.

Ein unsicherer Kunde sollte immer auf die Identität der Websitebesitzer schauen, dazu findet er im Browser den Hinweis, für wen das Zertifikat ausgestellt wurde. Im Beispiel ist das die Fiducia IT AG, der Betreiber der sicheren Bankverbindung. Das ist sicherlich den Bankmitarbeitern klar, ob es jeden Kunden klar ist, sei dahingestellt. Zumindest wird das Unternehmen auf der Seite nicht erwähnt, der Kunde sieht nur das Logo der Volksbank. Sicheres Homebanking sollte nicht zu viel Wissen über die interne Struktur der Bank voraussetzen. Besser ist auch hier eine vertrauensvolle Angabe wie Volksbank XY, die in diesem Fall ja der Geschäftspartner des Vertrauens des Kunden ist, zu verwenden.

Das Homebanking entspricht dem Besprechungszimmer

Besucht der Kunde die Homepage, so ist nicht nur die Internetadresse von zentraler Bedeutung, sondern auch das Erscheinungsbild. Es ist wie das Betreten des Bankgebäudes. Der Kunde findet auf vielen Bank-Homepages eine Fülle von Informationen und das ist sicherlich auch im Interesse des Kunden. Eine ganz andere Situation ist es aber, wenn sich der Kunde in den „Privatbereich" des Homebankings zurückzieht. Dieser sollte wie ein Besprechungszimmer sein.

Bemerkenswerterweise findet man häufig blinkende Animationen auf der Login-Seite des Onlinebankings, was während des konzentrierten Eingebens von Login und Passwort hinderlich ist. Ähnlich verhält es sich mit Seiten, in denen etwa die Sicherheitsregeln für Onlinebanking beschrieben werden. Aus der Wahrnehmungspsychologie ist bekannt, dass sich ein Mensch nur auf eine Sache so konzentrieren kann, dass er sie auch lernt und behält. Jede Ablenkung in solchen Situationen führt zum raschen Vergessen oder zu Orientierungsschwierigkeiten.

Den Kunden mit Namen ansprechen

Ist der Kunde auf seinem Zugang eingeloggt, so sollte er eindeutig erkennen, dass er die richtige Domain besucht. Es ist auf jeden Fall nützlich, wenn der Kunde jetzt mit seinem Namen angesprochen wird und das Erscheinungsbild vertraut ist. Ablenkung durch Werbeaussagen sollte in diesem Bereich tabu sein. Eine zentrale Bedeutung hat jetzt eine einfache, eindeutige Nutzerführung. Wenn man sich klar macht, dass viele Kunden älter sind und mit kleiner Schrift Schwierigkeiten haben, wundert es, dass häufig viel zu kleine Schriftfonts verwendet werden. Auch sind die Kontraste bei vielen Onlinebanking-Seiten ein Problem, nicht überall herrschen optimale Beleuchtungsverhältnisse vor.

Der Ablauf einer Transaktion besteht oft aus mehreren Schritten und ist aus der Realwelt in Form von Überweisungsträgern und Kontoauszügen vertraut. Leider findet der Kunde in vielen Onlinebanking-Abläufen eine andere, oft stark modifizierte Optik vor. Dies erfordert zusätzlichen Lernauf-

Beispiel: Maske bei der Eingabe von Login und Password auf der Website der Volksbank Triberg: Es wird als Zertifikatherausgeber die Fiducia IT AG genannt, das Eurosymbol rechts blinkt ablenkend.

wand und wird daher tendenziell gemieden.

Wiedereinstieg an derselben Stelle

Am Ende der Onlinebanking-Aktivität sollte das Ausloggen stehen, da dies aber häufig nicht von den Kunden genutzt wird, beenden viele Systeme das Homebanking nach einer bestimmten Zeit, etwa 15 Minuten nach der letzten Aktivität. Für viele Nutzer ist das sehr hinderlich, da im Lebensalltag häufig ein Telefonat oder die Suche nach PIN und TAN dazwischen kommen kann. Hier ist eine Rückkehr auf den letzten Screen nach wiederholter Eingabe von Login und Passwort wünschenswert. Dieses Verhalten ist der Nutzer bereits von anderen Computersystemen gewohnt, die nach Verlassen des Arbeitsplatzes auf Bildschirmschoner schalten und zum Wiedereinloggen auffordern. Danach wird nicht der Rechner gebootet, sondern der letzte Screen wieder angezeigt.

Die angesprochene Realität des Onlinebankings ist leider noch nicht die ideale Welt des sicheren Onlinebankings, wie es angestrebt wird. Nachdem klar ist, dass die technische Sicherheit mit TSL auch hohen Ansprüchen der Kryptografie genügt, müssen soziale und psychologische Aspekte der Nutzung in den Vordergrund rücken.

Phishing-Mails oft unbeholfen formuliert

Ein Grundkonzept für Vertrauen und Sicherheit ist Konsistenz. Stimmen alle Faktoren kohärent überein, so wird Vertrauen aufgebaut. Bemerkenswerterweise sind immer noch viele Phishing-Angriffe leicht zu erkennen, da an einigen Stellen Inkonsistenz auftritt, die Sprache ist ungewöhnlich, Anweisungen werden oft unüblich formuliert. Hier ein Beispiel aus einer Phishing-Mail des Internetlexikons Wikipedia: „den TAN-Codes, eine ganze Reihe der Mitteldiebstähle von den Konten unserer Kunden durch den Internetzugriff festgestellt. Zurzeit kennen wir die Methodik nicht, die die Missetäter für die Entwendung der Angaben aus den TAN – Tabellen verwenden."

Das bedeutet, dass die Nutzerführung als integraler Bestandteil der Sicherheit im Onlinebanking verstanden werden muss. Und unter Nutzerführung wird hier mehr verstanden, als nur das Benutzen einfacher Icons oder Links. Jedes Element, das in eine so kritische Anwendung wie ein Onlinebanking-Portal eingebaut wird, muss folgenden Kriterien genügen:

- Ist es eindeutig?
- Ist es üblich?
- Ist es hilfreich?
- Ist es dauerhaft?
- Ist es fehlerfrei?

Wenn Steve Krug sein Buch zum Internetdesign „Don´t make me think" nennt, könnte man im Onlinebanking die Regel „Lass mich nicht (ver)zweifeln" nehmen.

Daneben ist es sicherlich hilfreich, auch begleitende Element des Onlinebankings zu verbessern. So erhält der Autor immer die TAN-Liste auf billigstem Papier, wertvoll wie eine Banknote wirkt das Dokument nicht. Warum sollten diese Dokumente nicht ihren Wert auch in der geeigneten Form ausstrahlen?

Das Homebanking ist im Umbruch, auf Dauer werden PIN und TAN nicht den Sicherheitsanforderungen genügen. Die wesentlichen Alternativen bauen entweder auf digitale Zertifikate in Kombination mit einem Hardware-Schlüssel und andere auf biometrische Authentifizierung. Bisher haben sich alle biometrischen Verfahren als sehr labil erwiesen und auch für die Realität der privaten Bankhandlungen unpraktisch. Dies versteht jeder, der versucht hat älteren Leuten bei einer Onlineüberweisung zu helfen oder sich selbst mit seinem Fingerprintsensor von seinem eigenem Rechner ausgesperrt hat. Daher erscheint der Einsatz von biometrischen Verfahren in den nächsten Jahren unrealistisch.

Als Schlüssel nutzen: Hardware im USB-Stick

Völlig anders stellt sich die Situation bei hardwarebasierten Verfahren dar. Traditionell sind es Menschen in unserer Kultur gewohnt, sichere Bereiche mit einem physischen Schlüssel zu betreten. Es liegt daher nahe, auch im Onlinebanking ein Stück Hardware zu verwenden, das die wichtigsten Eigenschaften eines Schlüssels vereinigt. Durch die weite Verbreitung von USB-Sticks sind alle Computernutzer mit der Nutzung dieser Speicher vertraut.

Zudem kann ein USB-Stick, bei geeigneter Bauform, problemlos an einem Schlüsselbund angehängt werden und vermittelt dann zusätzlich das „Gefühl" einen Schlüssel zu besitzen. Damit wird aber auch rasch der Verlust des Schlüssels erkannt, ebenfalls ein wichtiges passives Sicherheitsmerkmal. Ist im USB-Stick die geeignete Hardware vorhanden, können alle denkbaren Transaktionen von jedem Rechner, der einen USB-Steckplatz hat, durchgeführt werden. Die Kosten für eine solche Lösung sind bei geeigneten Stückzahlen minimal.

Wir werden also in Zukunft ein einfach zu bedienendes und sehr sicheres Onlinebanking vorfinden. Das Interface erlaubt es, jede Transaktion rasch und überschaubar durchzuführen. Durch die Verfügbarkeit von Laptops und Rechnern mit USB-Anschluss ist überall das persönliche Verwalten der eigenen Konten möglich. Angriffe durch Hacker werden damit soweit erschwert, wie es auch heute kaum möglich ist, in fremde Bankgebäude ohne Schlüssel einzudringen. Je rascher diese Aspekte umgesetzt werden, um so höher wird die Akzeptanz des Onlinebankings und das Vertrauen der Kunden in die Banken in diesem Bereich erhöht.