Fraunhofer Institut
Sichere Informations-
Technologie

Phishing-Schutz im Online-Banking

Hilfe zum Selbstschutz für Nutzer

Wie gut unterstützen Banken ihre Kunden im Schutz vor Phishing?

Zwölf Web-Angebote im Vergleich

Zusammenfassung

Anbieter von Online-Diensten und deren Nutzer sind zunehmend von Phishing-Angriffen betroffen. Phishing unterscheidet sich von anderen Bedrohungen in der IT-Sicherheit: Die Täter täuschen die Nutzer mit gefälschten E-Mails und Webseiten, um sie zur Eingabe vertraulicher Daten zu verleiten. Herkömmliche Sicherheitstechnik kann dagegen wenig ausrichten.

Die Forschung zu geeigneten Gegenmitteln steckt noch in den Kinderschuhen. Am wirksamsten sind derzeit aufmerksame, misstrauische Benutzer. Anbieter können bereits jetzt einige grundlegende Maßnahmen ergreifen, um ihren Kunden die Erkennung und Abwehr von Phishing-Angriffen zu erleichtern.

Bisher konzentrierten sich die Phishing-Versuche in Deutschland auf Banken und ihre Kunden. Das Fraunhofer-Institut für Sichere Informationstechnologie SIT hat in einer unabhängigen Studie die Web-Angebote von 12 Banken bewertet. Im Hintergrund stand die Frage, wie gut die getesteten Banken ihren Kunden dabei helfen, Phishing-Versuche zu erkennen.

Die Bewertung erfolgte in drei Kategorien: technische Gestaltung des Online-Banking-Angebots, Unterstützung von HBCI als Alternative zum Web, sowie Kundeninformation. Zu jeder Kategorie gehören mehrere Einzelkriterien, für deren Erfüllung jeweils Punkte vergeben wurden.

Die Ergebnisse zeigen ein deutliches Potenzial für Verbesserungen. Nur ein Testkandidat, die Deutsche Bank, erreichte ein sehr gutes Ergebnis. Die Note „gut“ wurde nicht vergeben. Mit „befriedigend“ wurden fünf getestete Angebote bewertet: Postbank, Commerzbank, Dresdner Bank, ING-DiBA und Comdirect. Die übrigen Testteilnehmer erzielten ein ausreichendes Ergebnis, mit Ausnahme des Schlusslichts Sparda-Bank Hamburg.

Insgesamt zeigt dass Testergebnis, dass die Mehrzahl der Banken ihre Kunden besser vor Phishing schützen könnte. Dazu sind im ersten Schritt keine komplizierten Sicherheitsmaßnahmen erforderlich. Bereits ein konsistentes, erwartungskonformes Erscheinungsbild des Web-Angebots kann vorsichtigen Nutzern dabei helfen, Phishing-Angriffe zu erkennen. Auf lange Sicht erfordert der effektive Schutz vor Phishing verfeinerte Kriterien, geeignete Benutzermodelle und technische Schutzmaßnahmen.

Inhalt

1 Sicherheitsproblem Phishing

Phishing – eine Verballhornung des Wortes „fishing“ („Angeln“) – bedroht zunehmend die Sicherheit elektronischer Geschäftsprozesse. Es handelt sich um eine Form des Betrugs, die mit Hilfe technischer Manipulationen die Nutzer von Internet-Diensten täuscht. Bis vor kurzem waren vornehmlich englischsprachige Nutzer das Ziel solcher Angriffe. Seit einigen Monaten jedoch zeigen sich verstärkt auch Phishing-Versuche in deutscher Sprache. Besonders betroffen von Phishing-Angriffen sind Banken und andere Finanzdienste mit ihren Online-Angeboten sowie bekannte Webdienste wie zum Beispiel eBay und Yahoo [APWG04b, BlSch04, Kos04].

1.1 Was ist Phishing?

Phishing stützt sich meist auf die Netzdienste E-Mail und World Wide Web. Beide geben dem Absender beziehungsweise dem Anbieter weitreichende Kontrolle über die Informationsdarstellung beim Empfänger oder Nutzer. E-Mail lässt sich nach Belieben fälschen, und auch im Web ist der äußere Anschein kein geeigneter Indikator für die Echtheit einer Seite.

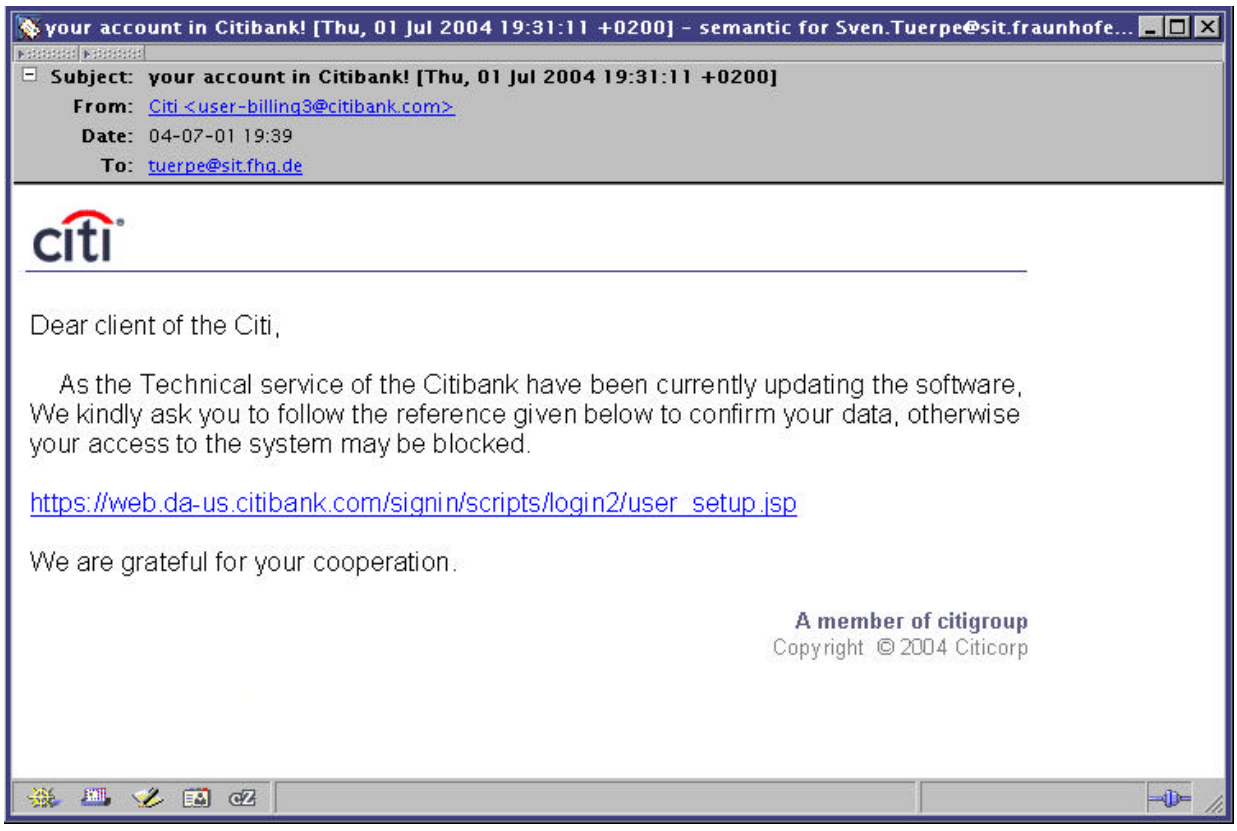
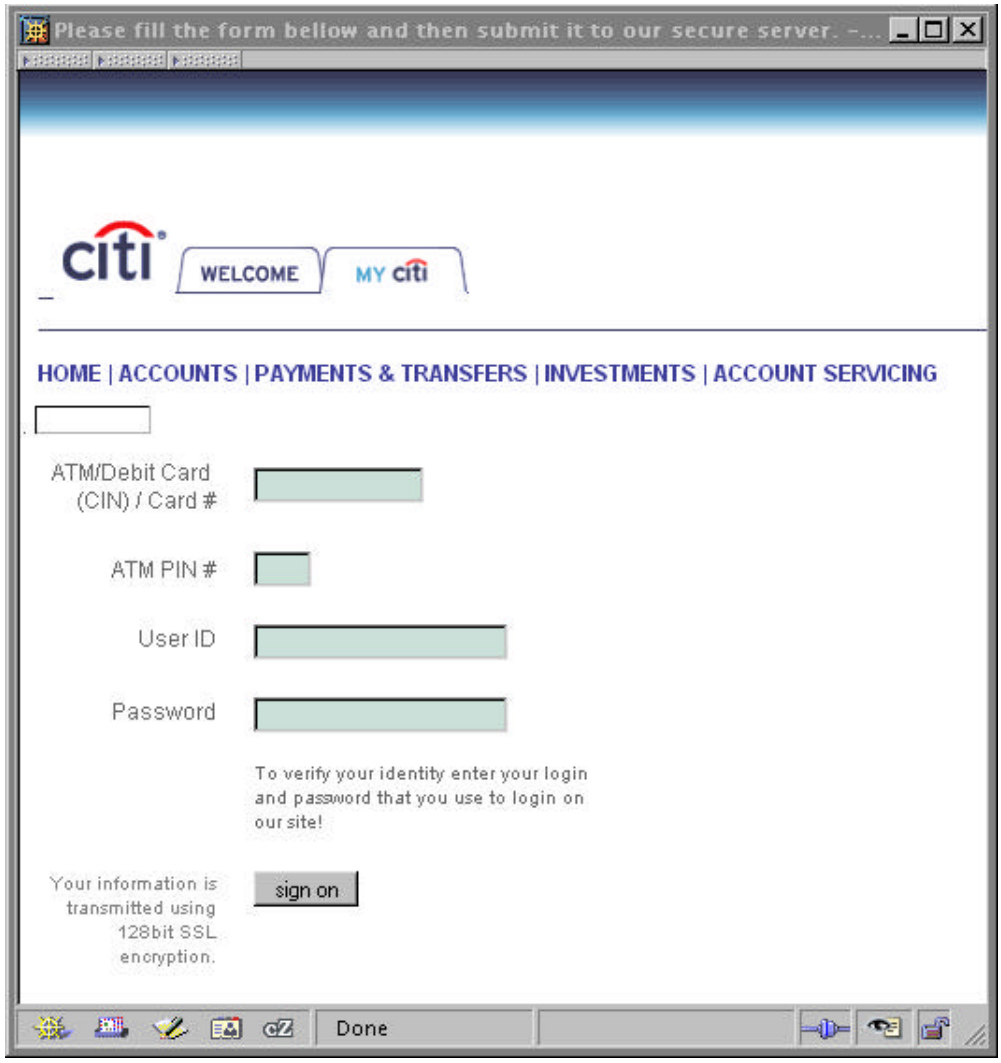


Bild 1 Eine Phishing-Mail. Der Absender ist gefälscht, der Link führt in Wirklichkeit zu einer Phishing-Website

Phishing beginnt mit einer gefälschten E-Mail, die die Täter massenhaft verbreiten. Die Empfänger werden darin unter einem Vorwand aufgefordert, die Website einer Bank oder eines Dienstanbieters zu besuchen und dort persönliche Daten einzugeben.

Bild 1 zeigt ein Beispiel in englischer Sprache. Der Absender der Nachricht ist gefälscht. Das Logo stammt vermutlich von der echten Website der Bank; E-Mail im HTML-Format macht die Einbettung von Bildern sehr einfach. Der enthaltene Link zeigt den Namen der echten Website der Citibank, führt in Wirklichkeit aber zur Website der Betrüger.

Bild 2 Eine Phishing-Website



Die Phishing-Website – Bild 2 zeigt die Website aus einem anderen Phishing-Fall, der ebenfalls auf Kunden der Citibank zielte – enthält ein Formular, das in seinem Erscheinungsbild der echten Website angepasst ist. Dort soll das Opfer vertrauliche Informationen eingeben, zum Beispiel Kartennummern, PINs und Passworte.

Phishing nutzt zum einen klassische Methoden des Betrugs. Den Opfern wird unter einem Vorwand nahegelegt, mit den Tätern zu kooperieren. Oft werden

sie auch subtil unter Druck gesetzt, beim Phishing etwa mit der Drohung, einen Dienst nicht mehr nutzen zu können. Hinzu kommen im Internet aber die leichte Fälschbarkeit gerade jener Merkmale, die für das Sicherheitsgefühl der Nutzer wichtig sind, sowie die Möglichkeit, eine Vielzahl potentieller Opfer gleichzeitig anzusprechen.

Phishing stützt sich also auf bestehende Vertrauensbeziehungen zwischen Nutzern und Anbietern, die durch Fälschung und Manipulation wesentlicher Erkennungsmerkmale ausgenutzt werden. Welche Merkmale relevant sind, hängt dabei vor allem vom gedanklichen Modell ab, das sich die Nutzer vom Netz und seinen Diensten gebildet haben, und das deren Erwartungen bestimmt. Erst in zweiter Linie spielen Sicherheitsmechanismen wie Sicherheitszertifikate eine Rolle.

1.2 Auswirkungen

Nach Schätzungen der Anti-Phishing Working Group (APWG) sind Phishing-Betrüger bei bis zu 5% der E-Mail-Empfänger erfolgreich [APWG04a]. Diese Zahl verdeutlicht, dass Phishing eine ernstzunehmende Bedrohung für die Sicherheit elektronischer Geschäftsprozesse darstellt. Ebenso zeigt sie, dass der Erfolg von Phishing-Angriffen nicht allein auf grobe Fahrlässigkeit der Nutzer zurückgeführt werden kann. Noch deutlicher ist das Ergebnis einer anderen Studie, der zufolge 7 von 10 befragten Nutzern schon einmal erfolgreich auf eine Phishing-Site gelockt wurden [Tru04]. Immerhin 15% davon gaben an, schon einmal zum Opfer eines Phishing-Betrugs geworden zu sein.

Ziele der Täter

Potentielle Ziele sind alle Informationen,

- die (teilweise) vertraulich sind, d.h. in der Regel nur zweckgebunden im Rahmen einer Geschäfts- und Vertrauensbeziehung weitergegeben werden,
- die im elektronischen Geschäftsverkehr üblicherweise ausgetauscht werden, und
- die sich unmittelbar oder indirekt missbrauchen lassen.

Dahinter steckt in der Regel eine finanzielle Motivation. Ein Beispiel für den unmittelbaren Missbrauch ist die Bezahlung von Online-Einkäufen mit mit durch Phishing oder auf andere Weise erlangten Kreditkartendaten. Indirekter Missbrauch liegt vor, wenn beispielsweise in Betrugshandlungen fremde Nutzeridentitäten missbraucht werden, um Spuren zu verwischen und etabliertes Vertrauen auszunutzen.

Zu den Informationen, die beim Phishing erschlichen werden, gehören folglich vor allem Zugangs- und Sicherheitscodes (Benutzernamen, Passworte, PINs, Transaktionsnummern). Darüber hinaus können die Täter aber auch an weiteren persönlichen Daten interessiert sein, die sich für die Vorspiegelung falscher Identitäten nutzen lassen. In den Vereinigten Staaten, wo häufig die Sozialversicherungsnummer als Identifikationsmerkmal eingesetzt wird, geht dies bis hin zum kompletten Identitätsdiebstahl. In den USA entstehen durch Identitätsdiebstahl jährlich Schäden in Höhe von 2,4 Milliarden US-Dollar [Hei04d,

Hei04g]. Phishing ist hier allerdings nur eine von mehreren verbreiteten Methoden des Identitätsdiebstahls.

In einer anderen Studie kamen TRUSTe und das Ponemon Institute zu dem Ergebnis, dass sich die Schäden durch Phishing in den USA auf 500 Millionen US-Dollar belaufen [Tru04]. Grundlage dieser Untersuchung war die Befragung von mehr als 1000 Internet-Nutzern, von denen 70% angaben, schon einmal unabsichtlich eine Phishing-Website besucht zu haben.

Betroffene Unternehmen

Der „Phishing Trends Report", den die APWG regelmäßig herausgibt [APWG04b], zeigt ein eindeutiges Bild: Phishing konzentriert sich derzeit auf Banken und Finanzdienstleister. Mit großem Abstand folgen Online-Shops und Handelsplattformen. Die naheliegende Erklärung: Finanzdienste bieten unmittelbaren Zugriff auf das Geld ihrer Kunden. Phishing-Versuche in Deutschland richteten sich bisher unter anderem auf Kunden der Deutschen Bank, der Postbank sowie der Volks- und Raiffeisenbanken.

Unter den Händlern und Handelsplattformen führt das Auktionshaus eBay die Liste an. Hier dürften vornehmlich die Benutzeraccounts von Interesse sein, die sich für Betrugshandlungen gegenüber anderen Nutzern missbrauchen lassen.

Da Phishing auf massenhaft verbreiteten E-Mails beruht, sind für die Täter vor allem solche Unternehmen interessant, deren Name bekannt ist und deren Online-Angebote von vielen Menschen genutzt werden.

Folgen

Neben den zu erwartenden Unannehmlichkeiten für die einzelnen Opfer haben Phishing-Angriffe vielfältige Auswirkungen auf die Geschäftstätigkeit betroffener Unternehmen:

- Phishing missbraucht etablierte Marken und Online-Angebote und untergräbt das Vertrauen der Kunden in den Anbieter.
- Erfolgreiche Phishing-Aktionen führen zu erhöhtem Aufwand in der Kundenbetreuung.
- Phishing macht neue Sicherheitsmaßnahmen zur Vermeidung, Erkennung und Verfolgung notwendig, die kostspielig sein können.
- Kommunikationswege werden entwertet. Dies gilt insbesondere für E-Mail: kritische Kunden verwerfen auch legitime Benachrichtigungen und Aufforderungen, wenn sie jederzeit mit Phishing rechnen müssen [Hei04b, Tru04].
- Unter Umständen werden Anbieter auch mit Schadensersatzforderungen konfrontiert. Wem im Zusammenhang mit Phishing welche Sorgfaltspflichten obliegen, ist noch nicht abschließend geklärt.

Es ist zu erwarten, dass sowohl die Zahl als auch die Qualität der Phishing-Angriffe in Zukunft zunehmen wird. Die zugrundeliegenden technischen Probleme aber lassen sich kaum kurzfristig lösen. Umso wichtiger sind optimale Sicherheitsmaßnahmen im Rahmen der existierenden technischen Standards.

Der vorliegende Vergleichstest widmet sich elementaren Maßnahmen, die jeder Anbieter ergreifen kann, ohne neuartige Sicherheitstechnologien einzuführen. Sie bilden die Voraussetzung dafür, dass weitergehende technische Mittel überhaupt sinnvoll eingesetzt werden können.

2 Testziel und Annahmen

Technische Schutzmaßnahmen gegen Phishing stecken noch in den Kinderschuhen. Der effektivste Schutz gegen Phishing-Angriffe sind daher zurzeit aufmerksame und misstrauische Benutzer. Aufmerksamkeit und Misstrauen fordern auch die betroffenen Banken von ihren Kunden, nicht nur in Sicherheitshinweisen, sondern auch in ihren Allgemeinen Geschäftsbedingungen. Es obliegt dem Bankkunden, sorgfältig mit sensiblen Daten wie PIN und TAN umzugehen. Erfahrungen etwa in Zusammenhang mit dem Missbrauch von EC-Karten zeigen, dass die Banken im Schadensfall häufig auf diese Sorgfaltspflichten pochen und die Beweislast für Unsicherheiten im System bei den geschädigten Kunden sehen.

Beim Phishing stellt sich die Frage nach der notwendigen und zumutbaren Sorgfalt neu. Wir wollten deshalb wissen, wie gut die Banken in Deutschland ihre Kunden dabei unterstützen, Phishing-Angriffe zu erkennen und richtig zu reagieren.

Ziel

Der hier vorgestellte Vergleichstest soll ermitteln, wie gut Banken in Deutschland ihre Online-Banking-Kunden bei der Erkennung und Abwehr des Phishing-Betrugs unterstützen. Grundlage sind öffentlich einsehbare Informationen aus den Web-Angeboten der getesteten Banken.

Bislang liegen kaum gesicherte Erkenntnisse darüber vor, welche Kunden unter welchen Umständen Opfer von Phishing-Betrügern werden. Unser Test stützt sich daher auf Annahmen. Er kann nur eine grobe Einschätzung liefern.

Idealer Nutzer

Der Vergleichstest geht von einem idealen Nutzer aus. Dieser ideale Nutzer:

- Ist sicherheitsbewusst,
- Hat von Phishing gehört und will sich explizit davor schützen,
- Verfügt über sicherheitstechnische Grundkenntnisse, z.B. zur Benutzung der Sicherheitsfunktionen im Browser; und
- Prüft aktiv die Echtheit einer Seite, bevor er Daten eingibt.

Der angenommene Idealnutzer versucht also, im Rahmen seiner Möglichkeiten die nötige Sorgfalt an den Tag zu legen. Mehr kann eine Bank von ihren Kunden kaum erwarten. Daraus folgt die Mindestanforderung, solchen Nutzern keine Steine in den Weg zu legen. Insbesondere müssen alle notwendigen Informationen zur Verfügung stehen und sichtbar sein. Um alle Kunden effektiv zu schützen, werden in der Praxis freilich weitere Sicherheitsmaßnahmen erforderlich sein, zum Beispiel zur schnellen Erkennung und Abschaltung von Phishing-Websites.

Annahmen

Den Testkriterien liegt die Annahme zugrunde, dass Phishing von den Nutzern am zuverlässigsten erkannt wird, wenn dazu wenige, einfache Regeln genügen. Am effektivsten sind dabei solche Regeln, die die Nutzer implizit lernen, während sie mit dem System interagieren. Solche Regeln sorgen dafür, dass bei unerwarteten Abweichungen Misstrauen entsteht.

Anleitungen und Sicherheitshinweise vermitteln dagegen explizites Wissen. Das tatsächliche Verhalten der Benutzer beeinflussen sie deshalb weniger stark als die Erfahrungen aus dem Umgang mit dem System. Zum einen ist explizites Wissen kein Handlungswissen. Zum anderen werden solche Informationsmaterialien nicht immer gelesen und der Inhalt behalten.

Regeln können sowohl die Interpretation wahrgenommener Informationen betreffen als auch das Verhalten des Nutzers. Beispiele für einfache Regeln:

- »Alle Online-Angebote der Sparstrumpfbank haben eine Adresse, die auf .sparstrumpf.de endet.«
- »Für das Online-Banking benutze ich ein eigenes Programm. Nur dort gebe ich meine PIN ein.«

Komplizierte Regeln wären zum Beispiel:

- »Die echte Online-Banking-Site der Hohe Kante Bank AG erkenne ich, indem ich das Sicherheitszertifikat gründlich prüfe. Der Fingerprint des Zertifikats muss zurzeit 5f:d4:c6:12:e3:07:3c:1e:16:61:97:2d:9d:f3:a5:74 lauten, ändert sich aber am 23. Oktober.«
- »Die Geldspeicherbank schickt mir unregelmäßig einen Newsletter sowie monatlich einen Hinweis auf meine online einsehbare Kreditkartenabrechnung. Die Links darin kann ich ohne Bedenken anklicken. Wenn ich aber per E-Mail aufgefordert werde, meine PIN einzugeben, dann ist diese Mail vielleicht gefälscht.«

Ein hinsichtlich der Phishing-Abwehr gut gestaltetes Online-Banking-Angebot unterstützt die Bildung einfacher Modelle und Regeln, informiert seine Nutzer deutlich und umfassend über die Gefahr und Schutzmöglichkeiten und bietet Alternativen zur Nutzung des Web-Browsers.

Grenzen

Der vorliegende Test widmet sich ausschließlich der Phishing-Gefahr. Andere Sicherheitsbedrohungen, zum Beispiel durch Würmer, Viren und Trojanische Pferde, bleiben unberücksichtigt.

Im Fokus liegen Sicherheitsmaßnahmen, die die Bankkunden dabei unterstützen, Phishing selbst zu erkennen. Darüber hinaus können betroffene Banken eine Reihe weiterer Maßnahmen ergreifen, etwa zur rechtzeitigen Erkennung von Angriffen und Verfolgung der Täter. Solche Aktivitäten konnten nicht berücksichtigt werden, da hierzu die Mitwirkung aller Testteilnehmer erforderlich

gewesen wäre. Darauf wollten wir verzichten, um schnell und unabhängig zu einem Ergebnis zu gelangen.

Der Bewertungsmaßstab weist eine gewisse Unschärfe auf. Sie lässt sich in einem Schnelltest, der mit vertretbarem Aufwand ausgeführt werden soll, kaum vermeiden. Die Testergebnisse können einen ersten Eindruck vermitteln, wie gut die berücksichtigten Maßnahmen insgesamt sowie bei den einzelnen Teilnehmern umgesetzt sind. Zur Sicherheitsoptimierung eines Web-Angebots reichen sie nicht aus. Hierfür sind gründlichere Untersuchungen unabdingbar.

Die Testkriterien wurden auch unter dem Gesichtspunkt ausgewählt, dass der Test ohne Mitwirkung der getesteten Banken und ohne Geschäftsbeziehung zu diesen möglich sein sollte. Eine andere Auswahl von Kriterien oder eine andere Gewichtung kann zu anderen Ergebnissen führen.

Das Testergebnis erlaubt keine abschließende Bewertung des Phishing-Risikos, dem Kunden bei den bewerteten Banken ausgesetzt sind. Dieses Risiko wird nicht nur von den hier betrachteten Sicherheitsmaßnahmen bestimmt, sondern auch von weiteren Faktoren, etwa dem Verhalten der Betrüger, dem Umgang der Bank mit Sicherheitsvorfällen und dem Verhalten der einzelnen Bankkunden.

3 Teilnehmer

Wir haben eine Auswahl aus den in Deutschland aktiven Banken getestet, die Girokonten für Privatkunden anbieten. Bei regional organisierten Banken – Sparkassen sowie Volks- und Raiffeisenbanken – erfolgte der Test jeweils anhand eines willkürlich gewählten Vertreters.

Die 12 Teilnehmer:

- Postbank
- Deutsche Bank
- Dresdner Bank
- Commerzbank
- Citibank
- Sparkasse Leipzig
- Volksbank Darmstadt
- Sparda-Bank Hamburg
- ING-DiBa
- Netbank
- 1822direkt
- Comdirect

Keiner der Teilnehmer war vorab über den Test informiert. Die Bewertung erfolgte in zwei Stufen: am 6. und 7. September 2004 führten wir den ersten Test aus, am 2. und 3. November eine Nachkontrolle. Nennenswerte Abweichungen zwischen beiden Tests ergaben sich lediglich bei der Volksbank Darmstadt, die ihr Ergebnis in der Nachkontrolle deutlich verbessern konnte.

4 Testkriterien

Aus den zugrundeliegenden Annahmen ergeben sich drei Gruppen von Bewertungskriterien, die im folgenden näher erläutert sind:

- Technische Gestaltung des Web-Angebots (4 Kriterien);
- Unterstützung von Homebanking-Software als Alternative zum Web (3 Kriterien);
- Kundeninformation und –kommunikation (4 Kriterien).

Um den Test schnell, unabhängig und mit vertretbarem Aufwand ausführen zu können, sind die einzelnen Kriterien so gewählt, dass sie sich ohne Kundenbeziehung zur Bank prüfen lassen.

Bewertungssystem

Die meisten Kriterien sind einfache Ja-Nein-Fragen. In einigen Fällen ist eine feinere Abstufung möglich und erforderlich, die allerdings mit einem subjektiven Urteil verbunden ist. Hierzu gehört zum Beispiel die Frage, wie leicht oder schwer Informationen zu finden sind.

Angesichts der Ziele unseres Tests, der subjektiven Komponente sowie der Schwierigkeit, Einschätzungen zu quantifizieren, haben wir uns für ein einfaches Punktesystem entschieden. Zu jedem Einzelkriterium haben wir einen Punkt vergeben, wenn dieses Kriterium voll erfüllt war. Wo es sinnvoll war, gab es für die teilweise Erfüllung einen halben Punkt. Auf eine feinere Abstufung haben wir verzichtet.

Die technische Gestaltung haben wir doppelt gewichtet. Sie geht also zu etwas mehr als 50 Prozent in das Gesamtergebnis ein. Die maximale Punktzahl bei voller Erfüllung aller Kriterien beträgt 15 Punkte.

Hintergrund

Die Testkriterien und ihre Gewichtung ruhen auf zwei Säulen. Zum einen basieren sie auf einer Grundannahme des Usability Engineering: Die Benutzer von IT-Systemen bilden im Laufe der Zeit gedankliche Modelle über das System, die in der Folge ihr Verhalten bestimmen. Diese Modelle können durch alle wahrnehmbaren Eigenschaften und Verhaltensweisen des Systems beeinflusst werden [Nor02]. Sie stimmen nicht unbedingt mit jenem Modell überein, das der Entwicklung tatsächlich zugrunde lag, sondern können davon abweichen oder unvollständig sein.

Die zweite Grundlage sind Äußerungen von Homebanking-Nutzern in Online-Foren [Hei04a, Hei04c, Bac04, Lid04]. Sie lassen Rückschlüsse auf Verhaltensweisen zum Selbstschutz zu. Hier finden sich beispielsweise Hinweise auf HBCI-fähige Software als Alternative zum Browser sowie auf die schwer nachvollziehbare Adressierung der Websites einiger Banken.

Hinzu kommt die Einschränkung, dass für den vorliegenden Vergleich nur allgemein verfügbare Informationen und öffentlich zugängliche Teile der jeweiligen Web-Angebote berücksichtigt werden sollten.

4.1 Technische Gestaltung

Zur technischen Gestaltung gehören Eigenschaften des jeweiligen Web- und Homebanking-Angebots, denen der Nutzer im täglichen Gebrauch begegnet. Diese Eigenschaften bestimmen die Erwartungen des Nutzers und damit dessen Möglichkeit, Abweichungen und Fälschungen zu erkennen.

Die optische Gestaltung ist als Erkennungsmerkmal für die Echtheit einer Website untauglich. Deshalb kommt jenen technischen Merkmalen eine besondere Bedeutung zu, deren Manipulation zumindest bei gründlicher Prüfung auffällt. Diese Merkmale sind zum einen die Adresse des Web-Angebots, zum anderen der Inhalt der SSL-Zertifikate.

Vier Eigenschaften haben wir bewertet:

- Konsistenz der Adressierung,
- Sichtbarkeit der URL,
- Angaben im SSL-Zertifikat, und
- Zeitpunkt des Verbindungsaufbaus zum gesicherten Server.

Das Ergebnis dieser Kategorie geht doppelt gewichtet in die Gesamtpunktzahl ein.

Konsistente Adressen

Eine konsistente Adressierung über das gesamte Web-Angebot hinweg erleichtert die Bildung einfacher, handhabbarer Regeln. Wir haben einen Punkt vergeben, wenn das Online-Banking-Angebot unter derselben 2nd-Level-Domain geführt wird wie die öffentliche Website der Bank.

Einige Banken haben bereits ihr öffentliches Web-Angebot auf mehrere Adressen verteilt. In diesen Fällen haben wir als Referenz das Angebot für Privatkunden gewählt und einen Punkt vergeben, wenn der dortige Link zum Online-Banking zu einer Website unter derselben 2nd-Level-Domain führte.

Sichtbare Adresse

Damit der Nutzer die Adresse prüfen kann, muss sie sichtbar sein. Wir haben das jeweilige Online-Banking-Interface von der Website aus aufgerufen. Einen Punkt gab es, wenn dabei die URL sichtbar blieb, keinen Punkt hingegen für Fenster, die sich ohne URL- und Menüzeile öffnen.

Bei ausgeblendeter Adresse bleibt dem gewissenhaften Nutzer nur noch das Kontextmenü. Es lässt sich mit der rechten Maustaste öffnen und gestattet den Abruf von Detailinformationen zur angezeigten Seite. Auch wenn die Adresszeile sichtbar ist, kann das Kontextmenü den Zugang zu wichtigen Informationen über die besuchte Seite liefern.

In zwei Fällen fanden wir im Laufe des Tests heraus, dass das Kontextmenü auf der Banking-Seite mittels JavaScript gesperrt war. Geschah dies bei sichtbarer Adresszeile, so haben wir beim Kriterium „URL-Zeile sichtbar" nur einen halben Punkt vergeben. Dies war bei der Volksbank Darmstadt der Fall. Bei der Sparda-Bank Hamburg war gleichzeitig auch die URL-Zeile ausgeblendet. Hier haben wir –1 Punkt vergeben, d.h. vom ungewichteten Ergebnis der Kategorie Technik einen Punkt abgezogen.

SSL-Zertifikat

Alle geprüften Banken setzen für ihre Online-Banking-Angebote das SSL-Protokoll ein. Die dabei übermittelten Sicherheitszertifikate sind die zuverlässigste Form der Echtheitsprüfung. Die Zertifizierungsstelle bescheinigt den Zusammenhang zwischen der besuchten Adresse und der Betreiberorganisation. Wir haben geprüft, ob das Sicherheitszertifikat gültig und auf den Namen der Bank ausgestellt ist. Keinen Punkt gab es, wenn das Zertifikat eine andere Organisation nannte oder ungültig war.

Ungültig sind jene Zertifikate, bei denen ein aktueller Web-Browser in der Default-Konfiguration mit den üblichen vorinstallierten Wurzelzertifikaten eine Fehlermeldung liefert. Ursache könnte zum Beispiel ein abgelaufener Geltungszeitraum sein. In unserem Testfeld kamen solche Fälle jedoch nicht vor.

Login-Seite

Damit der Nutzer das Zertifikat rechtzeitig prüfen kann, bevor er Daten eingibt, muss bereits die Login-Seite über eine gesicherte Verbindung geladen werden. Wir haben einen Punkt vergeben, wenn dies der Fall war.

4.2 Alternative: HBCI

Als grundsätzliche Alternative zum Web-basierten Online-Banking bieten sich spezielle Homebanking-Programme an. Dem Nutzer bieten sie den Vorteil einer einfachen, aber wirksamen Regel zum Schutz vor Phishing: Banking-Daten niemals im Web-Browser verwenden. Wir haben drei Kriterien bewertet:

- ob Banking-Software überhaupt unterstützt wird,
- Unterstützung für das PIN/TAN-Verfahren, sowie
- die Kundeninformation dazu.

Unterstützung für Homebanking-Software

Einen Punkt gab es hier für Banken, die erkennbar neben dem Web-Zugriff auch Homebanking-Software unterstützen. Wir haben dabei nur Informationen auf den jeweiligen Websites berücksichtigt.

Homebanking ohne Chipkarte

Der ursprüngliche HBCI-Standard erfordert beim Nutzer eine Chipkarte und das entsprechende Lesegerät. Diese Anforderung hat sich als eine wesentliche Hürde erwiesen, die viele Nutzer vom Einstieg abhält.

Als Alternative wurde später das PIN/TAN-Verfahren in den HBCI-Standard aufgenommen. Wir haben einen Punkt vergeben, wenn Homebanking-Programme auch im PIN/TAN-Verfahren unterstützt werden. Dies mag auf den ersten Blick paradox erscheinen, sind doch beim Web-basierten Online-Banking gerade PIN und TAN das Ziel der Betrüger. Jedoch zeigt die Erfahrung, dass sich Verfahren auf Smartcard-Basis nur schwer durchsetzen, da sie für die Benutzer mit vielerlei Beschwernissen verbunden sind. Unter diesem Gesichtspunkt betrachtet erscheint Homebanking-Software mit dem PIN/TAN-Verfahren als ein guter Kompromiss zwischen Sicherheitsanforderungen und Benutzerfreundlichkeit. Phishing wird schwerer, ohne dass der Benutzer allzu große Erschwernisse hinnehmen muss.

Ausführliche Information

Eine weitere Einstiegshürde bei den Homebanking-Programmen ist der damit verbundene Installationsaufwand. Unsere Tester haben subjektiv bewertet, wie ausführlich die Banken über die Installation und Konfiguration informieren, und wie leicht diese Informationen zu finden sind.

4.3 Informationen über Phishing

In der dritten Kategorie haben wir bewertet, wie gut die Banken ihre Kunden über das Problem Phishing und die Schutzmöglichkeiten informieren. Zum Thema Sicherheit äußern sich alle Testkandidaten in irgendeiner Form, aber die Hinweise sind nicht immer hilfreich und leicht zu finden. Wir haben vier Kriterien bewertet:

- Allgemeine Hinweise zum Thema Phishing,
- die Angabe konkreter Hilfen zur Echtheitsprüfung,
- die Angabe von Kontaktmöglichkeiten im Zusammenhang mit Phishing, und
- ob relevante Formulare nach der E-Mail-Adresse fragen.

Allgemeine Hinweise

Einen Punkt gab es, wenn Phishing und Schutzmaßnahmen ausführlich erklärt wurde, die Erklärung leicht zu finden war und Links zu spezifischen externen Informationsquellen (zum Beispiel www.antiphsishing.org) enthielt. Einen halben Punkt vergaben wir bei unvollständiger oder schwer auffindbaren Informationen oder wenn Links nur zu allgemeinen Informationsquellen (etwa www.bsi-fuer-buerger.de) führten. Keinen Punkt erhielten Banken, die überhaupt nicht über das Problem informierten, es bei unspezifischen allgemeinen Sicherheitshinweisen beließen oder die Informationen so gut versteckt hatten, dass unsere Tester sie nicht finden konnten.

Konkrete Parameter

Einen weiteren Punkt konnten sich Banken verdienen, indem sie konkrete Parameter angaben, an denen Kunden die Echtheit der Website prüfen können: die URL der Banking-Website und Parameter des Sicherheitszertifikats.

Kontaktmöglichkeit

Im Verdachtsfall sollten Kunden zunächst bei ihrer Bank nachfragen, ob eine Aufforderung zur Dateneingabe legitim ist. Wir haben einen Punkt vergeben, wenn zusammen mit Informationen über Phishing auch die entsprechenden Kontaktinformationen (z.B. Telefonnummern und E-Mail-Adresse) angegeben waren. Keinen Punkt gab es für allgemeine Kontaktinformationen an anderer Stelle.

Datenerhebung

Banken weisen im Zusammenhang mit Phishing immer wieder darauf hin, dass sie keine Aufforderungen zur Eingabe sensibler Daten per E-Mail versenden. Für den Kunden am leichtesten nachzuvollziehen ist es jedoch, wenn der E-Mail-Verkehr – zumindest auf Wunsch – gänzlich unterbleibt. Kunden sollten daher nicht zur Angabe der E-Mail-Adresse gezwungen werden.

Wir haben einen Punkt vergeben, wenn relevante Formulare, etwa für die Kontoeröffnung oder die Anmeldung zum Online-Banking, nicht nach der E-Mail-Adresse fragten. Einen halben Punkt gab es, wenn die Angabe zwar erfragt wurde, aber klar als freiwillig gekennzeichnet war.

5 Ergebnisse

5.1 Übersicht

Tabelle 1 zeigt die Testergebnisse im Überblick. Die Einträge sind absteigend nach der Gesamtpunktzahl geordnet. Maximal waren 15 Punkte erreichbar. Die Kategorie Technik geht doppelt gewichtet in die Gesamtpunktzahl ein, also mit maximal 8 Punkten. Die übrigen Kategorien wurden einfach gewichtet, HBCI mit maximal 3 Punkten und die Kundeninformation mit maximal 4 Punkten. Die Tabelle gibt in den Kategorien bereits die gewichteten Ergebnisse an.

Tabelle 1
Ergebnisse im Überblick

Bank	Technik	HBCI[1]	Info	Summe	Note
Deutsche Bank	8	3	3,5	**14,5**	**sehr gut**
Postbank	8	0	3,5	**11,5**	**befriedigend**
Commerzbank	8	2	1,5	**11,5**	**befriedigend**
Dresdner Bank	7	2	2	**11**	**befriedigend**
ING-DiBa	8	0	2,5	**10,5**	**befriedigend**
Comdirect	8	0	2,5	**10,5**	**befriedigend**
Citibank	8	0	1,5	**9,5**	**ausreichend**
Netbank	4	3	2	**9**	**ausreichend**
Sparkasse Leipzig	4	3	1,5	**8,5**	**ausreichend**
1822direkt	6	1,5	0	**7,5**	**ausreichend**
Volksbank Darmstadt	3	2	2,5[2]	**7,5**	**ausreichend**
Sparda-Bank HH	1	3	3	**7**	**mangelhaft**

Bewertungsschlüssel:
< 7,5: mangelhaft
7,5-9,5: ausreichend
10,0-11,5: befriedigend
12,0-14,0: gut
> 14,0: sehr gut

Die Punktzahlen sind nach dem Schulnotenprinzip auf die Bewertungen „mangelhaft“ bis „sehr gut“ abgebildet. Als mangelhaft gelten Angebote, die weniger als die Hälfte der möglichen Höchstzahl von 15 Punkten erzielten.

Auffällig ist der große Abstand des Testsiegers von den übrigen Teilnehmern. Zugleich zeigt sich am Beispiel der Deutschen Bank, dass die gesetzten Kriterien durchaus erfüllbar sind.

[1] Unterstützung von Homebanking-Software
[2] Frage nach E-Mail-Adresse nicht bewertet, da keine Formulare verfügbar waren.

5.2 Einzelbewertungen

Im folgenden sind die Bewertungen der einzelnen Testteilnehmer aufgeschlüsselt und kommentiert. Die Reihenfolge entspricht der obigen Tabelle.

5.2.1 Deutsche Bank

Webseite: http://www.deutsche-bank.de
Online Banking: https://meine.deutsche-bank.de

Beim Testsieger gibt es wenig zu kritisieren. Das Web-Interface fürs Online-Banking ist unter https://meine.deutsche-bank.de erreichbar, das SSL-Zertifikat ist auf die Bank ausgestellt und die gesicherte Verbindung wird rechtzeitig aufgebaut.

Die Deutsche Bank unterstützt HBCI und bietet ihren Kunden dazu die Software „db dialog" an. Sie unterstützt Smartcards ebenso wie das PIN/TAN-Verfahren. Ausführliche Informationen sind verfügbar.

Ausführlich sind auch die Informationen über Phishing und die Schutzmöglichkeiten. Lediglich für die Frage nach der E-Mail-Adresse in Formularen gab es einen halben Punkt Abzug. Die Angabe war jedoch deutlich als freiwillig gekennzeichnet.

Insgesamt kann die Deutsche Bank als Vorbild dienen, was die von uns geprüften Kriterien betrifft. Ein aufmerksamer Kunde ist hier gut aufgehoben.

Bewertung im Überblick

Tabelle 2 Testergebnis Deutsche Bank

Kriterium	Punkte
Technische Gestaltung	
Konsistente Adressen	1
Sicherheitszertifikat	1
Login-Seite über HTTPS	1
URL-Zeile sichtbar	1
Summe x 2	**8**
HBCI-Unterstützung	
HBCI wird unterstützt	1
PIN/TAN wird unterstützt	1
Detaillierte Informationen	1
Summe	**3**
Kundeninformation	
Informationen über Phishing	1
Konkrete Parameter	1
Kontaktmöglichkeit	1
Frage nach E-Mail-Adresse	0,5
Summe	**3,5**
Ergebnis	**14,5**

5.2.2 Postbank

Webseite: http://www.postbank.de
Online Banking: https://banking.postbank.de

Auch die Postbank erlaubt sich keine technischen Mängel. Ebenfalls gut ist die Kundeninformation; lediglich für die Frage nach der E-Mail-Adresse in Formularen mussten wir einen halben Punkt abziehen. Zwar ist die Angabe im Online-Formular für die Kontoeröffnung freiwillig, die Kennzeichnung erschien uns jedoch undeutlich und verwirrend.

Keinen Punkt gab es für die Postbank jedoch in der Kategorie HBCI. Homebanking-Software wird offenbar nicht unterstützt, so dass Kunden das Web-basierte Homebanking nicht vermeiden können. Mit einem Ergebnis von 11,5 Punkten verfehlt die Postbank nur knapp die Note „gut".

Bewertung im Überblick

Tabelle 3 Testergebnis Postbank

Kriterium	Punkte
Technische Gestaltung	
Konsistente Adressen	1
Sicherheitszertifikat	1
Login-Seite über HTTPS	1
URL-Zeile sichtbar	1
Summe x 2	**8**
HBCI-Unterstützung	
HBCI wird unterstützt	0
PIN/TAN wird unterstützt	0
Detaillierte Informationen	0
Summe	**0**
Kundeninformation	
Informationen über Phishing	1
Konkrete Parameter	1
Kontaktmöglichkeit	1
Frage nach E-Mail-Adresse	0,5
Summe	**3,5**
Ergebnis	**11,5**

5.2.3 Commerzbank

Webseite: https://www.commerzbank.de
Online Banking: https://portal04.commerzbanking.de

Alle technischen Testkriterien sind bei der Commerzbank erfüllt. Neben Web-basiertem Online-Banking unterstützt die Commerzbank auch HBCI für Homebanking-Software, offenbar aber nur in der Variante mit Chipkarte. Detaillierte Informationen über die nötige Software und ihre Konfiguration stehen unter http://www.hbci.commerzbank.de/ zur Verfügung.

Die Sicherheitshinweise auf www.commerzbanking.de gehen auf das Problem Phishing ein. Als externe Informationsquelle ist lediglich www.bsi-fuer-buerger.de angegeben, Hinweise auf Seiten zum Thema Phishing fehlen. Auch eine Hotline für Rückfragen und Verdachtsfälle ist angegeben. Dafür gab es insgesamt 1½ Punkte. Konkrete Parameter, an denen sich die Echtheit der Banking-Site prüfen lässt, fehlen jedoch. Zwar sind die Adressen der Website angegeben, jedoch keine Hinweise zur Zertifikatsprüfung. In Formularen wird nach der E-Mail-Adresse gefragt. Wie schon bei der Postbank fehlt auch hier nur ein halber Punkt zur Note „gut".

Bewertung im Überblick

Tabelle 4 Testergebnis Commerzbank

Kriterium		Punkte
Technische Gestaltung		
	Konsistente Adressen	1
	Sicherheitszertifikat	1
	Login-Seite über HTTPS	1
	URL-Zeile sichtbar	1
	Summe x 2	**8**
HBCI-Unterstützung		
	HBCI wird unterstützt	1
	PIN/TAN wird unterstützt	0
	Detaillierte Informationen	1
	Summe	**2**
Kundeninformation		
	Informationen über Phishing	0,5
	Konkrete Parameter	0
	Kontaktmöglichkeit	1
	Frage nach E-Mail-Adresse	0
	Summe	**1,5**
	Ergebnis	**11,5**

5.2.4 Dresdner Bank

Webseite: http://www.dresdner-bank.de
Online Banking: https://www.dresdner-privat.de

Die Dresdner Bank leistet sich eine kleine Schwäche bei der Technik: das Sicherheitszertifikat ist auf die „AGIS Allianz Dresdner Informationssysteme GmbH" ausgestellt. Da der Name der Bank immerhin noch erkennbar ist, gab es hier einen halben Punkt. Ansonsten ist auf technischer Seite nichts zu kritisieren.

Homebanking-Software wird auch bei der Dresdner Bank unterstützt, aber nur mit Chipkarte. Informationen zur Konfiguration und Nutzung erscheinen uns nicht vollständig und waren zudem schwer zu finden. Insgesamt erhält die Dresdner Bank daher zwei Punkte in der Kategorie HBCI.

Zum Testzeitpunkt machte ein Warnhinweis die Kunden auf die Phishing-Gefahr aufmerksam. Er war allerdings nicht besonders umfangreich. Auch fehlten Links zu externen Informationsquellen über das Thema Phishing. Konkrete Parameter für die Echtheitsprüfung waren nicht angegeben.

Eine unmittelbare Kontaktmöglichkeit ist im Zusammenhang mit der Phishing-Warnung nicht angegeben, aber ein Verweis auf eine Übersicht der allgemeinen Hotlines. Dafür vergaben wir einen halben Punkt. Erfreulich ist, dass die geprüften Formulare nicht nach der E-Mail-Adresse fragen.

Insgesamt wirken die Informationen bei der Dresdner Bank recht unübersichtlich. Die Auswirkungen konnten wir in unserem Schnelltest nicht überprüfen. Eine lesefreundliche Gestaltung mit weniger Fettschrift scheint jedoch empfehlenswert.

Bewertung im Überblick

Tabelle 5 Testergebnis Dresdner Bank

Kriterium	Punkte
Technische Gestaltung	
Konsistente Adressen	1
Sicherheitszertifikat	0,5
Login-Seite über HTTPS	1
URL-Zeile sichtbar	1
Summe x 2	**7**
HBCI-Unterstützung	
HBCI wird unterstützt	1
PIN/TAN wird unterstützt	0
Detaillierte Informationen	1
Summe	**2**
Kundeninformation	
Informationen über Phishing	0,5
Konkrete Parameter	0
Kontaktmöglichkeit	0,5
Frage nach E-Mail-Adresse	1
Summe	**2**
Ergebnis	**11**

5.2.5 Allgemeine Deutsche Direktbank (ING-DiBA)

Webseite: http://www.ing-diba.de
Online Banking: https://banking.diba.de

Die ING-DiBa, Allgemeine Deutsche Direktbank AG ist die bestplatzierte Direktbank in diesem Test. Auch hier waren keine technischen Mängel zu beanstanden. Keine Punkte gab es hingegen in der Kategorie HBCI. Offenbar unterstützt die ING-DiBa nur den Web-Zugriff.

In der Kategorie Kundeninformation verlor die ING-DiBa einen Punkt für das Fehlen konkreter Parameter zur Echtheitsprüfung. Formulare fragen nach der E-Mail-Adresse fragen. Die Angabe ist aber freiwillig.

Bewertung im Überblick

Tabelle 6 Testergebnis ING-DiBa

Kriterium		Punkte
Technische Gestaltung		
	Konsistente Adressen	1
	Sicherheitszertifikat	1
	Login-Seite über HTTPS	1
	URL-Zeile sichtbar	1
	Summe x 2	**8**
HBCI-Unterstützung		
	HBCI wird unterstützt	0
	PIN/TAN wird unterstützt	0
	Detaillierte Informationen	0
	Summe	**0**
Kundeninformation		
	Informationen über Phishing	1
	Konkrete Parameter	0
	Kontaktmöglichkeit	1
	Frage nach E-Mail-Adresse	0,5
	Summe	**2,5**
	Ergebnis	**10,5**

5.2.6 Comdirect

Webseite: http://www.comdirect.de
Online Banking: https://brokerage.comdirect.de

Ähnlich wie die ING-DiBa hat auch Comdirect im Rahmen unserer Testkriterien die Web-Technik im Griff und unterstützt keine Homebanking-Software. Die Kundeninformationen über Phishing enthalten Verweise auf weiterführende Informationsquellen, allerdings nicht speziell zum Thema Phishing. Ebenso ist eine Kontaktmöglichkeit angegeben. Zur Echtheitsprüfung sind lediglich Adressen der Banking-Website sowie der Aussteller des Sicherheitszertifikats angegeben, nicht jedoch weitere Zertifikatsparameter. Formulare fragen nach der E-Mail-Adresse, die Angabe ist aber freiwillig.

Bewertung im Überblick

Tabelle 7 Testergebnis Comdirect

Kriterium		Punkte
Technische Gestaltung		
	Konsistente Adressen	1
	Sicherheitszertifikat	1
	Login-Seite über HTTPS	1
	URL-Zeile sichtbar	1
	Summe x 2	**8**
HBCI-Unterstützung		
	HBCI wird unterstützt	0
	PIN/TAN wird unterstützt	0
	Detaillierte Informationen	0
	Summe	**0**
Kundeninformation		
	Informationen über Phishing	0,5
	Konkrete Parameter	0,5
	Kontaktmöglichkeit	1
	Frage nach E-Mail-Adresse	0,5
	Summe	**2,5**
	Ergebnis	**10,5**

5.2.7 Citibank

Webseite: http://www.citibank.de
Online Banking: https://cipehb7.cdg.citibank.de

Auch die Citibank setzt ganz auf Web-basiertes Online-Banking. Homebanking-Software wird nicht unterstützt. Die Technik für den Web-Zugang zeigt im Rahmen unserer Testkriterien keine Schwächen.

Die Citibank informiert ihre Kunden gut über Phishing, allerdings fehlten Verweise auf externe Informationsquellen zum Thema. Konkrete Parameter für die Echtheitsprüfung fanden wir ebenfalls nicht. Online verfügbare Formulare fragen nach der E-Mail-Adresse; die Angabe ist nicht als freiwillig gekennzeichnet.

Bewertung im Überblick

Tabelle 8 Testergebnis Citibank

Kriterium		Punkte
Technische Gestaltung		
	Konsistente Adressen	1
	Sicherheitszertifikat	1
	Login-Seite über HTTPS	1
	URL-Zeile sichtbar	1
	Summe x 2	**8**
HBCI-Unterstützung		
	HBCI wird unterstützt	0
	PIN/TAN wird unterstützt	0
	Detaillierte Informationen	0
	Summe	**0**
Kundeninformation		
	Informationen über Phishing	0,5
	Konkrete Parameter	0
	Kontaktmöglichkeit	1
	Frage nach E-Mail-Adresse	0
	Summe	**1,5**
	Ergebnis	**9,5**

5.2.8 Netbank

Webseite: http://www.netbank.de
Online Banking: https://www.netbank-money.de

In einem inkonsistenten Bild präsentiert sich die Netbank ihren Nutzern. Beim Aufruf der Online-Banking-Seiten wechselt die Adresse unmotiviert von netbank.de zu netbank-money.de. Im Sicherheitszertifikat steht als Betreiber die Sparda-Datenverarbeitung eG. Den Zusammenhang zwischen Betreiber und Bank können wohl nur Branchen-Insider nachvollziehen. Hier haben es Phishing-Betrüger also leicht, weil bereits der Normalbetrieb Merkmale eines Phishing-Angriffs trägt..

An der Unterstützung von Homebanking-Programmen als Alternative zum Web hingegen gibt es nichts auszusetzen. Alle Kriterien sind erfüllt.

Auch Sicherheitshinweise zum Thema Phishing stehen für Kunden bereit. Sie enthalten die Adresse und die Zertifikatsparameter, die für die Echtheitsprüfung der Website erforderlich sind.

Als Kontaktmöglichkeit fanden wir Web-Formulare, in die der Nutzer seine Nachricht eintragen kann, nach längerem Suchen auch Telefonnummern, unter denen sich jedoch nur ein sprechender Computer meldet. In Formularen gehört die E-Mail-Adresse zu den Pflichtfeldern, um deren Ausfüllung der Kunde nicht herumkommt.

Bewertung im Überblick

Tabelle 9 Testergebnis Netbank

Kriterium		Punkte
Technische Gestaltung		
	Konsistente Adressen	0
	Sicherheitszertifikat	0
	Login-Seite über HTTPS	1
	URL-Zeile sichtbar	1
	Summe x 2	**4**
HBCI-Unterstützung		
	HBCI wird unterstützt	1
	PIN/TAN wird unterstützt	1
	Detaillierte Informationen	1
	Summe	**3**
Kundeninformation		
	Informationen über Phishing	1
	Konkrete Parameter	1
	Kontaktmöglichkeit	0
	Frage nach E-Mail-Adresse	0
	Summe	**2**
	Ergebnis	**9**

5.2.9 Sparkasse Leipzig

Webseite: http://www.sparkasse-leipzig.de
Online Banking: https://ww2.homebanking-sachsen.de

Aufgrund ihrer regionalen Organisationen konnten die Sparkassen nicht umfassend getestet werden. Als Vertreter wurde daher die Sparkasse Leipzig ausgewählt.

Hier fallen zwei technische Schwächen ins Auge. Zum einen wird die Website für das Online-Banking unter der Adresse ww2.homebanking-sachsen.de angeboten. Sie steht in keinem erkennbaren Zusammenhang mit der Sparkasse Leipzig oder der Sparkassenorganisation. Zum anderen stellt auch das Sicherheitszertifikat keinen nachvollziehbaren Zusammenhang zwischen der Sparkasse und ihrem Online-Banking-Angebot her. Als Betreiber der Banking-Website ist eine FinanzIT GmbH aus Hannover angegeben. Phishing-Betrügern dürfte es hier leicht fallen, gefälschte Angaben echt wirken zu lassen – bereits das Original sieht aus wie ein schlechter Betrugsversuch.

Lobenswert ist, dass die Sparkasse Homebanking-Software in vollem Umfang unterstützt. Die Nutzung ist sowohl mit Chipkarte als auch im PIN/TAN-Verfahren möglich. Dazu stehen ausführliche Informationen bereit.

Auch Informationen über Phishing stellt die Sparkasse Leipzig bereit. Sie sind allerdings in der Rubrik „Tipps“ versteckt und enthalten keine Verweise auf externe Informationsquellen. Dafür gab es einen halben Punkt.

Einen halben Punkt vergaben wir auch für konkrete Parameter. Die Sparkasse gibt ausschließlich den digitalen Fingerabdruck (Fingerprint) des Zertifikats an. Er genügt zwar zur eindeutigen Prüfung, ist aber eine für Benutzer nur schwer handhabbare Zahlenkolonne.

Einen halben Punkt gab es schließlich auch für die angegebenen Kontaktmöglichkeiten. Die Aufforderung, sich bei Phishing-Verdacht oder Fragen an die Sparkasse zu wenden, enthält einen Link zu einem E-Mail-Formular. Dieses Formular verlangt eine Reihe persönlicher Informationen, lässt aber wenig Raum für die eigentliche Nachricht. Das ist abschreckend. Die Telefonnummer einer Hotline findet sich nur in einem Kasten, der auf allen Seiten neben dem primären Inhalt erscheint.

Bewertung im Überblick

Tabelle 10 Testergebnis Sparkasse Leipzig

Kriterium	Punkte
Technische Gestaltung	
Konsistente Adressen	0
Sicherheitszertifikat	0
Login-Seite über HTTPS	1
URL-Zeile sichtbar	1
Summe x 2	**4**
HBCI-Unterstützung	
HBCI wird unterstützt	1
PIN/TAN wird unterstützt	1
Detaillierte Informationen	1
Summe	**3**
Kundeninformation	
Informationen über Phishing	0,5
Konkrete Parameter	0,5
Kontaktmöglichkeit	0,5
Frage nach E-Mail-Adresse	0
Summe	**1,5**
Ergebnis	**8,5**

5.2.10 1822direkt

Webseite: http://www.1822direkt.com
Online Banking: https://banking.1822direkt.com

Bei der 1822direkt öffnet sich die Banking-Anwendung in einem neuen Fenster ohne sichtbare Adresszeile. In der Kategorie Technik erreichte sie daher nur drei Punkte.

Homebanking-Software nach dem HBCI-Standard wird unterstützt. Die Nutzung ist jedoch nur mit Chipkarte möglich, nicht im PIN/TAN-Verfahren. Die verfügbaren Informationen etwa zur nötigen Ausstattung und zur Konfigurati-

on erschienen uns lückenhaft und unvollständig. Insgesamt deshalb nur 1,5 Punkte in der Kategorie HBCI.

In der Kategorie Kundeninformation erzielte die 1822direkt als einzige im Test null Punkte. Wir fanden zwar verschiedene Sicherheitshinweise, aber keine deutliche Erklärung, wie Phishing-Angriffe ablaufen und wie sich Kunden schützen können. Hinzu kommt, dass Formulare die E-Mail-Adresse erfragen.

Bewertung im Überblick

Tabelle 11 Testergebnis 1822direkt

Kriterium	Punkte
Technische Gestaltung	
Konsistente Adressen	1
Sicherheitszertifikat	1
Login-Seite über HTTPS	1
URL-Zeile sichtbar	0
Summe x 2	**6**
HBCI-Unterstützung	
HBCI wird unterstützt	1
PIN/TAN wird unterstützt	0
Detaillierte Informationen	0,5
Summe	**1,5**
Kundeninformation	
Informationen über Phishing	0
Konkrete Parameter	0
Kontaktmöglichkeit	0
Frage nach E-Mail-Adresse	0
Summe	**0**
Ergebnis	**7,5**

5.2.11 Volksbank Darmstadt

Webseite: http://www.voba-darmstadt.de
Online Banking: https://www.vr-networld-ebanking.de

Die Volksbank Darmstadt zeigt Schwächen auf dem Gebiet der technischen Gestaltung. Das Online-Banking-System wird unter einer Adresse angeboten, die keine nachvollziehbare Verbindung zu jener der Bank hat. Das Sicherheitszertifikat ist auf die FIDUCIA AG ausgestellt, das gemeinsame Rechenzentrum der Genossenschaftsbanken. Ähnlich wie bei der Sparda-Bank Hamburg ist das Kontextmenü des Browsers deaktiviert; bei der Volksbank bleibt allerdings die URL-Zeile sichtbar, so dass dieser Kontrollverlust weniger gefährlich erscheint.

Banking-Software nach dem HBCI-Standard wird unterstützt, sowohl im klassischen HBCI-Verfahren mit Chipkarte als auch im PIN/TAN-Verfahren. Die Informationen dazu fallen allerdings dürftig aus.

Die Kundeninformation hat sich im Laufe unseres Tests deutlich verbessert. Waren anfangs kaum Informationen zu finden, so sind nun Parameter für die Zertifikatsprüfung sowie Ansprechpartner mit Telefonnummer und E-Mail-Adresse angegeben. Allerdings sind die Sicherheitshinweise sehr knapp gehalten und verweisen auch nicht auf weiterführende Informationen.

Relevante Formulare (Kontoeröffnung, Anmeldung zum Online-Banking) fanden wir nicht, so dass die Bewertung in diesem Punkt offen bleibt. Auf der Benotung mit „ausreichend" hat dieser Punkt keinen Einfluss.

Bewertung im Überblick

Tabelle 12 Testergebnis Volksbank Darmstadt

Kriterium	Punkte
Technische Gestaltung	
Konsistente Adressen	0
Sicherheitszertifikat	0
Login-Seite über HTTPS	1
URL-Zeile sichtbar	0,5[3]
Summe x 2	**3**
HBCI-Unterstützung	
HBCI wird unterstützt	1
PIN/TAN wird unterstützt	1
Detaillierte Informationen	0
Summe	**2**
Kundeninformation	
Informationen über Phishing	0,5
Konkrete Parameter	1
Kontaktmöglichkeit	1
Frage nach E-Mail-Adresse	–[4]
Summe	**2,5**
Ergebnis	**7,5**

5.2.12 Sparda-Bank Hamburg

Webseite: http://www.sparda-hh.de
Online Banking: https://www.bankingonline.de

Die Sparda-Bank Hamburg bildet das Schlusslicht im Test. Der Grund ist mangelhafte Technik. Die Online-Banking-Seiten werden unter der nichtssagenden Adresse www.bankingonline.de angeboten. Das zugehörige Sicherheitszertifikat gibt die Sparda-Datenverarbeitung eG als Betreiber an; diese teilweise Übereinstimmung mit dem Namen der Bank haben wir wie bei anderen auch mit einem halben Punkt bewertet.

[3] Punktabzug für deaktiviertes Kontextmenü
[4] Nicht gewertet, da keine relevanten Formulare online verfügbar waren.

Immerhin wird die gesicherte Verbindung rechtzeitig aufgebaut – dieses Kriterium ist bei allen Banken im Test erfüllt. Einen Minuspunkt gibt es freilich im folgenden Kriterium: das Kontextmenü des Web-Browsers funktioniert nicht. Vermutlich wird der Klick mit der rechten Maustaste mittels JavaScript abgefangen. Die Adresse der Seiten zu prüfen wird damit nahezu unmöglich. Abweichend vom übrigen Bewertungsschema zogen wir deshalb in der Kategorie Technik einen Punkt ab.

Die HBCI-Unterstützung für Homebanking-Software hingegen erfüllte alle Kriterien. Auch an der Kundeninformation gibt es wenig auszusetzen. Lediglich ein Punkt fehlt hier aufgrund der Frage nach der E-Mail-Adresse in Formularen.

Bewertung im Überblick

Tabelle 13 Testergebnis Sparda-Bank Hamburg

Kriterium	Punkte
Technische Gestaltung	
Konsistente Adressen	0
Sicherheitszertifikat	0,5
Login-Seite über HTTPS	1
URL-Zeile sichtbar	-1[5]
Summe x 2	**1**
HBCI-Unterstützung	
HBCI wird unterstützt	1
PIN/TAN wird unterstützt	1
Detaillierte Informationen	1
Summe	**3**
Kundeninformation	
Informationen über Phishing	1
Konkrete Parameter	1
Kontaktmöglichkeit	1
Frage nach E-Mail-Adresse	0
Summe	**3**
Ergebnis	**7**

[5] Punktabzug für deaktiviertes Kontextmenü

6 Fazit und Ausblick

Das Testergebnis zeigt, dass viele Banken Nachholbedarf haben, was den Schutz ihrer Kunden vor Phishing betrifft. Zwar umfasst der hier vorgestellte Test nicht alle relevanten Faktoren. Er stützt sich nur auf allgemein zugängliche Informationen und konzentriert sich auf Hilfestellungen für die Benutzer von Banking-Angeboten.

Doch die Auswahl ist keineswegs willkürlich. Unsere Kriterien zielen auf die Schnittstelle zum Kunden, dessen Mitwirkung zum Schutz vor Phishing unabdingbar ist. Gleichzeitig sind sie eine Indikator für das Sicherheitsbewusstsein und die Sicherheitskultur der getesteten Institute. Zu einem umfassenden Sicherheitskonzept gehört immer auch die Berücksichtigung unzähliger Details, an denen die Sicherheit in der Praxis scheitern kann. Der Kriterienkatalog der vorliegenden Studie stützt sich auf eine Auswahl solcher Details.

Die Mehrzahl der getesteten Banken muss sich mit den Noten „befriedigend" oder „ausreichend" begnügen. Keine einzige erreichte „gut" und nur eine erfüllte die Testkriterien vorbildlich. Angesichts der großen Rolle, die Vertrauen und Sicherheit gerade in dieser Branche spielen, darf man bessere Ergebnisse erwarten. Andernfalls drängt sich der Eindruck auf, dass Sicherheitsmaßnahmen nur pro forma ergriffen werden.

Etwas erfreulicher als das Gesamtergebnis ist die Wertung in der Kategorie Technik. Die Hälfte der untersuchten Websites zeigte hier keine Schwächen, zwei weitere mit 3 oder mehr Punkten (ungewichtet) noch ein akzeptables Ergebnis. Mit schlechten Ergebnissen fallen in dieser Kategorie vor allem die regional organisierten Sparkassen und Genossenschaftsbanken auf. Diese Organisationsform macht es offenbar schwer, sich den Kunden in einem konsistenten Bild zu präsentieren und ihnen die erforderlichen Informationen und Sicherheitshinweise in angemessenem Umfang zur Verfügung zu stellen. Für grobe Patzer wie unsichtbar gemachte Adressen oder gar deaktivierte Browserfunktionen ist die Organisationsform freilich keine Entschuldigung.

Weiter fällt auf, dass – zumindest nach unseren Testkriterien – die klassischen Großbanken die Nase vorn haben. Die Erwartung, bei den Direktbanken die größte Internet-Kompetenz vorzufinden, hat sich damit nicht erfüllt. Das ist erstaunlich, stellt doch das Internet gerade hier den primären Kommunikationskanal zum Kunden dar.

Die Forschung zur Klasse der semantischen Angriffe, zu denen das Phishing gehört, steckt noch in den Kinderschuhen. Abschließend soll deshalb ein Ausblick gegeben werden, welche Fragen für die effektive Bekämpfung von Phishing-Angriffen zu klären sind.

6.1 Bewertungskriterien

Die vorliegende Untersuchung stützt sich auf einen ad hoc aufgestellten Kriterienkatalog. Sie geht von einem idealisierten Benutzermodell aus. Notwendig zur Verbesserung der Sicherheit sind schärfere Kriterien, die gute Vorhersagen über die Gefahr eines erfolgreichen Phishing-Angriffs erlauben.

Nicht überprüft haben wir zum Beispiel:

- Wie erfasste E-Mail-Adressen von den betreffenden Banken verwendet werden. Regelmäßige Aussendungen an Kunden mit Links, die auf Login-Seiten verweisen, können die Erkennung von Phishing-Angriffen erschweren, da sie die Erwartungen der Kunden prägen [BlSch04].
- Weitere technische Kriterien, etwa den Einsatz von Frames oder die Anfälligkeit für Cross-Site-Scripting. Technische Sicherheitslücken in den Web-Angeboten wie auch in Web-Browsern können Phishing-Angriffe erleichtern. Sie sind jedoch keine unabdingbare Voraussetzung für deren Erfolg [Net04].
- Andere Schwachstellen und Angriffsmethoden. Phishing ist nicht die einzige Bedrohung für die Sicherheit elektronischer Geschäftsprozesse. Maßnahmen gegen Phishing müssen auch danach beurteilt werden, welche Auswirkungen sie hinsichtlich anderer Sicherheitskriterien haben.

Phishing ist eine vielschichtige Bedrohung. Effektive Schutzmaßnahmen erfordern handhabbare Kriterienkataloge insbesondere auch für die Entwickler von Web-Angeboten und –Anwendungen, sowie geeignete Untersuchungsmethoden.

Vorbild Usability Engineering?

Ein Vorbild könnte das Usability Engineering liefern. Hier wurden bereits seit vielen Jahren Kriterien sowie Untersuchungs- und Entwicklungsmethoden geschaffen und verbessert, mit denen sich Systeme und Anwendungen leichter benutzbar machen lassen. Offen ist noch, inwieweit sich diese Ergebnisse auf die Entwicklung sicherer Systeme übertragen lassen. Zwar sind die Probleme verwandt. In beiden Fällen geht es um die Interaktion zwischen Mensch und Technik. Doch die Zielrichtung unterscheidet sich deutlich. Bloße Benutzerfreundlichkeit reicht nicht aus, um Anwender vor Phishing und anderen semantischen Angriffen zu schützen. Mit den Sicherheitserwägungen kommt die zusätzliche Forderung nach korrektem Verhalten des Benutzers hinzu, die im herkömmlichen Usability Engineering keine Rolle spielt.

Bewertung der Sicherheitskultur

Erweitert man den Fokus der Untersuchung, so dass neben dem Webauftritt auch andere Kanäle der Kundenkommunikation sowie weitere Kriterien berücksichtigt werden, so ergibt sich vielleicht ein handhabbarer Test für die Sicherheitskultur eines Unternehmens. Ein solcher Test könnte, ähnlich den klassischen Penetrationstests, darauf zielen, Schwächen im Sicherheitsmanagement und seiner Umsetzung aufzudecken. Im Gegensatz zum Einsatz von Tigerteams liegt der Schwerpunkt dabei aber nicht beim Schutz der Infrastruktur vor uner-

laubtem Zugriff, sondern auf der Sicherheit jener Geschäftsprozesse, in denen das Unternehmen mit Dritten interagiert. Das kann Kundenkontakte ebenso betreffen wie die Kooperation mit Partnern oder Zulieferern.

6.2 Benutzermodelle

Phishing und andere semantische Angriffe zielen auf die Benutzer von IT-Systemen. Wo sie sich mit technischen Mitteln nicht abwehren lassen, bleibt nur die Aufmerksamkeit und das Misstrauen des Benutzers als letztes Mittel. Das wirft eine Reihe von Fragen auf:

Welche Benutzer sind besonders anfällig für Phishing? Benutzer lassen sich im Verhältnis zum benutzten System nach verschiedenen Kriterien klassifizieren, zum Beispiel nach ihrer Erfahrung im Umgang mit dem System und mit Computern schlechthin. Bei regelmäßiger Nutzung bilden sich Gewohnheiten und Erwartungen heraus. Sie können einerseits dazu führen, dass Abweichungen leichter erkannt und misstrauisch bewertet werden. Andererseits ist aber auch denkbar, dass die – adaptiven – Angreifer gerade mutmaßliche Erwartungen und Gewohnheiten der Benutzer ausnutzen und ihr Vorgehen darauf abstimmen.

Welche Bedeutung hat der Kontext einer Benutzerinteraktion? Erwartungen des Benutzers können sich auch aus Sachverhalten abseits der unmittelbaren Interaktion mit einem System ergeben. Macht zum Beispiel die Bitte um Datenaktualisierung immer noch misstrauisch, wenn der Benutzer kurz zuvor eine neue Kreditkarte erhalten hat? Anwender können heute kaum noch überblicken, welchen Weg ihre Daten hinter den Kulissen nehmen. Dies kann zu falschen gedanklichen Modellen führen, die eine mögliche Grundlage für Phishing und andere semantische Angriffe bilden.

Welche Warnungen sind nützlich? Eine leicht zu realisierende Schutzmaßnahme sind Warnungen. Sie können allgemein gehalten sein, etwa in Form von Sicherheitshinweisen, oder sich spezifisch auf bestimmte Situationen und Sachverhalten beziehen, wie zum Beispiel Popup-Fenster oder Zustandsanzeigen des Web-Browsers. Die Wirksamkeit ist in beiden Fällen fraglich. Sicherheitshinweise und anderes explizites Wissen werden nicht notwendig in jederzeit verfügbares Handlungswissen umgesetzt.

Selbst situationsbezogene Warnungen können vom Benutzer übergangen werden, wenn sie als bloßes Hindernis beim Erreichen eines als richtig angenommenen Zieles eingestuft werden. Ungeeignete Warnmechanismen und häufige Fehlalarme können zur Bildung entsprechender Gewohnheiten führen. Eine einmal gebildete Plausibilitätsvermutung des Benutzers lässt sich durch ungeeignete und zu spät eingreifende Warnmechanismen oft nicht mehr erschüttern.

Bild 3 zeigt eine Kundeninformation, die zusammen mit einer Kreditkartenabrechnung vom Kontoauszugdrucker einer Sparkasse ausgegeben wurde. Gewiss sind solche Warnungen gut gemeint, doch sind sie auch nützlich? Erinnern sich die Kunden im entscheidenden Moment daran? Genügt ein einmaliger Hinweis? Wie leicht oder wie schwer ist es für die Betrüger, sich mit einem gut

konstruierten Vorwand dennoch das Vertrauen der Kunden zu erschleichen? Können die Täter solche Hinweise gar ausnutzen, etwa indem sie durch konkrete Bezugnahme darauf Authentizität vortäuschen?

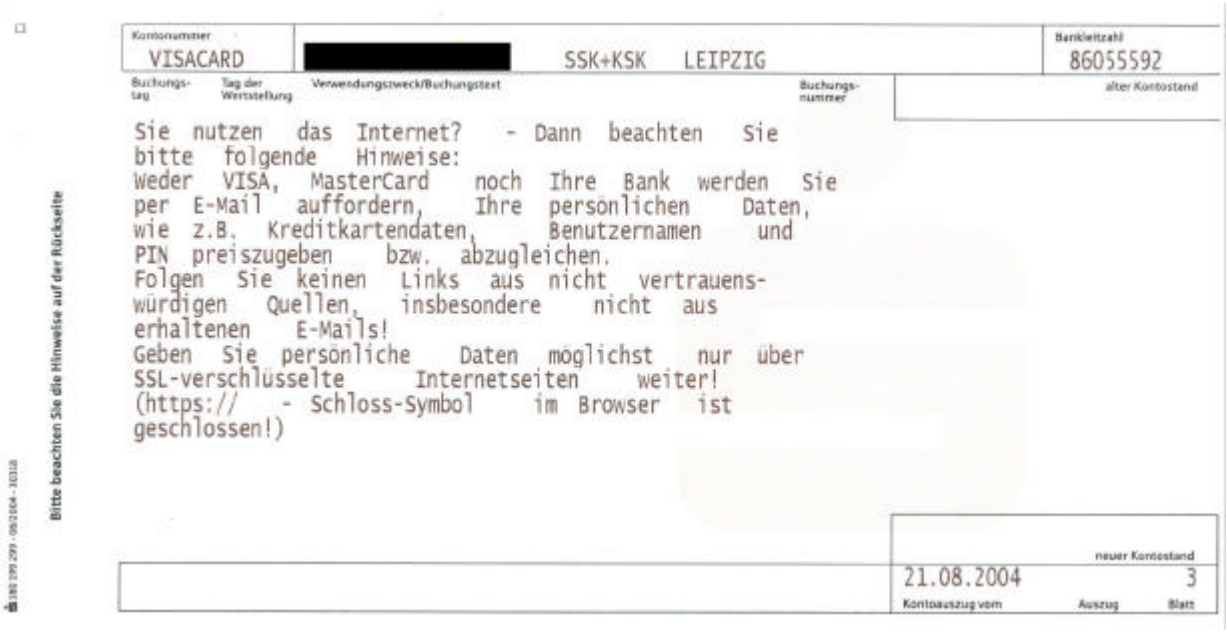

Kontonummer
VISACARD
[redacted] SSK+KSK LEIPZIG
Bankleitzahl
86055592
Buchungs-tag
Tag der Wertstellung
Verwendungszweck/Buchungstext
Buchungs-nummer
alter Kontostand
Sie nutzen das Internet? - Dann beachten Sie bitte folgende Hinweise:
Weder VISA, MasterCard noch Ihre Bank werden Sie per E-Mail auffordern, Ihre persönlichen Daten, wie z.B. Kreditkartendaten, Benutzernamen und PIN preiszugeben bzw. abzugleichen.
Folgen Sie keinen Links aus nicht vertrauenswürdigen Quellen, insbesondere nicht aus erhaltenen E-Mails!
Geben Sie persönliche Daten möglichst nur über SSL-verschlüsselte Internetseiten weiter!
(https:// - Schloss-Symbol im Browser ist geschlossen!)
Bitte beachten Sie die Hinweise auf der Rückseite
neuer Kontostand
21.08.2004
3
Kontoauszug vom
Auszug
Blatt

Bild 3 Phishing-Warnung als Anlage zur Kreditkartenabrechnung

6.3 Systemarchitektur

Zwar zielen semantische Angriffe auf die Benutzer eines Systems. Dazu werden jedoch Eigenschaften dieses Systems ausgenutzt. Neben den Sicherheitsmechanismen sind hier Fragen der Systemarchitektur von Bedeutung.

Manipulierbarkeit der Präsentation. Das grundlegende technische Problem, das von den Phishing-Betrügern ausgenutzt wird, ist die leichte Manipulierbarkeit der Präsentation sowohl von E-Mail-Nachrichten als auch von Web-Inhalten. Sie reicht so weit, dass sogar sicherheitsrelevante Anzeigen des Web-Browsers ersetzt oder beeinflusst werden können. Hinzu kommt, dass jeder ohne größeren Aufwand als Sender beziehungsweise Anbieter auftreten kann. Das macht es den Betrügern leicht, eine Echtheits- und Legitimitätsillusion zu erzeugen.

Aus diesem Grunde haben wir auch die Unterstützung von Homebanking-Software in einer eigenen Kategorie bewertet. Sie bieten – zumindest hinsichtlich der Phishing-Gefahr – weitaus weniger Manipulationsmöglichkeiten, da die Präsentation, anders als im World Wide Web, von einer lokal beim Benutzer installierten Komponente gesteuert wird.

Vertrauen in den Benutzer. Benutzern wird in der IT-Sicherheit häufig uneingeschränkt vertraut. Sie entscheiden jedoch mit ihrem Verhalten über die Wirksamkeit oder Unwirksamkeit von Sicherheitsmechanismen. Dabei machen sie Fehler. Angemessene Sicherheitstechnik muss diese Fehlerquelle berücksichtigen [WhiTy99]. Dies kann etwa geschehen, indem dem Benutzer Eingriffs- und

Handlungsmöglichkeiten genommen werden. Der umstrittene Ansatz des „Trusted Computing“ ist ein Beispiel hierfür. Eine andere Möglichkeit besteht in der Einbettung von Fallback-Mechanismen, die ein Versagen der primären Sicherheitstechnik abfangen können.

Korrekte Modellbildung unterstützen. In der wiederholten Interaktion mit einem System bilden dessen Benutzer unwillkürlich gedankliche Modelle über dessen Funktionsweise. Diese Modelle bestimmen das Verhalten des Benutzers, seine Erwartungen und seine Reaktionen auf unvorhergesehene Zustände oder Vorgänge. Sie spielen deshalb besonders beim Schutz vor Phishing eine große Rolle. So nutzen Phishing-Betrüger zum Beispiel oft mehrere Browserfenster: In einem Popup-Fenster wird die Phishing-Seite angezeigt, während im Hintergrund ein zweites Fenster die Original-Website der Bank lädt. Dass zwischen diesen gleichzeitigen Vorgängen keine Verbindung besteht, wird den Benutzern im User Interface nicht vermittelt.

Kaum untersucht ist bisher, wie sich die Bildung angemessener Modelle in Hinblick auf sicherheitsrelevante Verhaltensweisen unterstützen lässt. Sicherheit ist ein Sekundärziel; die gängigen Methoden des Usability Engineering konzentrieren sich jedoch auf die primären Ausgaben und Ziele der Benutzer. Zukünftig sind verfeinerte Instrumente erforderlich, die auch Nebenziele wie eben Sicherheit erfassen und modellieren können.

Systemkomplexität und Interaktion zwischen Komponenten. Die derzeitigen Phishing-Angriffe nutzen nicht zuletzt die enge Integration der Dienste E-Mail und World Wide Web aus. Den Opfern wird ein Ziel – Login und Dateneingabe aus irgendeinem Grund – vorgegeben, und der Weg zu diesem Ziel geebnet: die E-Mail enthält gleich den passenden Link. Ohne die Möglichkeit, potentielle Opfer mittels massenhaft versandter E-Mail anzusprechen, wäre Phishing wohl kein großes Problem.

Hier zeigt sich, dass auch solche Dienste und Systeme in Sicherheitserwägungen einbezogen werden müssen, die außerhalb des unmittelbaren Einflussbereichs eines Anbieters liegen. Eine besondere Schwierigkeit liegt darin, dass sich die unerwünschte Interaktion zwischen Diensten oder Systemen unter Umständen erst dann zeigt, wenn sie vom Angreifer bewusst herbeigeführt wird.

Sicherheitsfunktionen und –werkzeuge. Etablierte Systeme wie das World Wide Web und andere Internet-Dienste erlauben kaum kurzfristige grundlegende Modifikationen ihrer Architektur. Neben grundsätzlichen Erwägungen bei Neuentwicklungen ist deshalb auch Sicherheitstechnik gefragt, die als Add-on in bestehende Systeme eingebunden werden kann. Auch hier befindet sich die Entwicklung noch im Anfangsstadium.

Grundvoraussetzung dafür, dass zum Beispiel Browsererweiterungen die Sicherheit wirksam verbessern können, ist allerdings ein sicherer Kanal zum Benutzer. Es muss Zustands- und Ereignisanzeigen geben, die sich von außen nicht manipulieren oder ersetzen lassen, und den Benutzern muss klar sein, welchen Anzeigen sie vertrauen können. Hierzu gibt es erste Ergebnisse der Grundlagenforschung, aber noch keine praxistauglichen Umsetzungen.

Literatur

[APWG04a] Anti-Phishing Working Group: Website. http://www.antiphishing.org/, 2004-10-06.

[APWG04b] Anti-Phishing Working-Group: *Phishing Attack Trends Report - July 2004*. http://www.antiphishing.org/APWG_Phishing_Attack_Report-Jul2004.pdf, 2004-10-06.

[Bac04] M. Bacon: Banks don't understand phishing social risks. in: *The Risks Digest,* Volume 23, Issue 39; http://catless.ncl.ac.uk/Risks/23.39.html#subj18, 2004-10-07.

[BdB04] Bankenverband: *Online-Banking-Sicherheit. Informationen für Online-Banking-Nutzer.* Informationsbroschüre; Bundesverband Deutscher Banken e.V., 2004; http://www.bankenverband.de/pic/artikelpic/072004/0407_Online_Sicherheit.pdf, 2004-10-11.

[BeSch02] P. Bednorz, M. Schuster: *Einführung in die Lernpsychologie.* Utb, 2002.

[BlSch04] H. Bleich, J. Schmidt: Auf Phishzug. Passwort-Diebstahl im Web wird raffinierter. in: c't 17/2004, S. 178.

[Dar02] Dartmouth PKI Lab: *Web Spoofing Demonstration.* http://www.cs.dartmouth.edu/~pkilab/demos/spoofing/, 2004-10-26

[Gre04] K. Gregory: Citibank assists scammers. in: *The Risks Digest,* Volume 23, Issue 46; http://catless.ncl.ac.uk/Risks/23.46.html#subj12, 2004-10-07.

[Hei04a] Heise News: *Phishing und die Hersteller von Homebanking-Software.* Meldung vom 31. 08. 2004, http://www.heise.de/newsticker/meldung/50561, 2004-10-07.

[Hei04b] Heise News: *eBay: Kein Handel ohne Rufnummer.* Meldung vom 02. 09. 2004; http://www.heise.de/newsticker/meldung/50602, 2004-10-07.

[Hei04c] „hiro": *Chaos bei Domainnamen der vr Gruppe.* Beitrag im Artikelforum auf www.heise.de; http://www.heise.de/security/news/foren/go.shtml?read=1&msg_id=5773271&forum_id=57036, 2004-10-07.

[Hei04d] Heise News: *Studie: Milliardenschaden durch betrügerische E-Mails.* Meldung vom 06. 05. 2004; http://www.heise.de/newsticker/meldung/47170; 2004-10-07.

[Hei04e] Heise News: *Online-Bank plant Rasterfahndung.* Meldung vom 11. 09. 2004; http://www.heise.de/newsticker/meldung/50961, 2004-10-07.

[Hei04f] Heise News: *Trojaner klauen Bank-Kunden PINs und TANs.* Meldung vom 09. 09. 2004; http://www.heise.de/newsticker/meldung/50793; 2004-10-07.

[Hei04g] Heise News: *Identitätsklau kostet die Opfer in den USA jährlich 2,4 Milliarden Dollar.* Meldung vom 18. 06. 2004; http://www.heise.de/newsticker/meldung/48358, 2004-10-07.

[Kos04] A. Kossel: Das E-Mail-Fiasko. in: c't 19/2004, S. 132; http://www.heise.de/ct/04/19/132/, 2004-10-07.

[Leg04] D. Legard: *Phishing Lures Increase by Half.* http://www.pcworld.com/news/article/0,aid,117263,00.asp, 2004-10-06.

[Ley04a] J. Leyden: Phishing scams cost UK banks £1m+. The Register, 26. 04. 2004; http://www.theregister.co.uk/2004/04/26/phishing_scams/.

[Ley04b] J. Leyden: Sloppy banks open the door to phishermen. *The Register*, 20. 07. 2004; http://www.theregister.co.uk/2004/07/20/phishing_attack/.

[Ley04c] J. Leyden: DIY phishing kits hit the Net. *The Register*, 19. 08. 2004; http://www.theregister.co.uk/2004/08/19/diy_phishing/.

[Lid04] S. Liddicott: Banks don't understand phishing social risks. in: *The Risks Digest,* Volume 23, Issue 37; http://catless.ncl.ac.uk/Risks/23.37.html#subj10, 2004-10-07.

[Neu98] P. G. Neumann: *Computer-Related Risks.* Addison-Wesley, 1998.

[Net04] Netcraft Ltd.: *Bank's own developers a much bigger problem than browsers.* http://news.netcraft.com/archives/2004/07/18/banks_own_developers_a_much_bigger_problem_than_browsers.html.

[Nie93] J. Nielsen: *Usability Engineering.* Academic Press, 1993.

[Nor02] D. A. Norman: *The Design of Everyday Things.* Basic Books, 2002.

[Per99] C. Perrow: *Normal Accidents: Living with High Risk Technologies.* Princeton University Press, 1999.

[Tru04] TRUSTe: *U.S. Consumer Loss of Phishing Fraud to Reach $500 Millon.* Presseerklärung, http://www.truste.org/about/press_release/09_29_04.php.

[WhiTy99] A. Whitten, J. D. Tygar: Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. in: *Proceedings of the 8th USENIX Security Symposium, August 23-36, 1999, Washington, D.C.;* http://citeseer.ist.psu.edu/whitten99why.html.

[YeSm02] E.Z. Ye, S. Smith: Trusted Paths for Browsers. in: *Proceedings of the 11th USENIX Security Symposium*; http://www.usenix.org/events/sec02/full_papers/ye/ye_html/, 2004-10-26.

Fraunhofer SIT im Profil

Bei der Nutzung der Informationstechnologie wird IT-Sicherheit immer stärker zum entscheidenden Erfolgsfaktor, denn bestehende Synergie- und Rationalisierungspotenziale lassen sich nur dann vollständig realisieren, wenn ein grundsätzliches Vertrauen in die Sicherheit der eingesetzten Technologien vorhanden ist. Bei der zukunftsfähigen Gestaltung von Diensten, Prozessen und Infrastrukturen gilt es deshalb stets, Sicherheitsinteressen von Kunden und Geschäftspartnern zu berücksichtigen. Diese marktgerechte, skalierbare IT-Sicherheit steht im Zentrum der Arbeit am Fraunhofer-Institut für Sichere Informationstechnologie SIT.

Auf Grundlage exzellenter, strategischer Vorlaufforschung entwickelt das Institut unmittelbar einsetzbare Lösungen, die vollständig auf die Bedürfnisse der Auftraggeber ausgerichtet sind. Möglich werden diese maßgeschneiderten Dienste durch über hundert hochqualifizierte Mitarbeiter, deren Kenntnisse alle Bereiche der IT-Sicherheit abdecken. Sie bilden die breite Kompetenzbasis für technologieübergreifende Leistungen auf höchstem Niveau. Das Fraunhofer-Institut SIT ist für Unternehmen aller Branchen tätig. Viele erfolgreiche Projekte mit internationalen Partnern sind eindrucksvoller Beweis für eine vertrauensvolle und zuverlässige Zusammenarbeit.

Unsere Mission: Vorsprung durch Sicherheit

Das Fraunhofer-Institut SIT sieht IT-Sicherheit nicht absolut, sondern setzt sie stets in Relation zu den zu schützenden Infrastrukturen und Werten. Entsprechend sind die sicherheitsrelevanten Fragestellungen je nach Marktumfeld und Unternehmensgröße höchst unterschiedlich zu beantworten. Kleinere oder mittelständische Betriebe etwa erfordern mitunter ganz andere Lösungsstrategien als international agierende Konzerne.

Ziel des Instituts ist deshalb die Ausrichtung der IT-Sicherheit an den tatsächlichen Bedürfnissen der Partner. Dies erreicht SIT durch individuelle Analysen, die auch betriebswirtschaftliche und juristische Faktoren mit einbeziehen. Erst durch diese ganzheitliche Herangehensweise ergeben sich innovative, nachhaltige Lösungen. IT-Sicherheit erweist sich oft sogar als befördernder Faktor, der Unternehmen neue Anwendungsfelder erschließt und Marktanteile dauerhaft sichert. Dabei gilt: Je früher IT-Sicherheit in die Prozesse integriert wird, desto zukunftsfähiger und effizienter sind die entsprechenden Systeme. So wird Sicherheit zum klaren Marktvorteil.

Breite Kompetenz in IT-Sicherheit

Als Spezialist für IT-Sicherheit befasst sich SIT mit allen relevanten Technologien und deren effizientem Einsatz. Durch staatlich geförderte Vorlaufforschung ist das Institut in der Lage, Entwicklungen in der Forschung strategisch zu begleiten und kann schnell und zuverlässig auf die Erfordernisse des Marktes reagieren. So kann es seine Kompetenzen optimal einsetzen.

Im Bereich der sicheren Identifikationstechnologien (Smartcards, Biometrie, elektronische Signatur und PKI) gehört das Fraunhofer-Institut SIT deshalb zu den führenden Anwendungsentwicklern. Eine weitere Stärke stellt das Wissen in der Sicherheit mobiler Systeme und Endgeräte dar. Die unmittelbare Beteiligung des Instituts an der aktuellen Forschung verschafft seinen Partnern hierbei einen großen Wissensvorsprung, zum Beispiel in der Gestaltung sicherer Funk- und Mobilfunk-Netze sowie entsprechender Schnittstellen und sicherer mobiler Arbeitsumgebungen.

Aber auch beim Schutz unternehmenskritischer Infrastrukturen und Netzwerke bietet das Fraunhofer-Institut SIT Dienste von höchster Qualität und Individualität. Beides entsteht durch die Kombination formaler Sicherheitsmodelle mit der Praxisnähe des Forschungsbereichs "Praktische Systemsicherheit" und des SIT-Testlabors. Hier überprüfen SIT-Wissenschaftler mit aktuellen Angriffswerkzeugen die Sicherheit in eingebetteten Systemen (Embedded Systems), W-LANs oder Computernetzwerken anhand von realitätsnahen Bedrohungszenarien, die genau auf die jeweiligen Gegebenheiten beim Kunden abgestimmt sind. Reichhaltige Erfahrung besitzt das Institut zudem in den Anwendungsfeldern E-Learning, E-Health und E-Government sowie elektronischer und mobiler Handel.

Ergänzt wird das Institutsprofil durch die Partner und Netzwerke in Industrie und Forschung. Die enge Kooperation mit der Technischen Universität Darmstadt etwa findet ihren sichtbaren Ausdruck in der Besetzung des Lehrstuhls für "Sicherheit in der Informationstechnik" durch SIT-Institutsleiterin Prof. Dr. habil. Claudia Eckert. Die Nähe zur Wirtschaft verdeutlicht der Sitz der Fujitsu Laboratories Europe im Institutsgebäude.

SIT-Leistungsangebot

Das Fraunhofer-Institut SIT hilft seinen Partnern durch maßgeschneiderte Lösungen, Anwendungsfelder zu erschließen und zu behaupten. In seinen Kompetenzbereichen bietet SIT:

- Entwicklung prototypischer IT-Sicherheitslösungen
- Einbettung von Sicherheitstechnologien in bestehende Systeme
- Hersteller- und produktneutrale IT-Beratung und Systemanalyse
- Marktorientierte Technologiestudien
- Modellierung und Realisierung sicherer elektronischer Geschäftsprozesse und Dienste
- Spezifikation und Entwicklung von praxistauglichen Sicherheitsmodellen mittels allgemein anerkannter Methoden, zum Beispiel Unified Modeling Language (UML)
- Praxisnahe Schulungen und individuelle Mitarbeiter-Fortbildung

Das Institut bietet seine Leistungen in vier Geschäftsfeldern an:

- Sicherheit und Mobilität,
- Identitäts- und Rechtemanagement,
- Sichere Geschäftsprozesse,
- Ganzheitliches Sicherheitsmanagement und Business Continuity.

Ansprechpartner

Fraunhofer-Institut für Sichere Informationstechnologie SIT
Rheinstraße 75
D-64295 Darmstadt

Tel.: +49 (0)6151-869-0
Fax: +49 (0)6151-869-224
http://www.sit.fraunhofer.de

Planung und Ausführung dieser Studie

Sven Türpe
Tel.: +49 (0)6151-869-4238
Sven.Tuerpe@sit.fraunhofer.de

Anke Baumann
Tel.: +49 (0)6151-869-289
Anke.Baumann@sit.fraunhofer.de

Forschungsbereich „Sichere Prozesse und Infrastrukturen“

Dr. Michael Zapf
Tel.: +49 (0)6151-869-60024
Michael.Zapf@sit.fraunhofer.de

Presse- und Öffentlichkeitsarbeit

Oliver Küch
Tel.: +49 (0)6151-869-213
Oliver.Kuech@sit.fraunhofer.de