Trickbetrügern auf der Spur

Wie man der Phishing-Welle entkommen kann

Malte Hesse und Norbert Pohlmann

Foto: Erich Kuchling/Westend61

Meldungen über Trickbetrug im Internet und die daraus resultierenden Schäden sind inzwischen an der Tagesordnung. Das aktuelle Schlagwort in diesem Zusammenhang: „Phishing". Dieser Beitrag nimmt das „Password Fishing" (= Phishing) genauer unter die Lupe und erarbeitet Vorschläge, diesem angemessen zu begegnen.

Anfang 1996 tauchte der Begriff erstmals in der Hackerszene auf und bezog sich auf den Diebstahl von Internetzugangsdaten von AOL-Kunden. Inzwischen hat sich der Begriff als allgemeiner Ausdruck für den Identitäts- und Passwortdiebstahl im Internet etabliert und beschäftigt viele Branchen. Laut einer Statistik der Anti-Phishing Working Group (APWG) erfolgen über 80 Prozent aller Phishingangriffe auf den Finanzdienstleistungssektor.

Die ersten Fälle gegen deutsche Bankkunden wurden im Juli 2004 verzeichnet. Ab Anfang 2005 erfolgte eine massive Zunahme von Phishing-Angriffen. Während von der APWG im Jahr 2004 noch 200.000 Phishing-E-Mails pro Monat verzeichnet wurden, steigerte sich die Zahl auf heute durchschnittlich 100.000 Phishing-E-Mails pro Tag.

Dabei entstehen für die Banken nicht nur Schäden aufgrund von zunehmendem Misstrauen gegenüber der Onlinebanking-Sicherheit, sondern auch tatsächliche Verluste. In der Öffentlichkeit finden sich Angaben von 4.000 bis 12.000 Euro Schaden pro erfolgreichem Angriff. Der bisher höchste veröffentlichte Einzelschaden betrug 29.000 Euro. In Berlin wurden zwischen Januar und August 2005 etwa 120 Fälle angezeigt. Das LKA Baden-Württemberg verzeichnete in demselben Zeitraum rund 200 Fälle. Eine Nachfrage beim LKA Nordrhein-Westfalen ergab für das Jahr 2005 bis November 248 Fälle und einen Gesamtschaden von etwa 640.000 Euro. Focus Online sprach Mitte Oktober 2005 von 4,5 Millionen Euro Schaden und „tausenden Fällen" in ganz Deutschland. Neben den materiellen Verlusten entsteht zusätzlich ein zunehmender Imageschaden für den gesamten Finanzsektor. Zugleich nimmt die Verunsicherung der Onlinebanking-Kunden permanent zu.

Automatisierter Betrug

Vor Jahren häuften sich die Überfälle auf Kunden, die Geld von einem Geldautomaten der Bank abgehoben haben. Später kam der Missbrauch von Debitkarten hinzu. Heute scheint die größte Herausforderung der Kampf gegen Betrug im Internet zu sein. Innovativ an dieser Form des Trickbetrugs ist dabei nur, dass dieser über das Internet mithilfe von Maschinen automatisiert erfolgt und er damit eine ganz neue Dimension erreichen kann. Durch das Internet haben wir neben einem drastisch erhöhten Aktionsradius auch eine starke Abstraktion zwischen Handlung und Wirkung. Der Dieb kann kriminelle Machenschaften von Zuhause aus bei Kaffee und Kuchen durchführen. Tatsächlich haben wir es nicht mit Amateuren zu tun, sondern mit organisierter Kriminalität.

An den verschiedenen Stufen einer Phishing-Welle sind mehrere Personen mit speziellen Fähigkeiten beteiligt. Im Phishing-Milieu ist eine regelrechte Kommerzialisierung zu beobachten, die eine Kooperation mit anderen kriminellen Internetakteuren wie Spammern und Botnetzbetreibern einschließt. Das Internet als weltweites Datennetz geht über alle Landesgrenzen hinweg. Deshalb können Angreifer auch aus dem Ausland heraus einfach agieren. Erste Festnahmen meldet das BKA in Estland. Aber der Fluss des Geldes strömt auch nach Russland, in die USA, nach Asien und auch in die EU. In einigen Fällen wird die Geldwäsche auch über deutsche Mittelsmänner abgewickelt, die zum Beispiel den Service von Western

Union nutzen, mit dem weltweit Geld in Minutenschnelle versandt oder empfangen werden kann.

Das Internet in Deutschland hat sich in den vergangenen Jahren zu einer wichtigen Kommunikations- und Dienstinfrastruktur entwickelt, von der viele Unternehmen, Organisationen und Privatpersonen abhängig sind. Onlinebanking ist dabei immer noch ein vergleichsweise neues Angebot der Banken an ihre Kunden und bietet neben der Bequemlichkeit für den Benutzer auch ein Einsparpotenzial. Gerade deshalb muss es vorrangiges Ziel sein, das Vertrauen der Kunden in das Onlinebanking zu stärken und auf ein zukunftorientiertes und sicheres Verfahren zu setzen.

Phisher-Tricks

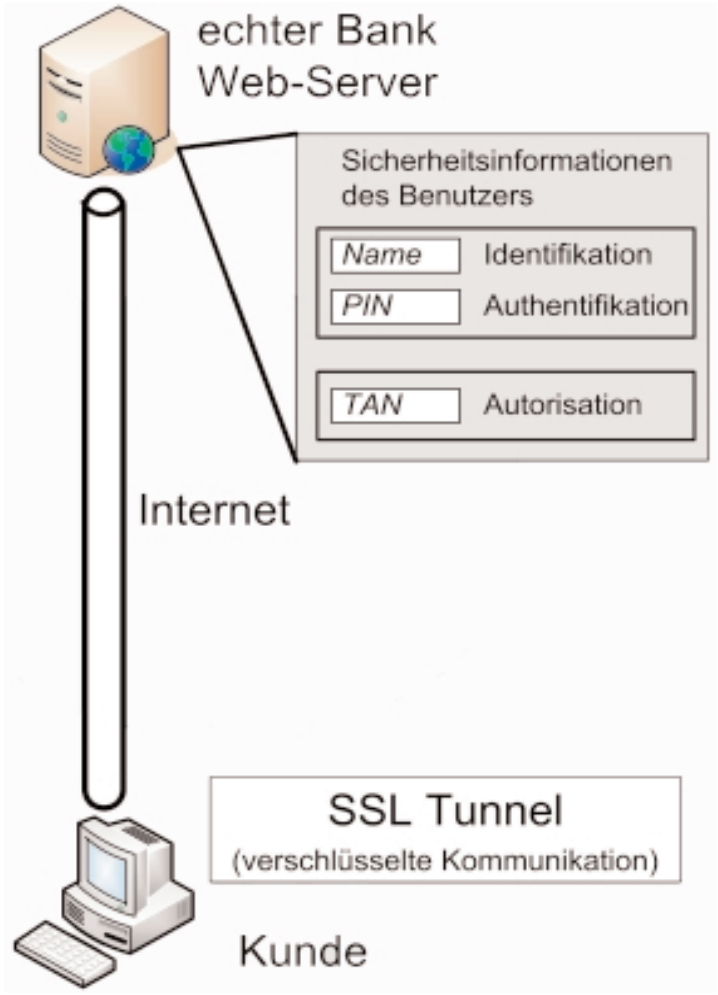
Das klassische Onlinebanking (siehe Abbildung 1) setzt auf eine Kombination aus Übertragungskanalverschlüsselung mit einem SSL-Tunnel, die Identifikation und Authentikation des Benutzers mit seinem Benutzernamen (Identifikation) und der PIN sowie die Autorisation von Vorgängen mit Einmalkennwörtern, die als Transaktionsnummer (TAN) bezeichnet werden. Diese Sicherheitsinformationen des Benutzers benötigt ein Trickbetrüger für seinen Angriff.

Um an diese Sicherheitsinformationen des Benutzers und an dessen Geld zu gelangen, wendet der Phisher (Angreifer) verschiedene Tricks an (siehe Abbildung 2). Als erstes erstellt er einen falschen Bank-Web-Server, der vom Erscheinungsbild her dem echten Bankserver täuschend ähnelt. Als zweites sendet er hunderttausende gefälschter E-Mails, die aussehen, als wären sie von einer Bank, an potenzielle Kunden. Diese E-Mail fordert den Bankkunden auf, Aktionen auf dem falschen Bank-Web-Server durchzuführen. Fällt ein Empfänger auf die falsche Bank-E-Mail herein und folgt dem Link, so gelangt dieser auf einen gefälschten Bank-Web-Server. Dabei geben meist sogar die Links auf den ersten Blick nur wenig Grund zur Annahme, dass es sich dabei um eine Fälschung handeln könnte.

Die Schwierigkeit besteht im Wesentlichen darin, dass es für den Kunden nur schwer ersichtlich ist, dass diese E-Mail gefälscht ist und nicht von seiner Bank versendet wurde.

Im dritten Schritt werden dem Opfer dann seine Sicherheitsinformationen auf dem falschen Bank-Web-Server entlockt. Sowohl die gefälschte E-Mail als auch die gefälschte Webseite wirken wie die der echten Bank. Dabei ist zu beobachten, dass Layout und Sprache der Phisher sich mit jeder Angriffswelle verbessern. Neben falschen Bank-E-Mails werden weitere Techniken verwendet, um die Kunden auf falsche Web-Server zu leiten.Da-

Abb. 1: **Funktionsweise des klassischen Onlinebankings**



runter befinden sich etwa falsche Werbebanner oder falsche Suchmaschineneinträge. Im vierten Schritt nutzt dann der Angreifer die Sicherheitsinformationen, um sich gegenüber dem echten Bank-Server als Kunde zu präsentieren und unberechtigt Geld auf sein Konto zu transferieren.

Unterschiedliche Reaktionen

Als eine direkte Reaktion der Banken auf die Phishing-Angriffe wurden verschiedenste Modifikationen des PIN/TAN Verfahrens eingeführt. Bei iTAN (indizierte TAN) muss eine ganz bestimmte TAN benutzt werden, um eine Transaktion zu autorisieren. Damit soll sich die Wahrscheinlichkeit verringern, dass ein Angreifer bei einem Phishing-Angriff die richtige TAN abfragt. Das iTAN-Verfahren sorgt dafür, dass der Phisher gezwungen wird, in Echtzeit zu arbeiten. Dazu stellt der Angreifer selbst – zur Zeit des Angriffs – eine Anfrage an den echten Bank-Server mit den vom Opfer erhaltenen Daten. Dieser Angriff kann ebenfalls automatisiert mit Hilfe von falschen Web-Servern erfolgen. Ähnliches gilt für andere Verfahren der gezielten TAN-Anforderung, wie eTAN und eToken und TAN-Generatoren.

Alte und unsichere Verfahren müssen im Übrigen mit der Einführung neuer Verfahren abgeschaltet werden, um Hintertüren auszuschließen. Bei einem kürzlich aufgetretenen Betrugsfall wurde zwar ein neues iTAN-Verfahren eingeführt, aber das alte TAN-Verfahren nicht abgeschaltet. Somit konnten durch Phishing gewonnene iTAN theoretisch weiterhin uneingeschränkt als TAN genutzt werden.

Einen etwas anderen Weg geht das mTAN-Verfahren, das auch als SMS-TAN bekannt ist. Dabei wird ein zweiter separater Kommunikationsweg per SMS zum Kunden verwendet, um die Überweisungsdaten zu überprüfen. mTAN

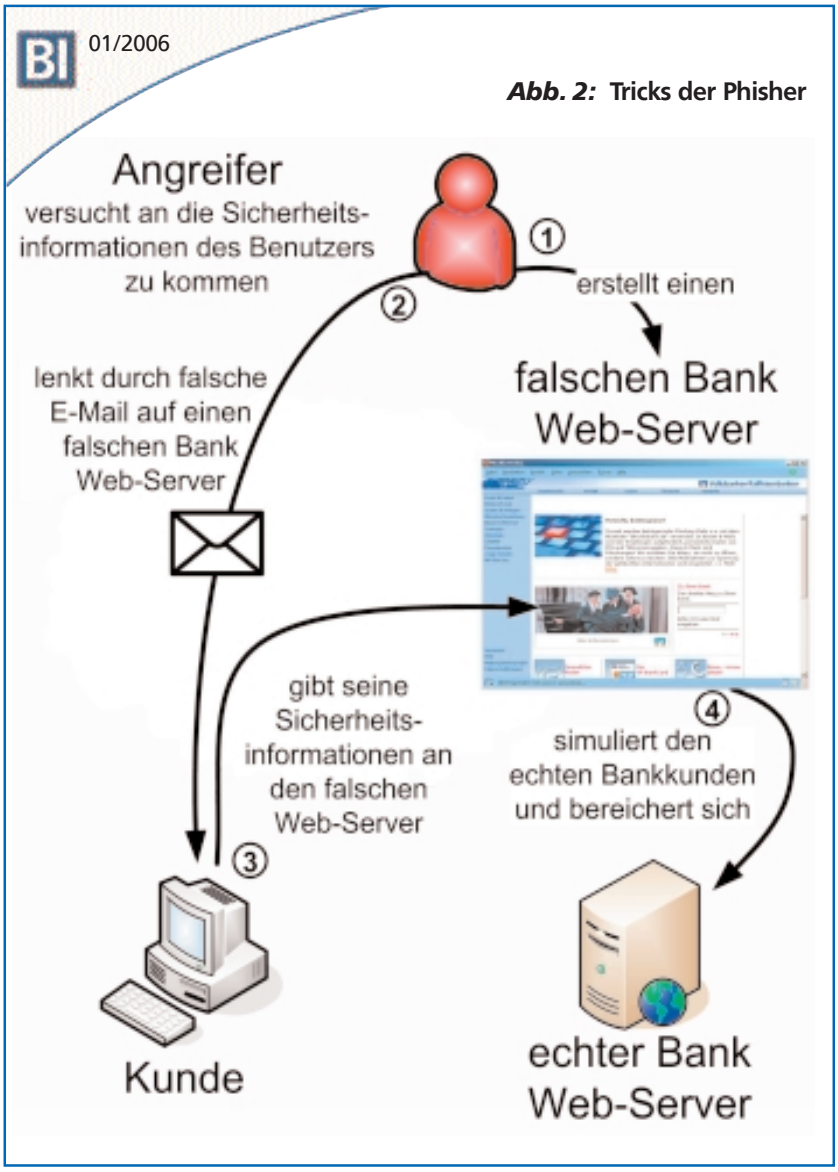


Abb. 2: **Tricks der Phisher**

ist zurzeit wahrscheinlich die interessanteste Erweiterung zu dem PIN/TAN-Verfahren. Inhalt der SMS-Nachricht ist eine TAN mit den dazugehörigen Überweisungsdaten, die der Kunde benötigt, um die Überweisung im Browserfenster abzuschließen. Es liegt damit in der Hand des Kunden, die in der SMS übersendeten Überweisungsdaten zu prüfen und zu autorisieren. Voraussetzung für das mTAN-Verfahren ist natürlich der Besitz eines Mobiltelefons und die Möglichkeit eine SMS zu empfangen. Bei Geschäftskunden wird dieses Verfahren nur schwer zu realisieren sein, da hier die Zuordnung der richtigen Informationen zum richtigen Empfänger-Handy problematisch werden könnte. Zusätzlich müsste vermutlich der Kunde – zumindest teilweise – die höheren Kosten für dieses Verfahren mittragen.

Schadsoftware-Phishing

Neben den Phishing-E-Mails gibt es eine weitere, zukünftig noch bedeutendere Bedrohung für den Internetnutzer. Oft ist an die unerwünschten E-Mails zusätzlich noch Schadsoftware angehängt. Zu Schadsoftware, auch bekannt als Malware, gehören unter anderem Trojanische Pferde, Keylogger, Screenlogger und Spyware. Diese verbreiten sich über das Internet und nutzen Sicherheitslücken in Browsern, Mail-Clients und Betriebssystemen aus, um sich zu installieren. Kostenlose Programme oder illegale Downloads können ebenfalls Schadsoftware enthalten. Der unbedachte Benutzer hat sich schnell einen Schädling eingefangen. Seine Anwesenheit bleibt ihm oft verborgen.

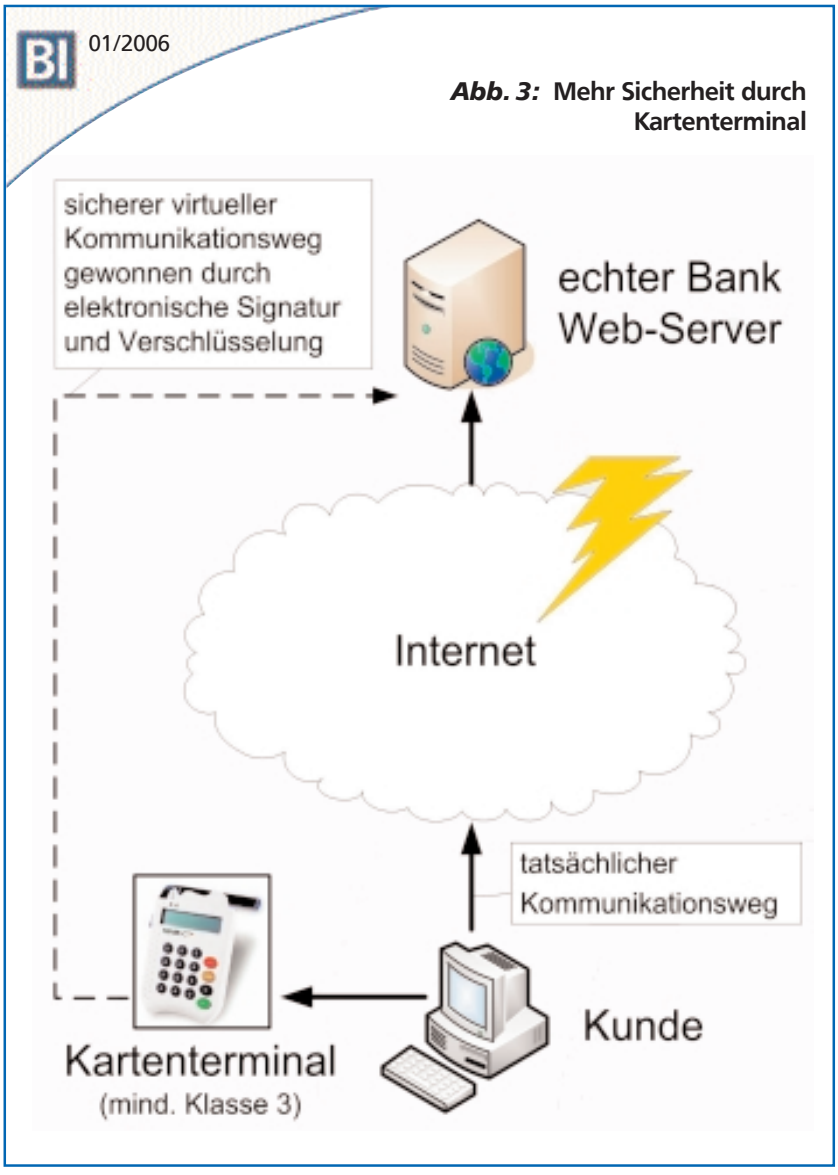
Wenn der Nutzer seinen Computer ungenügend geschützt hat und sich der Schädling installiert, kann die Integrität des Kunden-Computers nicht mehr gewährleistet werden. Sämtliche Daten können vom Angreifer mitgelesen und verändert werden. Dies gilt auch für verschlüsselte SSL-Verbindungen zu einem echten Bank-Server.

Im Fall der kürzlich verhafteten estnischen Phisher wurde so ein Trojanisches Pferd verwendet. Laut Aussage des BKA ließ dieses die Kunden beim Onlinebanking solange gewähren, bis die Transaktion mit der TAN bestätigt werden sollte. Dann blockierte es den Zugriff auf die Onlinebanking-Seite und die Benutzerdaten wurden an den Phisher weitergeleitet.

Es hat sich gezeigt, dass die Phisher äußerst kreativ auf die Einführung neuer Verfahren reagieren. Es ist schwer, an die meist im Ausland sitzenden Hintermänner zu kommen und sie zur Verantwortung zu ziehen. Immer mehr Gruppierungen springen auf den „Phishing-Zug" auf. Selbst wenn die Onlinebanking-Benutzer gegen Phishing-E-Mails sensibilisiert sind, wird es stets das stark wachsende Problem der Schadsoftware geben.

Die Sicherheitsfirma iDefense verzeichnete allein in diesem Jahr schon über 6.000 verschiedene Keylogger-Programme. Im Vergleich zum Vorjahr ist das ein Anstieg um 65 Prozent. Von den 248 in Nordrhein-Westfalen gemeldeten Phishing-Fällen für das Jahr 2005 fallen nach Angaben des LKA 117 Fälle auf das Ausspähen von Benutzerdaten durch Trojanische Pferde. Um hier Einhalt zu gebieten, sollten zukünftig sichere Betriebssysteme oder zusätzliche Sicherheitskerne, die Standard-Betriebssysteme sicherer machen, genutzt werden. Für diese Form der sicheren Systeme besteht zurzeit jedoch noch großer Forschungsbedarf und die Technologien sind für die breite Masse leider noch nicht verfügbar.

Abb. 3: **Mehr Sicherheit durch Kartenterminal**



Entschlossenes Handeln notwendig

Das Problem Phishing ist akut. Es nutzt die Verunsicherungen des neuen Mediums Internet sowohl beim Kunden als auch bei den Banken aus. Nüchtern betrachtet gibt es Wege, das Problem auf ein für alle Seiten tragbares Maß zu reduzieren. Diese Sicherheitsmaßnahmen müssen nur nachhaltig umgesetzt werden.

Wichtig ist die Aufklärung der Kunden über das Thema Phishing und auch über die möglichen Folgen von Schadsoftware auf ihren Systemen. Kundenaufklärung bedeutet dabei auch Aufklärung über die Notwendigkeit der Verwendung von Virenscannern, Personal Firewalls, Anti-Spam-Tools und das Aufspielen von Sicherheitspatches, die bekannte Sicherheitslücken von Betriebssystemen und Anwendungen schließen.

Die Mitarbeiter der Banken müssen zum Thema Phishing geschult werden. Ein Krisenmanagement muss eingerichtet und Abläufe für den Ernstfall geprobt werden. Dazu gehört auch die Pflege von Kontakten zu externen Ansprechpartnern, etwa zu Institutionen wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) oder Forschungseinrichtungen, die sich mit den Hintergründen auskennen. Rechtliche Aspekte des Phishings sollten vorbereitend geklärt werden. So gibt es nach Aussage des BKA bisher noch keine abschließende juristische Bewertung zur Frage, ob alleine schon das Versenden einer Phishing-E-Mail strafbar ist. In einem Artikel zum Thema findet man die Auffassung, dass in Phishing-E-Mails die Grundlage für die Begehung diverser Straftaten zu sehen ist und dass die Nachahmung der Original-Webseiten gegen das Marken- und Namensrecht verstößt.

Ein weiterer Aspekt ist, dass die EU-Kommission plant, bis spätestens 2010 eine drastische Ausweitung des Verbraucherschutzes für Bankkunden umzusetzen. Dann sollen die Banken im Schadensfall haften oder Kunden nur einen bestimmten Maximal-Betrag zahlen müssen.

Sicherheitsmechanismen

Durch die Analyse des Surfverhaltens der Kunden auf Bank-Servern können manchmal Abweichungen von Referenzschemata mit einem Phishing-Frühwarnsystem erkannt werden. Dazu gehören unter anderem die Häufigkeit des Einloggens, die Höhe der Beträge, das vermehrte Auftreten von Passwortänderungen. Die Auswertung kann mithilfe von Data-Mining-Verfahren zu erstaunlichen Ergebnissen führen. Ein einfaches Beispiel in diesem Zusammenhang ist eine Häufung von Passwortänderungen mit nachfolgenden hohen Überweisungen als Hinweis auf Phishingangriffe. Ein Limit für Überweisungen dürfte aber besonders für Geschäftskunden unpraktikabel sein.

Die Banken sollten das Internet nicht nutzen, um den Kontakt zu ihren Kunden zu pflegen. Dies würde die Kunden unnötig an E-Mails von ihrer Bank gewöhnen und das Vertrauen in Informationen aus dem Internet stärken. Will die Bank nicht auf E-Mails für den Kundenkontakt verzichten, sollten diese personifiziert werden, ohne gleich auf persönliche Daten zurückzugreifen.

Um gut im Kampf gegen Phishing gerüstet zu sein, ist möglicherweise eine Zusammenarbeit mit anderen Banken ratsam. Bei der Anti-Phishing Working Group sind acht der zehn führenden US-Banken und vier der fünf Spitzen-US-Internet Service Provider vertreten. Eine Mitarbeit in dieser Gruppe oder die Gründung eines nationalen Gremiums könnten durchaus hilfreich sein.

Eine sichere Kommunikation zwischen Kunden und Bank über das Internet benötigt die Integrität der Nachrichten und der IT-Systeme, die Authentizität der Kommunikationspartner, die Vertraulichkeit und die Verbindlichkeit der Nachrichten. Dies sind genau die Anforderungen, die an eine qualifizierte elektronische Signatur in Deutschland gestellt werden. Mit HBCI (Homebanking Computer Interface) wurde schon vor vielen Jahren ein solider offener Homebanking Standard in Deutschland eingeführt. HBCI ist inzwischen in einer neuen Version unter FinTS (Financial Transaction Services) bekannt. Dieser sieht die Verwendung einer Smartcard – ausgestattet mit elektronischer Signatur – vor.

Seminartipp

Phishing und andere aktuelle Gefahren im Online-Banking für Genossenschaftsbanken

Termin: 2. Februar 2006

Ort: Schloss Montabaur

Preis: 475 Euro (ADG-Mitglieder)/
593,75 Euro (Nicht-Mitglieder)

Anmeldung und Infos:
E-Mail: axel_gürntke@adgonline.de

Interessante Links

Anti-Phishing Working Group:
www.antiphishing.org

Bundesamt für Sicherheit in der Informationstechnik:
www.bsi-fuer-buerger.de

European Multilaterally Secure Computing Base:
www.emscb.de

Heise Verlag:
www.heise.de

Institut für Internet-Sicherheit:
www.internet-sicherheit.de

Glossar auch mit Begriffen aus diesem Artikel finden Sie unter:
www.internet-sicherheit.de/center-glossar.html

Eine sichere Technologie steht damit in Deutschland bereits zur Verfügung. Das Verfahren setzt beim externen Onlinebanking auf Kartenleser, für die verschiedene Sicherheitsklassen existieren. An dieser Stelle ist es möglich, der wachsenden Bedeutung der Schadsoftware bei Phishing-Angriffen gerecht zu werden. Ein Kartenleser muss unabhängig vom Kunden-Computer die Überweisungsdaten anzeigen und die elektronische Signatur ausführen können. Ein Kartenleser, mindestens der Klasse 3, erfüllt genau diese Vorraussetzungen.

Er verfügt neben der eigentlichen Technik zum Auslesen der Karten über ein Display und ein Tastenfeld, das für die PIN-Eingabe genutzt wird. Sowohl das Display als auch das Tastenfeld können nur vom Kartenleser gesteuert werden. Die Integrität des Kartenlesers muss dabei nachweislich sichergestellt werden. Durch HBCI und der damit verbundenen elektronischen Signatur und Verschlüsselung wird über ein öffentliches Netz ein sicherer virtueller Kommunikationsweg ermöglicht.

Verbindlicheres Verfahren

Leider wurde das HBCI-Verfahren bei den Kunden bisher nicht so gut angenommen. Es ist aufgrund der benötigten Hard- und Software recht teuer und nicht so flexibel. Außerdem wurden die PIN/TAN-Verfahren von den Banken stärker beworben. Findet HBCI doch Anwendung, werden meist aus Kostengründen nur Kartenleser der Klassen 1 eingesetzt. Diese Kartenleser können den Kunden zusätzlich ein trügerisches Gefühl der Sicherheit vermitteln. Ein durch Schadsoftware manipulierter Computer wird zukünftig in der Lage sein, Klasse 1-Kartenleser gezielt anzusteuern und die PIN-Eingabe zu verfolgen. Der Kunde kann sich somit nicht sicher sein, auf welche Daten er seine Signatur durch PIN-Eingabe anwendet. Die elektronische Signatur hat rechtlich eine andere Verbindlichkeit für den Kunden als das bisher genutzte PIN-TAN-Verfahren.

Die so gewonnene Verbindlichkeit dürfte für die Banken ein erfreulicher Aspekt sein. Um einem weiteren Imageverlust und finanziellen Schaden durch Phishing entgegenzuwirken, wäre die Subvention von Klasse 3-Kartenlesern zu überlegen. Damit lassen sich hoffentlich in der Zukunft Schlagzeilen wie „Schwedische Bank geht wegen Phishing offline" (Heise News vom 6. Oktober 2005) vermeiden.

Vorreiterrolle übernehmen

Der Finanzsektor hat zurzeit das größte Problem mit Phishing, was stark dem Image der Banken schadet. Die bisher genutzten PIN-TAN-Verfahren sind mit Ausnahme des mTAN-Verfahrens nicht mehr empfehlenswert und sollten so schnell wie möglich durch eine HBCI-Technik mit Klasse 3-Kartenleser abgelöst werden. Dies gilt insbesondere für die Zielgruppe der Geschäftsleute. Alte und unsichere Verfahren sollten mit der Einführung der neuen Verfahren sofort abgeschaltet werden.

„Banken haben hier und heute die Möglichkeit, eine Vorreiterrolle zu übernehmen, um eine branchenübergreifende elektronische Signaturlösung zu schaffen."

Die Banken haben dabei hier und heute die Möglichkeit, eine Vorreiterrolle zu übernehmen und eine branchenübergreifende, qualifizierte elektronische Signaturlösung für ihre Kunden zu schaffen, die dann auch bei anderen Lösungen angewendet werden kann. So kann das Vertrauen der Kunden in das Onlinebanking und in die Banken wieder gestärkt und nachhaltig gesichert werden. ■

Zu den Autoren

Malte Hesse (links) ist wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen.
E-Mail: malte.hesse@internet-sicherheit.de

Prof. Dr. Norbert Pohlmann ist Geschäftsführender Direktor des Instituts für Internet-Sicherheit der Fachhochschule Gelsenkirchen.
E-Mail: norbert.pohlmann@informatik.fh-gelsenkirchen.de