Finanzen

Sicherheit beim Onlinebanking

Schutzwall mit Lücken

1. Juni 2012 **- Bankgeschäfte am Computer zu erledigen gehört fast schon zum Standard - leider auch für Kriminelle, die es auf das Geld anderer abgesehen haben. Um Bösewichtern das Leben zu erschweren, entwickelt die Geldwirtschaft ständig neue Sicherheitssysteme, mit denen sich die Kunden vertraut machen müssen. Garantien, dass sie funktionieren, gibt es nicht.**


Foto: davidevison – Fotolia.com

Onlinebanking - bequem, aber mit Restrisiko: Jeder Kunde muss selbst Vorsorge treffen, damit er nicht betrogen werden kann.

Am 27. Juli dieses Jahres schließt die NorisBank ihre Schalterhallen, um dann nur noch als Onlinebank weiter zu bestehen. Damit macht die Deutsche-Bank-Tochter den Schritt, den viele Banken anstreben. Ginge es nach den Vorstellungen der Geldinstitute, gehört die persönliche und kostenlose Betreuung im täglichen Geschäft in Banken und Sparkassen längst der Vergangenheit an. Es ließen sich große Summen an Personal- und Verwaltungskosten sparen, würden die Kunden ihre Bankgeschäfte nur noch elektronisch betreiben.

Aber auch viele Verbraucher empfinden es als komfortabel, ihre Bankgeschäfte vom heimischen Sofa aus betreiben zu können. Inzwischen nutzen mehr als 27 Millionen Deutsche die elektronische Verbindung zur Bank. Das sind rund 43 Prozent aller Bundesbürger zwischen 16 und 74 Jahren. Als sichere Methode hat sich das Onlinebanking in der Vergangenheit jedoch nicht erwiesen. 2010 registrierte die Statistik der Kriminalpolizei 6 331 Fälle, das bedeutete einen Anstieg um 82 Prozent im Vergleich zum Vorjahr. Im Schnitt belief sich der Schaden auf 4 000 Euro. Das BKA glaubt sogar, dass nur rund 40 Prozent der Fälle überhaupt gemeldet werden.

Und die Diebe halten beinahe Schritt mit der Entwicklung immer raffinierterer Sicherheitssysteme. Sie schicken dem Opfer eine E-Mail mit einem Link, der angeblich von der Bank des Users stammt. Klickt er diesen Link an, glaubt er, dass er sich auf der Homepage seiner Bank befindet. In Wirklichkeit sieht die Seite dem Original nur täuschend ähnlich, aber es handelt sich um eine Fälschung. Bemerkt der Kunde seinen Irrtum nicht und gibt Benutzernamen, Passwort, Kontodaten sowie die Persönliche Identifikationsnummer (PIN) und die Transaktionsnummer (TAN) ein, hat der Täter, was er braucht, um sich auf dem Konto zu bedienen.

Bis vor Kurzem erstatteten die Banken aus Kulanzgründen den gestohlenen Betrag. Am 24. April 2012 aber hat der Bundesgerichtshof BGH (AZ: XI ZR 96/11) zugunsten der Geldwirtschaft entschieden. Ein Kunde, der beim Onlinebanking um 5 000 Euro betrogen wurde, muss für seinen Fehler selbst geradestehen, so das Gericht. Der Kunde hatte die Täuschung nicht bemerkt und die E-Mail für eine Nachricht von seiner Bank gehalten. Er kam der Aufforderung, PIN und TAN anzugeben, nach - und hatte sowohl finanziell wie auch juristisch das Nachsehen.

Firewall unabdingbar

Kaum noch eine Chance, die Fälschung zu erkennen, haben die Nutzer des Onlinebankings beim sogenannten Pharming. Hierbei schleusen die Täter eine Schadsoftware auf den Computer des Kunden. Das geschieht zum Beispiel, wenn man den Anhang einer dubiosen Mail öffnet. Anschließend wird das System so manipuliert, dass die gefälschte Webseite selbst dann erscheint, wenn der Nutzer die korrekte Adresse seiner Bank eingegeben hat. Schützen kann man sich nur mit einer Firewall und einem Virenschutzprogramm.

INFO

Vorsichtsmaßnahmen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt, folgende Punkte zu beachten:

- Zugangs- und Transaktionsdaten nicht auf dem PC oder auf dem Smartphone speichern - auch nicht in einem Passwortmanager. Sichere Passwörter wählen und in regelmäßigen Abständen ändern.

- Onlinebanking sollte immer über das geschützte https-Protokoll erfolgen. Das erkennt man an der Browser-Zeile. Dort steht statt http:// dann https://. Häufig zeigt die Zeile ein Schloss-Symbol. Das bedeutet, dass die Richtigkeit der Adresse zertifiziert ist. Mit einem Klick auf das Schloss erhält man Informationen über das Zertifikat und darüber, ob die Webseite tatsächlich die ist, für die sie sich ausgibt. Bei Unstimmigkeiten sollte die Transaktion sofort abgebrochen werden.

- Nutzer sollten die Echtheit der Bank-Webseite prüfen. Dazu geben sie am besten die Bankadresse jedes Mal neu ein. Wird beim Login schon nach einer TAN gefragt, handelt es sich bestimmt um eine gefälschte Seite. Auch minimale Abweichungen bei der Internetadresse wie Trennungsstriche sind ein Zeichen für eine Fälschung.

- Sicherer ist, nur vom eigenen Computer aus Onlinebanking zu betreiben und Internetcafés für diese Zwecke zu meiden. Nach jeder Sitzung sollte man sich abmelden und nach Beendigung der Transaktionen den Zwischenspeicher (Cache) löschen.

- Es empfiehlt sich, mit der Bank ein Limit für die täglichen Geldbewegungen zu vereinbaren. So können Betrüger nicht unbemerkt höhere Summen abbuchen.

- Regelmäßig die Kontobewegungen überprüfen. Dabei reicht es nicht, sich auf die Online-Auszüge zu verlassen. Besser ist, sich an den am Bankterminal gedruckten Auszügen zu orientieren.

- Nicht auf Phishing-Mails reagieren. Auch wenn Nutzer mit Namen angesprochen werden, dürfen sie sich nicht täuschen lassen. Die Bank fordert ihre Kunden niemals per E-Mail dazu auf, vertrauliche Daten wie PIN, TAN oder Kontonummer bekannt zu geben. Solche Aufforderungen sollten der Bank gemeldet, aber auf keinen Fall befolgt werden.

- Die Weitergabe der Bankverbindung hat in sozialen Netzwerken nichts zu suchen. Auch beim Kauf im Internet sollte man erst einmal prüfen, ob es sich um einen seriösen Anbieter handelt, bevor man die sensiblen Daten preisgibt.

- Bei Verdacht, sofort den Onlinebanking-Zugang sperren. Dazu reicht ein Anruf bei der Bank oder der Kunde gibt die Information über die entsprechende Funktion im Onlinebanking-Fenster weiter.

- Wer Opfer eines Phishing-Angriffs, das sind gefälschte Mail-Nachrichten, um dem Empfänger geheime Daten zu entlocken, oder eines schadhaften Computerprogramms (Trojaner) geworden ist, muss seinen PC fachgerecht von der Schadsoftware befreien (lassen).

Doch gegen Trojaner können auch diese Vorsichtsmaßnahmen häufig nichts ausrichten. Hierbei installieren Kriminelle eine Spionagesoftware auf den Computer des Betroffenen, die ständig den Datenverkehr überwacht. Registriert sie eine Banküberweisung, manipuliert sie unbemerkt Betrag und Empfänger. Das Ergebnis sieht der Geschädigte erst bei der Kontrolle seines Bankauszugs.

Wirklich schützen können sich Bankkunden nur mit viel Aufmerksamkeit, und indem sie immer das sicherste System wählen, das ihre Bank anbietet. TAN-Listen auf Papier haben längst ausgedient. Auch die iTAN, die von der Bank vorgegeben wird, hat sich nicht wirklich bewährt. Clevere Schadprogramme greifen auch darauf zu.

Sicherheitssysteme der Banken
Um von ihrer Seite aus das Onlinebanking so sicher wie möglich zu machen, bieten die Institute inzwischen drei Systeme an, die Dieben den Zugriff auf die Kundenkonten verwehren sollen:

ChipTAN
Für dieses Verfahren lässt der Kunde seine Girocard bei der Bank registrieren und fordert einen TAN-Generator an. Das Gerät ähnelt einem Taschenrechner, verfügt über einen Schlitz für die Karte sowie Display und Tastatur. Bei dem Verfahren gibt der Kunde wie sonst auch seine Daten für die Überweisung am Bildschirm ein. Klickt er auf "weiter", erscheint ein Code. Nun schiebt er die Karte in den Generator und gibt den Code, erneut die Kontonummer des Empfängers und den Betrag ein. Anschließend erscheint auf dem Display eine TAN. Damit bestätigt der Kunde nun auf dem Bildschirm den Überweisungsauftrag. Die TAN funktioniert nur eine begrenzte Zeit.

Manche Generatoren verfügen sogar über optische Sensoren auf der Rückseite. Dann erscheint auf dem Bildschirm statt eines Codes eine schwarz-weiß blinkende Grafik. Hält der Kunde seinen Generator davor, erscheint nach Bestätigung der Auftragsdaten ebenfalls die TAN auf dem Display. Je nach Bank liegen die Kosten für den Generator zwischen null und 15 Euro. Die Sicherheit dieses Verfahrens ist deshalb sehr hoch, weil der Auftrag über zwei getrennte Übertragungswege - Internet und Generator - ausgeführt wird.

Das ChipTAN- Verfahren ist ein Sicherheitssystem von mehreren, das Banken zum Schutz anbieten.

MobileTan
Ist der Kunde bei seiner Bank fürs Onlinebanking angemeldet, teilt er dem Institut die Handynummer mit, an die es die TAN schicken soll. Das Verfahren funktioniert wie gehabt: Der Kunde gibt die Daten für die Überweisung am Computer ein und klickt dann auf "TAN anfordern". Kurz darauf erhält er die geforderte Nummer per SMS auf dem Handy. Mit dabei sind die zuvor in den Computer eingegebenen Daten für die Überweisung. Am Bildschirm gibt der Kunde die TAN in das entsprechende Feld auf der Onlineüberweisung ein und bestätigt so den Auftrag. Nutzt er die TAN nicht, verfällt sie nach kurzer Zeit.

FinTS/HBCI
Während das normale Onlinebanking über Browser funktioniert, kommunizieren die Kunden bei FinTS/HBCI mithilfe eines speziellen Sicherheitsprogramms mit ihrer Bank. Das Kürzel HBCI steht für Homebanking Computer Interface. Damit kann beispielsweise eine Überweisung in verschlüsselter Form über das Internet versendet werden. FinTS oder Financial Transaction Service ist eine Weiterentwicklung dieses Standards. Es gleicht einem Baukasten, mit dem verschiedene Sicherheitsverfahren möglich sind. Funktionsweise: Der Kunde lädt sich das Programm auf seinen Computer. Wählt er die Chipkarte, muss er das Lesegerät anschließen. Für die Überweisung gibt er die Daten ein, für die Bestätigung schiebt er die Karte ins Lesegerät und tippt die PIN der Chipkarte ins Lesegerät ein. Der Kartenchip verschlüsselt daraufhin den Auftrag und versieht ihn mit einer elektronischen Signatur. Anschließend werden die Daten zur Bank geschickt. Die Kommunikation mit der Bank funktioniert nur an einem Computer, auf dem FinTS installiert ist.

Auch Smartphones sichern
Manche Lesegeräte erzeugen eine TAN, die zur Bestätigung des Auftrags dient. Die Kosten für das Programm liegen bei zehn Euro. Lesegeräte kosten zwischen null und 98 Euro und die Chipkarte null bis 15 Euro. Die Sicherheit bei diesen Verfahren gilt als sehr hoch, weil der Computer vor Schadprogrammen geschützt ist und der Auftrag gut verschlüsselt wird. Stand HBCI früher fast ausschließlich Geschäftskunden zur Verfügung, bieten inzwischen viele Banken diese Möglichkeit auch Privatkunden an.

Andrea Heyer, Finanzexpertin der Verbraucherzentrale Sachsen, zeigt sich mit den derzeit angebotenen Verfahren unzufrieden: "Die Banken "drängen" die Kunden ins Onlinebanking. Sie können ihnen aber kein wirklich sicheres System zur Verfügung stellen." Andererseits weiß sie aber aus ihrer täglichen Arbeit auch, dass den Kunden oftmals nicht klar ist, was sie

beim Onlinebanking beachten müssen.

So erledigen besonders junge Leute ihre Kommunikation gern mit Smartphones. Die internetfähigen Minicomputer erlauben Bankgeschäfte in jeder Lebenssituation. Wer sich aber auf dieses Handy auch die nötigen TAN schicken lässt, lädt zum Missbrauch geradezu ein und handelt grob fahrlässig. Verbindet der stolze Besitzer sein Smartphone auch noch mit seinem Computer zu Hause, um sich eventuell Musik herunterzuladen, können Schadprogramme bequem auf den Hauptrechner installiert werden. Deshalb raten Experten dazu, auch Smartphones mit einer entsprechenden Sicherheits-Software auszustatten.

AGB der Banken lesen

Auf dieses Risiko weisen die Banken auch in den Allgemeinen Geschäftsbedingungen (AGB) hin - eine mühsame Lektüre auf die Kunden gerne verzichten. Das weiß auch Verbraucherschützerin Heyer: "Es ist wichtig, dass sich die Bankkunden die AGB genau anschauen bevor sie sich für das Onlinebanking entscheiden. Anschließend sollten sie sich dann fragen, ob sie die darin vorgeschriebenen Pflichten erfüllen können."

Entwickelt sich das Onlinebanking so rasant weiter wie bisher, werden auch die Schadensfälle zunehmen. Zurzeit reicht es aus, wenn Nutzer ihren Computer mit einem Antivirenschutz und einer Firewall schützen, um nicht für einen entstandenen Schaden haften zu müssen. Doch werden die Banken von ihren Kunden ständig mehr Achtsamkeit im Umgang mit den sensiblen Daten verlangen.

Marlene Endruweit
Fachjournalistin Wirtschaft
m.endruweit@netcologne.de

zm 102, Nr. 11, 01.06.2012, Seite 90-92