bankenverband
BUNDESVERBAND DEUTSCHER BANKEN

ONLINE-BANKING-SICHERHEIT

Informationen für Online-Banking-Nutzer
Berlin, Juli 2004

ONLINE-BANKING-SICHERHEIT

Informationen für Online-Banking-Nutzer
Berlin, Juli 2004

Vorbemerkung

Neben den enormen Vorteilen und Möglichkeiten sind mit der Nutzung des Internet auch verschiedene Sicherheitsrisiken verbunden. Deshalb führen die Banken umfangreiche Maßnahmen zur Absicherung der im Rahmen des Online Banking übermittelten und bankseitig verarbeiteten Daten durch. Diese Maßnahmen gewährleisten beispielsweise, dass vertrauliche Daten bei der Übertragung über das Internet nicht unberechtigt eingesehen und nicht unautorisiert verändert werden können.

Auf die von den Kunden der Banken eingesetzten Systeme haben die Banken in der Regel keinen Einfluss. Bankkunden können die Systeme, die sie für das Online Banking einsetzen, frei wählen. Außerdem werden diese Systeme – beispielsweise ein an das Internet angeschlossener PC – in der Regel auch für viele andere Anwendungen genutzt.

Die vom Bankkunden eingesetzten Systeme sind damit potenziellen Gefahren ausgesetzt, die von den Banken nicht kontrolliert werden können. Aus diesem Grund können die Banken keine Haftung für die eingesetzten Systeme übernehmen.

Typische Gefahren im Internet sind heute:

- Mitlesen, Verändern und Löschen von Daten bei der Übertragung.
- Viren, Würmer: Programme, die sich selbständig verbreiten bzw. über E-Mails im Internet versandt werden und Schäden auf Ihrem PC anrichten können.
- Trojanische Pferde: Programme, die unbemerkt vom Nutzer sicherheitskritische Funktionen, wie zum Beispiel das Abfangen von Passworten, durchführen.
- Maskerade oder auch „Phishing“, das heißt Vortäuschung von falschen Namen, Seiten und Adressen.
- Hackereinbrüche: Unberechtigte dringen über das Internet in Ihren PC ein.

Für das Online Banking wurden seitens der Banken bereits eine Reihe von Sicherheitsvorkehrungen getroffen, die einen wirksamen Schutz gegen Angriffe bei der Übertragung der Daten über das Internet oder der Verarbeitung auf dem Bankenserver bieten. Damit die von den Banken vorgesehenen Sicherheitsvorkehrungen aber nicht durch unberechtigte Manipulationen unterlaufen werden können, müssen deshalb auch Ihrerseits Vorkehrungen zum Schutz der von Ihnen eingesetzten Systeme getroffen werden.

Selbstverständlich lauern nicht überall im Internet Gefahren. Nicht jeder Kommunikationspartner will und wird Sie schädigen. Schon wenn Sie die folgenden zehn Regeln beachten, können Sie die Sicherheit an Ihrem PC, den Sie für das Online Banking benutzen, um ein Vielfaches steigern und die verbleibenden Restrisiken auf ein Minimum reduzieren.

Sicherheitsregeln

Regel 1: Schützen Sie sensible Daten bei der Übertragung über offene Netze
Jede ungesicherte Datenübertragung im Internet kann von unberechtigten Dritten abgefangen oder ausgespäht werden. Deshalb sollten Sie sensible Daten niemals unverschlüsselt über offene Netze übertragen. Schützen Sie daher Ihre vertrauliche Korrespondenz durch den Einsatz sicherer Verschlüsselungsverfahren.

Die Banken haben dafür gesorgt, dass die im Rahmen des Online Banking übermittelten Daten bei der Übertragung bereits mit sicheren Verfahren verschlüsselt werden. Geben Sie Ihre PIN und TANs nur ein, wenn Sie sich auf der geschützten Seite der Bank befinden und Sie eine verschlüsselte Verbindung haben. Dies können Sie unter anderem daran erkennen, dass die URL Ihrer Bank mit „https://“ beginnt.

Beachten Sie weiterhin, dass die beim Online Banking übertragenen Daten bei der Speicherung auf dem PC nicht automatisch verschlüsselt werden und deshalb durch weitere Sicherheitsvorkehrungen geschützt werden sollten.

Regel 2: Vergewissern Sie sich, mit wem Sie es zu tun haben
Nicht jeder ist im Internet das, was er zu sein vorgibt. Für Experten ist es vergleichsweise einfach, eine E-Mail-Adresse zu fälschen oder eine ganze Web-Seite vorzugaukeln – eventuell auch die einer Bank, bei der Sie sich einloggen wollen.

Überprüfen Sie die URL, das heißt die Adresszeile des Browsers daraufhin, dass die Adresse Ihrer Bank korrekt wiedergegeben ist. Bereits minimale Abweichungen könnten auf eine gefälschte Web-Seite hinweisen.

Überprüfen Sie auch die vom Browser gelieferten Sicherheitsinformationen wie die Ergebnisse einer „Zertifikatsprüfung“. Mit diesen wird unter anderem die Richtigkeit der Angaben des Servers, mit dem Sie verbunden sind, von einer unabhängigen Instanz bestätigt. Einer Adresse, bei der der (scheinbare) Adressinhaber gleichzeitig

der Zertifikatsaussteller ist, sollten Sie nicht vertrauen. Im Zweifelsfall können Sie sich auch bei Ihrer Bank über die vertrauenswürdigen Instanzen, die Serverzertifikate für das Online-Banking ausstellen, informieren.

Geben Sie Informationen nur preis, wenn Sie verlässlich wissen, wer diese Daten erhält und was mit diesen geschehen soll. Abweichungen vom gewohnten Ablauf sollten Sie misstrauisch machen, zum Beispiel die Aufforderung zur PIN-Eingabe in einem unerwarteten Zeitpunkt.

Vortäuschen einer Vertrauensfunktion ist bei Hackern beliebt, um an benötigte Informationen zu kommen: Hierzu gibt es beispielsweise das so genannte „Phishing", bei dem Sie eine E-Mail erhalten, die angeblich von Ihrem Kreditinstitut stammt. In dieser E-Mail werden Sie dazu aufgefordert, Ihre vertraulichen Zugangsdaten auf der Web-Seite Ihres Instituts zu aktualisieren. Der in der E-Mail angegebene Link führt dann allerdings zu einer gefälschten Web-Seite des Angreifers, der auf diesem Weg Ihre vertraulichen Zugangsdaten ausspäht. Achten Sie deshalb darauf, dass Sie Ihre vertraulichen Zugangsdaten immer nur auf der echten Web-Seite Ihres Instituts eingeben.

Regel 3: Gehen Sie sorgfältig mit sensiblen Daten und Zugangsmedien um
Schützen Sie Ihre Zugangsdaten bzw. Ihr Zugangsmedium zum Online Banking (PINs und TANs bzw. Chipkarte) vor unberechtigtem Zugriff. Speichern Sie sensible Daten (Passworte, PINs und TANs, Kreditkartennummern) insbesondere nicht auf Ihrer Festplatte ab. Dies könnte sonst an PCs, die nicht ausschließlich von Ihnen benutzt werden wie zum Beispiel am Arbeitsplatz, dazu führen, dass Dritte die von Ihnen gespeicherten Daten einsehen können. Auch spezielle Programme, die auf Ihren Rechner gelangt sind, könnten diese Dateien ausspähen und zum Beispiel per E-Mail versenden. Wenn Sie zur Erhöhung der Sicherheit zusätzliche Ausrüstung wie zum Beispiel einen Chipkartenleser mit PIN-Eingabetastatur benutzen, dann geben Sie die dafür vorgesehenen vertraulichen Daten nur dann ein, wenn Sie von diesem Gerät dazu aufgefordert werden.

Speichern Sie vor allem Ihr Passwort für den Anwählvorgang nicht ab. So erschweren Sie den Aufbau unerwünschter Internet-Verbindungen.

Regel 4: Wählen Sie ein sicheres Passwort

Wenn Sie Ihren PC benutzen wollen und beispielsweise eine Anwendung wie das Online Banking starten, müssen Sie sich in der Regel mit einem Passwort ausweisen. Mit Hilfe dieses persönlichen Geheimnisses zeigen Sie, wer Sie sind und beweisen, dass Sie berechtigt sind, an diesem Gerät oder mit dieser Anwendung zu arbeiten. Deswegen kommt es darauf an, dass Sie dieses Geheimnis mit niemandem teilen. Das bedeutet aber auch, dass Sie dieses Kürzel nirgendwo aufschreiben sollten und Sie sich ihr ganz individuelles und schwer zu erratendes Passwort ausdenken.

Ein gutes Passwort ist sechs bis acht Stellen lang und besteht aus einer Mischung aus Groß- und Kleinbuchstaben sowie Ziffern und Sonderzeichen. Auf jeden Fall sollten Sie Eigennamen, wohl bekannte Begriffe, Wiederholungen einzelner Zeichen („AAAAAA“) oder Tastaturfolgen („qwertz“) vermeiden. Für die Auswahl eines schwer zu erratenden Passwortes gibt es verschiedene Strategien: Eine einfache stellt die Bildung des Passwortes aus den Anfangsbuchstaben eines Mottos oder Gedichtes dar. Durch Einfügen von Sonderzeichen oder Ziffern kann es noch weiter verfremdet werden. So kann „VinF&HnH“ etwa für „Vorsicht ist nicht Furcht und Hast nicht Heldenmut“ stehen. Wechseln Sie Ihr Passwort, wenn Sie Grund zur Annahme haben, dass irgend jemand Ihr Geheimnis erfahren haben könnte.

Regel 5: Setzen Sie nur Programme aus vertrauenswürdiger Quelle ein

Laden Sie nur solche Programme aus dem Internet auf Ihre Festplatte, deren Quelle Sie als seriös betrachten können und stellen Sie sicher, dass es sich wirklich auch um diesen Anbieter handelt. Mit Programmen können Viren oder Trojanische Pferde übertragen werden. Dies kann auch durch das Öffnen eines Anhangs einer E-Mail geschehen. Deshalb öffnen Sie solche Anhänge nicht, wenn Ihnen Absender oder Inhalt unbekannt sind. Speichern Sie den Inhalt zuerst ab, prüfen Sie ihn mit entsprechenden Sicherheitsprogrammen und öffnen Sie erst dann die fragliche Datei.

Überlegen Sie sich genau, ob Sie Zusatzprogramme (Plug-Ins) beispielsweise zum Darstellen von 3D-Welten oder zum Audio-Empfang in Ihren Web-Browser einbinden wollen. Denn auch solche Plug-Ins können zusätzliche, unkontrollierbare Sicherheitslücken eröffnen.

Regel 6: Nutzen Sie aktuelle Programmversionen
Nutzen Sie nur die aktuelle Version Ihres bevorzugten Internet-Browsers und des Betriebssystems Ihres PCs. Denn nur die jeweils aktuellen Versionen der gängigen Internet-Software können gewährleisten, dass die bis dahin bekannt gewordenen Sicherheitslücken in diesen Programmen geschlossen sind.

Zusätzlich zu den Programmversionen werden von den Herstellern kleine Programme, so genannte Bug-Fixes oder Patches, entwickelt, die entdeckte Sicherheitsprobleme beheben. Diese Bug-Fixes oder Patches sollten Sie schnellstmöglich installieren, um Ihren PC vor den entdeckten Sicherheitslücken zu schützen. Informieren Sie sich deshalb regelmäßig über die neuesten Entwicklungen: Die meisten Hersteller oder auch die Banken unterhalten entsprechende Informationsdienste. Microsoft bietet beispielsweise auf der Web-Seite http://windowsupdate.microsoft.com einen Check an, der die Aktualität des Internet-Explorers und des Windows-Betriebssystems überprüft und benötigte Patches zur Verfügung stellt.

Regel 7: Führen Sie einen Sicherheitscheck auf Ihrem PC durch
Nehmen Sie sich einige Minuten Zeit, bevor Sie Online Banking über Ihren PC durch führen, und machen Sie einen persönlichen Sicherheitscheck. Aktivieren Sie die vorhandenen Sicherheitsmechanismen, mit denen der Zugriff auf Ihren PC geschützt wird. Diese bestehen beispielsweise in der Eingabe eines Passwortes, das beim Starten des PCs durch das Betriebssystem oder durch den Bildschirmschoner abgefragt wird.

Beachten Sie, dass Sie bei einem nicht nur von Ihnen genutzten PC, wie dies beispielsweise in einem Internet-Café der Fall ist, niemals genau wissen können, welche

Programme im Einzelnen auf diesem PC tatsächlich ausgeführt werden. Auch die Tastaturen können manipuliert sein. Hundertprozentige Sicherheit können Sie hier nicht erwarten. Wenn Sie Online Banking zum Beispiel in einem Internet-Café durchführen, sollten Sie anschließend den Cache des Browsers löschen, damit nachfolgende Nutzer nicht Ihre Seiten und die von Ihnen gegebenenfalls eingegebenen Passwörter ansehen können.

Regel 8: Aktivieren Sie die Sicherheitseinstellungen des Browsers
Aktivieren Sie die Sicherheitseinstellungen Ihres Internet-Browsers. Denn Ihre Sicherheit im Internet lässt sich beträchtlich steigern, wenn Sie die Sicherheitsoptionen Ihres Internet-Browser intelligent einsetzen. Wichtig ist hier vor allem, dass Sie die Zulassung von ActiveX-Controls ausschließen und die Ausführung von Java-Applets nur nach Rückfrage gestatten.

Bei diesen sogenannten „Aktiven Inhalten" handelt es sich um kleine eigenständige Programme, die auf Ihrem PC ausgeführt werden und dort unter Umständen unerwünschte Aktionen auslösen können (z. B. Ihre Passwortdatei per E-Mail versenden). Verwenden Sie nicht die „Auto-Vervollständigen"-Funktion Ihres Browsers, durch die Ihre Eingaben von Benutzernamen und Passworten gespeichert und Übereinstimmungen vorgeschlagen werden.

Cookies legen Informationen in ein ganz spezielles Verzeichnis auf der Festplatte ab, lesen aber keine anderen Daten aus. Im Zweifel entscheiden Sie sich gegen solche „Kekse", die eine fremde Web-Seite auf Ihrer Festplatte ablegt, denn diese Daten könnten auch dazu genutzt werden, Benutzerprofile anzulegen. Doch eine grundsätzliche Ablehnung von Cookies ist nicht in allen Fällen die beste Strategie. Lehnen Sie ein Cookie ab, können Sie möglicherweise einige Webangebote nicht nutzen. Nehmen Sie die Datenpakete an, erkennt Sie der Webserver bei jeder Einwahl wieder. Dem Server ist es so möglich, eine „Akte" zu führen und ein Nutzerprofil zu erstellen. Registriert wird beispielsweise, welche Suchbegriffe verwendet und welche Seiten angesteuert werden. Sind Ihre Vorlieben bekannt, werden Werbe-

banner zielgerichtet nach Ihren Interessen platziert. Durch den Einsatz von zusätzlicher Sicherheitssoftware kann die Erstellung von Nutzerprofilen jedoch verhindert werden. So können Sie die Vorzüge der Cookies nutzen und gleichzeitig verhindern, dass Unbefugte Ihr Verhalten für von Ihnen nicht gewünschte Zwecke auswerten.

Regel 9: Setzen Sie Virenscanner und zusätzliche Sicherheitssoftware ein
Setzen Sie zusätzliche Sicherheitssoftware ein. Denn manche Sicherheitsprobleme lassen sich nicht alleine mit „Bordmitteln" des Betriebssystems lösen. Ein wichtiges Zusatzwerkzeug ist ein leistungsfähiger Virenscanner, der permanent aktualisiert wird und damit in der Lage ist, auch neue Viren zu erkennen. Fast täglich werden neue Viren entdeckt, und es ist durchaus möglich, dass Sie sich bei einem Ausflug in die Online-Welt „infizieren".

Ferner können sich grundsätzlich auch außenstehende Dritte ein Bild von den auf Ihrem PC gespeicherten Daten machen, solange Sie online sind, da Ihr Computer im Netz eine eigene Adresse hat und so von außen erreichbar ist.

Bei unzureichenden Sicherheitsmaßnahmen laufen Sie Gefahr, dass Unbefugte auf die auf Ihrem PC gespeicherten Informationen zugreifen könnten. Außerdem können Hacker auch eine „Hintertür" auf Ihrem PC einbauen und Ihren PC so bei jeder Internetverbindung beispielsweise für das Versenden unerlaubter Werbe-E-Mails unbemerkt missbrauchen. Gegen diese Angriffe von Außen bietet die Installation einer persönlichen Firewall Schutz. Eine Firewall ist ein Programm, das den gesamten eingehenden und ausgehenden Netzverkehr überwacht und nur bekannte oder autorisierte Verbindungen zulässt.

Im Fachhandel gibt es darüber hinaus eine Vielzahl von Programmen, die Ihnen dabei helfen, das Sicherheitsniveau Ihres PCs zu heben, wie beispielsweise PC-Sicherheitssysteme mit Zugriffsschutz und Verschlüsselung.

Regel 10: Fertigen Sie regelmäßig Sicherheitskopien (Backups) Ihrer Daten an
Ganz unabhängig von der Nutzung des Online Banking ist die Datensicherung eine der wichtigsten Regeln für einen Computerbenutzer überhaupt. Denn es ist meist unmöglich oder zumindest sehr aufwändig, die gespeicherten Informationen zu retten, falls das „Kind erst einmal in den Brunnen gefallen ist". Zum bequemen Datensichern können Sie zum Beispiel eine Wechselfestplatte, einen CD- oder DVD-Brenner oder ein Bandlaufwerk einsetzen.

Wichtig ist jedoch, dass Sie regelmäßig eine Sicherung der geänderten sowie der neu dazugekommenen Daten vornehmen. Und bewahren Sie Ihre Backups sicher, das heißt getrennt vom PC und geschützt vor dem Zugriff unbefugter Dritter, auf.

Allgemeine Information zur Sicherheit im Internet erhalten Sie unter der Adresse http://www.sicherheit-im-internet.de.

Glossar

ActiveX-Control	Ein ActiveX-Control ist ein kleines Windows-Programm, das sich beispielsweise mit Hilfe eines Web-Browsers ausführen lässt. Diese Controls können bereits auf dem Rechner vorhanden sein oder werden beim Aufruf einer Web-Seite automatisch heruntergeladen.
Cache	Ein Cache ist ein Zwischenspeicher auf der Festplatte eines Computers oder eines externen Rechners.
Cookie	Ein Cookie ist eine kleine Textdatei, die der Web-Browser auf Anweisung eines Web-Servers in dem PC des Anwenders speichert und die zum Beispiel Angaben über seine Web-Anfragen enthält. Cookies dienen hauptsächlich als elektronischer Merkzettel für den Server, um benutzerspezifische Browser-Abfragen festzuhalten, zum Beispiel, welche Web-Sites ein Nutzer wie häufig und wie lange besucht hat oder ob die angeforderte Web-Seite in einer bestimmten, vom Nutzer festgelegten Version übersandt werden soll.

Firewall	Als Firewall bezeichnet man Rechner, die den Datenverkehr zwischen einem lokalen Netz oder einem allein stehenden Rechner und anderen Netzwerken, zum Beispiel dem Internet, regeln. Die Firewall soll das lokale Netz bzw. Rechner vor unbefugten Zugriffen schützen. Unter einer persönlichen Firewall wird ein Programm verstanden, das auf Ihrem PC eine Firewall realisiert, das heißt Ihren PC ohne Einsatz eines Zusatz-Rechners vor unerwünschten Zugriffen bewahrt.
Java Applet	Java ist eine Anfang der 90er Jahre entwickelte Programmiersprache. Ein Java-Applet ist ein kleines Programm, das – nachdem es aus dem Internet geladen worden ist – innerhalb eines Browsers interpretiert und ausgeführt wird. Hierzu werden die Java-Befehle in HTML-Seiten eingebunden und beim Laden dieser HTML-Seite ausgeführt.
Maskerade	Vortäuschung von falschen Namen, Seiten und Adressen.
Patch	Kleines Programm, das zusätzlich zu den Programmversionen entwickelt wird, um entdeckte Sicherheitsprobleme möglichst zeitnah zu beheben.
Phishing	Angriffmethode, bei der ein Angreifer die E-Mail-Adresse von bekannten Dienstleistern wie Internet-Service-Providern, Internet-Kaufhäusern oder Banken vortäuscht, um die Kunden aufzufordern, ihre Kontodaten sowie dazu gehörige PINs und Passwörter auf einer gefälschten Web-Seite einzugeben.
Trojaner	Trojaner sind Programme, die unbemerkt vom Nutzer sicherheitskritische Funktionen durchführen. Ziel der meisten Trojaner ist es, sensible Daten wie Passwörter auszuspähen und sie per E-Mail/ Internet an den „Besitzer“ des Trojaners zu senden. Mit Hilfe von sogenannten Backdoor-Trojanern kann der Hacker auf fremde Rechner zugreifen und hat dann praktisch die Fernkontrolle über alle Funktionen.
Viren	Computerviren sind Programme, die sich selbst reproduzieren und sich beispielsweise per E-Mail über das Internet weiterverbreiten können. Viren können auf den infizierten PCs teilweise erhebliche Schäden anrichten.
Würmer	Würmer sind Schadprogramme, die sich von Computer zu Computer über das Netzwerk selbsttätig weiter verbreiten. Ziel der Würmer ist es, so viele Computer wie möglich innerhalb eines Netzwerks zu befallen und auf diesen Schäden anzurichten.

ONLINE-BANKING-SICHERHEIT

Berlin, Juli 2004

HERAUSGEBER Bundesverband deutscher Banken

Postfach 040307
10062 Berlin
Telefon (030) 1663-0
Telefax (030) 1663-1299