bankenverband
BUNDESVERBAND DEUTSCHER BANKEN

ONLINE-BANKING-SICHERHEIT

Informationen für Online-Banking-Nutzer
Berlin, Juni 2005

ONLINE-BANKING-SICHERHEIT

Informationen für Online-Banking-Nutzer
5., vollständig aktualisierte Auflage
Berlin, Juni 2005

Vorbemerkung

Neben den enormen Vorteilen und Möglichkeiten sind mit der Nutzung des Internets 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 Ihnen, den Kunden der Banken, eingesetzten Systeme haben die Banken in der Regel keinen Einfluss. Sie können die Systeme, die Sie für das Online Banking einsetzen, frei wählen. Außerdem werden diese Systeme – beispielsweise ein an das Internet angeschlossener PC – von Ihnen 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 diese Systeme übernehmen.

Typische Gefahren im Internet sind heute:

- Mitlesen, Verändern und Löschen von Daten bei der Übertragung
- Viren, Würmer: Programme, die sich selbstständig 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 Passwörtern, durchführen
- Maskerade oder auch Phishing: Vortäuschung von falschen Namen, Internetseiten und Adressen
- Hackereinbrüche: Unberechtigte dringen über das Internet in Ihren PC ein

Für das Online Banking wurden seitens der Banken umfangreiche 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 Sie deshalb auch Ihrerseits Vorkehrungen zum Schutz der von Ihnen eingesetzten Systeme treffen. Dazu gehören insbesondere auch ein sicherheitsbewusstes Verhalten im Internet sowie eine regelmäßige Kontrolle der Kontobewegungen.

Selbstverständlich lauern nicht überall im Internet Gefahren. Nicht jeder Kommunikationspartner will und wird Sie schädigen. Schon wenn Sie die folgenden zehn Regeln beachten, die wir Ihnen nachstehend vorstellen, 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.

Sollten Sie dennoch einmal den Verdacht haben, auf betrügerische Aktionen von Internetkriminellen gestoßen zu sein, dann reklamieren Sie nicht nachvollziehbare Umsätze umgehend bei Ihrer Bank. Bei Betrugsverdacht sollten Sie den Online-Zugang zu Ihrem Konto sofort sperren lassen. Halten Sie hierzu die Kontaktdaten Ihrer Bank bereit. Sichern Sie zwecks Nachvollziehbarkeit des Betrugs relevante Informationen.

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.

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 Ihre TANs nur ein, wenn Sie sicher davon ausgehen können, dass Sie sich auf der geschützten Internetseite der Bank befinden und Sie eine verschlüsselte Verbindung nutzen. 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 lokalen Speicherung nicht automatisch verschlüsselt werden und deshalb durch weitere Sicherheitsvorkehrungen geschützt werden müssen.

Sensible Daten sollten Sie niemals unverschlüsselt über offene Netze übertragen. Schützen Sie daher Ihre vertrauliche Korrespondenz durch den Einsatz sicherer Verschlüsselungsverfahren.

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

Überprüfen Sie die URL, das heißt die Adresszeile des Browsers, daraufhin, ob die Adresse Ihrer Bank korrekt wiedergegeben ist. Bereits minimale Abweichungen könnten auf eine gefälschte Internetseite 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 von Ihnen genutzte 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 zu einem unerwarteten Zeitpunkt.

Um an benötigte Informationen zu kommen, täuschen Hacker gerne Vertrauensfunktionen vor: Hierzu gibt es beispielsweise das so genannte Phishing (eine Zusammensetzung aus den englischen Wörtern „password“ und „fishing“), bei dem Sie von kriminellen Betrügern aufgefordert werden, Ihre vertraulichen Zugangsdaten (zum Beispiel PIN und TAN) auf der Internetseite Ihres Instituts zu aktualisieren oder erneut einzugeben. Die Aufforderung dazu kann sowohl mittels einer E-Mail als auch durch manipulierte Internetseiten erfolgen. Der jeweilige Link führt dann allerdings zu einer gefälschten Internetseite des Angreifers, der auf diesem Weg Ihre vertraulichen Zugangsdaten ausspäht. Stellen Sie sicher, dass Sie Ihre vertraulichen Zugangsdaten immer nur auf der echten Internetseite Ihres Instituts eingeben. Dies können Sie unter anderem dadurch gewährleisten, dass Sie die Internetadresse Ihrer Online-Banking-Verbindung immer nur von Hand in die Adresszeile Ihres Browsers eingeben. Bequemer ist es, die betreffende Internetadresse einmal als Favorit in Ihren Bookmarks abzuspeichern und dann immer darauf zu achten, über diesen Weg die Online-Banking-Verbindung herzustellen. Ferner sollten Sie auf Auffälligkeiten beim Online Banking – beispielsweise auf Abweichungen im Erscheinungsbild des gewohnten Online-Banking-Auftritts Ihrer Bank – achten.

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. Geben Sie die geheimen Zugangsdaten niemals einem Dritten preis.

Speichern Sie sensible Daten (Passwörter, 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 Daten 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, 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 Internetverbindungen.

Vergewissern Sie sich bei jeder Eingabe Ihrer persönlichen Zugangsdaten wie beispielsweise PIN und TAN, dass es sich beim Adressaten um Ihre Bank handelt. Ihre Bank wird Sie niemals zum Beispiel per E-Mail oder auch Telefon kontaktieren und nach Ihren geheimen Zugangsdaten wie PIN und TAN fragen. Beantworten Sie solche E-Mails nicht, und folgen Sie auch nicht den dort angegebenen Instruktionen – selbst wenn Ihnen mit negativen Konsequenzen wie beispielsweise einer Kontosperre gedroht wird. Informieren Sie Ihre Bank über diesen Betrugsversuch.

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 dieser persönlichen Identifikation 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 diese Identifikationshilfe nirgendwo aufschreiben sollten und Sie sich Ihr ganz individuelles und schwer zu erratendes Passwort ausdenken.

Ein gutes Passwort ist in der Regel sechs bis acht Stellen lang und besteht aus einer Mischung aus Groß- und Kleinbuchstaben sowie Ziffern und Sonderzeichen. Beim Internet-Banking wird diese Sicherheit durch die Kombination aus PIN und TAN erreicht. Auf jeden Fall sollten Sie Eigennamen, wohl bekannte Begriffe, Wiederholungen einzelner Zeichen („AAAAAA“) oder Tastaturfolgen („qwertz“) vermeiden. Für die Auswahl eines schwer zu erratenden Passworts gibt es verschiedene Strategien: Eine einfache stellt die Bildung des Passworts aus den Anfangsbuchstaben eines Mottos oder Gedichts 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 irgendjemand 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. Denn: Mit Programmen können Viren oder trojanische Pferde übertragen werden. Dies kann auch durch das Öffnen eines Anhangs einer E-Mail geschehen. Öffnen Sie deshalb solche Anhänge nicht, wenn Ihnen Absender oder Inhalt unbekannt ist. 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 3-D-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 Internetbrowsers und des Betriebssystems Ihres PCs. Denn nur die jeweils aktuellen Versionen der gängigen Internetsoftware 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.

Regel 7: Führen Sie einen Sicherheitscheck auf Ihrem PC durch

Nehmen Sie sich einige Minuten Zeit, bevor Sie Online Banking über Ihren PC durchführen, 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 Passworts, das beim Starten des PCs durch das Betriebssystem oder durch den Bildschirmschoner abgefragt wird.

Grundsätzlich sollten Sie im Internet nicht als Administrator, sondern bei Online-Aktivitäten nur mit minimalen Nutzerrechten arbeiten. Dadurch werden unerlaubte Zugriffe erschwert.

Beachten Sie, dass Sie bei einem nicht nur von Ihnen genutzten PC, wie dies beispielsweise in einem Internetcafé der Fall ist, niemals genau wissen können, inwieweit der Zugang durch aktuelle Sicherheitssoftware geschützt ist und welche Programme im Einzelnen auf diesem PC tatsächlich ausgeführt werden. Auch die Tastaturen können manipuliert sein. Hundertprozentige Sicherheit können Sie hier nicht erwarten. Deshalb ist von Online Banking von solchen Orten aus generell abzuraten. Falls Sie auf Online Banking zum Beispiel in einem Internetcafé nicht verzichten können, sollten Sie anschließend den Cache des Browsers löschen, damit nachfolgende Nutzer nicht Ihre Internetseiten und die von Ihnen eventuell eingegebenen Passwörter ansehen können.

Regel 8: Aktivieren Sie die Sicherheitseinstellungen des Browsers

Aktivieren Sie die Sicherheitseinstellungen Ihres Internetbrowsers. Ihre Sicherheit im Internet lässt sich beträchtlich steigern, wenn Sie die Sicherheitsoptionen Ihres Internetbrowsers intelligent einsetzen. Wichtig ist hier vor allem, dass Sie die Zulassung von ActiveX-Controls ausschließen und die Ausführung von Java-Applets/ Skripten nur nach Rückfrage und Prüfung gestatten.

Bei diesen so genannten aktiven Inhalten handelt es sich um kleine eigenständige Programme, die auf Ihrem PC ausgeführt werden und dort unter Umständen unerwünschte Aktionen auslösen können (zum Beispiel Ihre Passwortdatei per E-Mail versenden). Verwenden Sie nicht die „Auto-Vervollständigen“-Funktion Ihres Browsers, durch die die Eingabe von Benutzername und Passwörtern gespeichert wird 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 Internetseite auf Ihrer Festplatte ablegen, 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 Web-Angebote nicht nutzen. Nehmen Sie die Datenpakete an, erkennt Sie der Web-Server 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 Internetseiten angesteuert werden. Sind Ihre Vorlieben bekannt, werden Werbebanner 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 allein 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. Kriminelle setzen dazu Spyware ein. Diese Spionage-Programme können unbemerkt auf Ihrem Computer installiert werden und sind in der Lage, im Hintergrund nach sensiblen Daten wie Kontoinformationen oder Passwörtern zu suchen oder Ihre Tastatureingaben aufzuzeichnen. Die Daten werden dann ebenfalls unbemerkt an eine fremde E-Mail-Adresse oder einen fremden Server verschickt. Kriminelle bauen Spyware

getarnt in Internetseiten, E-Mails oder E-Mail-Anhänge ein, daher werden solche Programme auch als trojanische Pferde oder Trojaner bezeichnet. Sobald ein infiziertes Objekt geöffnet wird, installiert sich die Spyware auf Ihrem Computer – ohne dass Sie es merken. Deshalb löschen Sie verdächtige E-Mails, ohne sie zu öffnen. Öffnen Sie keine verdächtigen Anhänge, auch wenn sie von einer Ihnen bekannten E-Mail-Adresse zu kommen scheinen. Deaktivieren Sie die „Autovorschau"-Funktion Ihres Mail-Programms, um ein automatisches Öffnen der Mail zu verhindern.

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.

Informieren Sie sich regelmäßig über Sicherheitsaspekte bei der Nutzung des Internets sowie geeignete Schutzmaßnahmen. Informationen zur Sicherheit beim Online Banking erhalten Sie auf der Internetseite Ihrer Bank. Darüber hinaus finden Sie Informationen rund um das Thema Sicherheit im Internet beim Bundesamt für Sicherheit in der Informationstechnik unter der Adresse http://www.bsi-fuer-buerger.de.

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 aufwendig, 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 auf, das heißt getrennt vom PC und geschützt vor dem Zugriff unbefugter Dritter.

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 dessen Web-Anfragen enthält. Cookies dienen hauptsächlich als elektronischer Merkzettel für den Server, um benutzerspezifische Browser-Abfragen festzuhalten, zum Beispiel, welche Web-Seite 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. den allein stehenden 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 Zusatzrechners 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 heruntergeladen 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	Angriffsmethode, bei der ein Angreifer die E-Mail-Adresse oder die Internetseite von Banken und Dienstleistern wie Internetserviceprovidern oder Internetkaufhäusern vortäuscht. Die Kunden werden aufgefordert, ihre Kontodaten sowie dazugehörige PINs, TANs und Passwörter auf einer gefälschten Internetseite einzugeben.

PIN	Persönliche Identifikationsnummer, dient zur Authentifikation einer Person.
Spyware	Als Spyware werden Softwareprogramme bezeichnet, die Informationen über den PC des Nutzers, dessen Surfgewohnheiten oder auch dessen persönliche Daten (zum Beispiel geheime Zugangsdaten für das Online Banking) ohne dessen Wissen oder gar Zustimmung an Dritte senden.
TAN	Transaktionsnummer, dient zur Autorisierung einer Transaktion.
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 so genannten Backdoor-Trojanern kann der Hacker auf fremde Rechner zugreifen und hat dann praktisch die Fernkontrolle über alle Funktionen.
Viren	Computerviren sind Schadprogramme, 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 weiterverbreiten. Ziel der Würmer ist es, so viele Computer wie möglich innerhalb eines Netzwerks zu befallen und auf diesen Schäden anzurichten.

ONLINE-BANKING-SICHERHEIT

5., vollständig aktualisierte Auflage

Berlin, Juni 2005

HERAUSGEBER Bundesverband deutscher Banken

Postfach 04 03 07
10062 Berlin
Telefon (030) 1663-0
Telefax (030) 1663-1299

Der Bankenverband ist die Interessenvertretung der privaten Banken in Deutschland und repräsentiert mehr als 230 Banken mit ca. 170.000 Mitarbeitern.