33. Bundesjugendschreiben 2006 – Autorenkorrektur

Die Bearbeitungsvorlage besteht aus 9 Seiten. Bitte prüfen Sie diese auf Vollständigkeit und Lesbarkeit. Der vorliegende Text ist auf Diskette unter dem Dateinamen *bjs06* in verschiedenen Dateiformaten gespeichert. Bitte laden Sie den Text in den Arbeitsspeicher. Nach der Bearbeitungszeit ist der Text auszudrucken. Bitte beachten Sie, dass ein Ausdruck in Proportionalschrift nicht gestattet ist. In Proportionalschrift ausgedruckte Arbeiten werden vom Wettbewerb ausgeschlossen!

Sicherheit im Internet

Neben den enormen Vorteilen und Mögchkeiten sind mit der Nutzung des Internets auch verschiedene Sicherheitsrisiken verbunden. Deshalb führen die ~~Geld~~institute umfangreiche Maßnahmen zur Absicherung der im Rahmen des Online-Banking übermittelten und bankseitig verarbeiteten Daten durch. Diese Maßnahmen gewehrleisten ~~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 Kreditinstitute eingesetzten Systeme haben die Institute ~~aber~~ keinen Einfluss. Kunden können die Systeme, die sie für das Online-Banking einsetzen, frei wählen. Außerdem werden diese Systeme - ~~beispielsweise~~ ein an ~~an~~ das Internet angeschlossener PC - ~~in der Regel~~ auch für viele andere Anwendungen genutzt.

Die vom Kunden eingesetzten Systeme sind damit potentiellen Gefahren ausgesetzt, die von den Kreditinstituten nicht kontrolliert werden können. Aus diesem Grund können die Kreditinstitute keine Haftung für die eingesetzten Systeme übernehmen.

Die Gefahren im Internet sind sehr vielseitig. Daten können bei der Übertragung mitgelesen, verändert oder auch gelöscht werden. Viren und Würmer können Schäden auf dem PC anrichten. Durch Trojanische Pferde können vom Nutzer unbemerkt sicherheitskritische Funktionen, wie ~~zum Beispiel~~ das Abfangen von Passworten, durchgeführt werden. Durch „Pishing" werden

—fett
li
—unterstreichen
H Kredit
— kursiv
lö H z. B.
H manipuliert
H in der Regel
H z. B.
H ng H meist
lz
lng
lde
— kursiv
—fett
H beispielsweise
lhi

dem Anwender falsche Namen, Seiten und Adressen angezeigt. Hacker dringen unberechtigt über das Internet auf den PC ein.

Für das Online-Banking wurden seitens der ~~Geld~~institute bereits ~~umfangreiche~~ Sicherheitsvorkehrungen getroffen, die einen wirksamen Schutz gegen ~~Hacker~~-Angriffe bei der ~~Daten~~übertragung über das Internet oder der Verarbeitung auf dem Banken-Server bieten.

Damit die von den ~~Geld~~instituten vorgesehenen Sicherheitsvorkehrungen aber nicht durch ~~unberechtigte~~ Manipulationen unterlaufen werden können, müssen deshalb auch vom Kunden Vorkehrungen ~~zum Schutz der von ihnen eingesetzten Systeme~~ getroffen werden.

Selbstverständlich lauern nicht überall im ~~Netz~~ 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 ~~zum Beispiel~~ für das Online-Banking benutzen, um ein Vielfaches steigern und die ~~verbleibenden~~ Risiken 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. Schützen Sie daher Ihre vertrauliche Korrespondenz durch den Einsatz sicherer Verschlüsselungsverfahren. Deshalb sollten Sie sensible Daten niemals unverschlüsselt über offene Netze übertragen.

Die Kreditinstitute haben ~~dafür gesorgt~~, dass die im Rahmen des Online-Banking übermittelten Daten bei der Übertragung bereits mit sicheren Verfahren verschlüsselt werden. Geben Sie Ihre PINs und TANs nur ein, wenn Sie sich auf der geschützten

Seite des Kreditinstituts befinden und Sie eine verschlüsselte Verbindung haben. Dies können Sie ~~unter anderem~~ daran erkennen, dass die URL ~~Ihres Instituts~~ 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 vergibt. Für Experten ist es vergleichsweise einfach, eine E-Mail-Adresse zu fälschen oder eine ganze Web-Seite vorzugaukeln - ~~eventuell~~ auch die eines Kreditinstituts, bei dem Sie sich einloggen wollen.

Prüfen Sie die URL, ~~das heißt~~ die Adresszeile des Browsers daraufhin, dass die Adresse Ihres Kredit instituts korrekt wiedergegeben ist. Bereits ~~kleine~~ Abweichungen können auf eine gefälschte Web-Seite hinweisen. Überprüfen Sie auch die vom Browser gelieferten Sicherheitsinformationen wie die Ergebnisse einer „Zertifikatsprüfung". Mit dieser wird ~~unter anderem~~ die Richtigkeit der Angaben des ~~Versenders~~, mit dem Sie verbunden sind, von einer unabhängigen Instanz bestätigt. Einer Adresse, bei der der (scheinbare) Adressinhaber gleichzeitig der Zertifikationsaussteller ist, ~~sollten~~ Sie nicht vertrauen. Im Zweifelsfall können Sie sich auch bei Ihrem Kreditinstitut ~~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 gescheh soll. Abweichungen vom gewohnten Ablauf sollten Sie misstrauisch machen, ~~zum Beispiel~~ die Aufforderung zur PIN-Eingabe zu einem unerwarten 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 (TANs und PINs bzw. Chipkarte) vor unberechtigtem Zugriff. Speichern Sie sensible Daten (Passworte, TANs und PINs, Kreditkartennummern) insbesondere nicht auf Ihre Festplatte ab. Diese 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~~, dann geben Sie die dafür vorgesehenen vertraulichen Daten nur dann ein, wenn Sie von ~~dem~~ 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 ~~beigen Sie, wer Sie sind und~~ beweisen Sie, dass Sie berechtigt sind, an diesem ~~Gerät~~ oder mit dieser ~~Anwendung~~ zu arbeiten. Deswegen kommt es darauf an,

dass Sie diese 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~~ von Groß- und Kleinbuchstaben sowie Ziffern und Sonderzeichen. Auf jeden Fall sollten Sie Eigennamen, wohl bekannte Begriffe, Wiederholungen einzelner Zeichen oder Tastaturfolgen 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 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.

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 Bugfixes oder Patches, entwickelt, die entdeckte Sicherheitsprobleme ~~beheben~~. Diese Bugfixes 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 Kreditinstitute~~ 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 ~~Stunden~~ 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 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, nie genau wissen können, welche Programme im Einzelnen auf diesem PC ~~tatsächlich~~ ausgeführt werden. Auch die Tastaturen können manipuliert sein. Hundertprozentigen ~~Schutz~~

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-Browsers 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 so genannten „Aktiven Inhalten" handelt es sich um kleine eigene Programme, die auf Ihrem PC ausgeführt werden und dort ~~unter Umständen~~ unerwünschte Aktionen auslösen können (z. B. Passwortdatei per E-Mail versenden). ~~Verwenden Sie nicht die „Auto Vervollständigen"-Funktion Ihres Browsers, durch die Ihre Eingabe von Benutzernamen und Passwörtern gespeichert und Übereinstimmungen vorgeschlagen werden.~~ Cookies legen Daten 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 generelle 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, ~~keine „Akte" zu führen und~~ ein Nutzerprofil zu erstellen. Registriert wird beispielsweise, welche Suchbegriffe verwendet und welche

Seiten 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 Ihre 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 ständig aktualisiert wird und damit in der Lage ist, auch aktuelle Viren zu erkennen. Fast ~~stündlich~~ 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. Weiterhin können Hacker auf eine „Hintertür" auf Ihrem PC einbauen und ~~Ihren~~ PC so bei jeder Internet-Verbindung ~~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.

Thierdurch
Ire
— kursiv
lrg
Tfu lrg
L
— rechtsbündig, fett, kursiv
— größere Schrift
lrg
— doppelt unterstreichen
— täglich
Tög
— rg
— rg Im Hzugreifen
— PC
lrg
Hrg Im Hrg
Ich
Hdem
Hz. B.
— kursiv
— zentrieren
Hverkehr
Hausschließlich
zweizeilig, Blocksatz, Arial, 10pt.

Im Handel 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 ~~da~~zugekommenen Daten vornehmen. ~~Und b~~ewahren Sie Ihre Backups sicher, das heißt getrennt vom PC und geschützt vor dem Zugriff unbefugter Dritter auf

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

Quelle: Online-Banking Sicherheit, RatgeberService der Sparkassen-Finanzgruppe, Bundesverband deutscher Banken e. V., Berlin