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 Möglichkeiten sind mit der Nutzung des Internets auch verschiedene Sicherheitsrisiken verbunden. Deshalb führen die Kreditinstitute umfangreiche Maßnahmen zur Absicherung der im Rahmen des *Online-Banking* übermittelten und bankseitig verarbeiteten Daten durch. Diese Maßnahmen gewährleisten z. B., dass vertrauliche Daten bei der Übertragung über das Internet nicht unberechtigt eingesehen und nicht unautorisiert manipuliert werden können.

Auf die von den Kunden der Kreditinstitute eingesetzten Systeme haben die Institute in der Regel keinen Einfluss. Kunden können die Systeme, die sie für das Online-Banking einsetzen, frei wählen. Außerdem werden diese Systeme – z. B. ein an das Internet angeschlossener PC – meist auch für viele andere Anwendungen genutzt. Die vom Kunden eingesetzten Systeme sind damit potenziellen Gefahren ausgesetzt, die von den Kreditinstituten nicht kontrolliert werden können. Aus diesem Grunde 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. Würmer und Viren können Schäden auf dem PC anrichten. Durch **Trojanische Pferde** können vom Nutzer unbemerkt sicherheitskritische Funktionen, wie beispielsweise das Abfangen von Passworten,

Kommentar: (1)
Kommentar: (2)
Kommentar: (3)
Kommentar: (4)
Kommentar: (5)
Kommentar: (6) (7)
Kommentar: (8)
Kommentar: (9)
Kommentar: (10)
Kommentar: (11) (12)
Kommentar: (13)
Kommentar: (14)
Kommentar: (15)
Kommentar: (16) (17)
Kommentar: (18)
Kommentar: (19)
Kommentar: (20)

durchgeführt werden. Durch „Phishing“ werden dem Anwender falsche Namen, Seiten und Adressen angezeigt. Hacker dringen unberechtigt und unbemerkt über das Internet auf den PC ein.

Für das Online-Banking wurden seitens der Kreditinstitute 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 Banken-Server bieten. Damit die von den Kreditinstituten vorgesehenen Sicherheitsvorkehrungen aber nicht durch Manipulationen unterlaufen werden können, müssen deshalb auch vom Kunden Sicherheitsvorkehrungen getroffen werden.

Selbstverständlich lauern nicht überall im Internet Gefahren. Nicht jeder Kommunikationspartner betrügt. Schon wenn Sie folgende zehn Regeln beachten, können Sie die Sicherheit an Ihrem PC, den Sie für das Online-Banking benutzen, um ein Vielfaches steigern und die 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 unbedingt Ihre vertrauliche Korrespondenz durch den Einsatz sicherer Verschlüsselungsverfahren.

Die Kreditinstitute haben sichergestellt, dass die im Rahmen des Online-Banking übermittelten Daten bei der Übertragung bereits mit *sicheren Verfahren* verschlüsselt

Kommentar: (21) Ende Seite 1
Kommentar: (22)
Kommentar: (23)
Kommentar: (24)
Kommentar: (25) (26)
Kommentar: (27)
Kommentar: (28) (29)
Kommentar: (30)
Kommentar: (31) (32)
Kommentar: (33)
Kommentar: (34)
Kommentar: (35 – 37)
Kommentar: (38)
Kommentar: (39 – 41)
Kommentar: (42) (43)
Kommentar: (44 – 46)
Kommentar: (47)
Kommentar: (Umstellung = 51)
Kommentar: (48)
Kommentar: (49) (50)
Kommentar: (52)
Kommentar: (53) (54)
Kommentar: (55)

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 u. a. daran erkennen, dass die URL mit https:// beginnt. Beachten Sie außerdem, dass die beim Online-Banking übertragenen Daten auf dem PC nicht automatisch verschlüsselt gespeichert werden und deshalb durch weitere Sicherheitsvorkehrungen geschützt werden müssten.

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 – sehr oft auch die eines Kreditinstituts, bei dem Sie sich einloggen wollen.

Prüfen Sie die URL, d. h. die Adresszeile des Browsers daraufhin, dass die Adresse Ihres Kreditinstituts korrekt wiedergegeben ist. Bereits minimale Abweichungen können auf eine **gefälschte** Web-Seite hinweisen. Überprüfen Sie auch die vom Browser gelieferten Sicherheitsinformationen wie die Ergebnisse einer „Zertifikatsprüfung". Mit diesen wird u. a. die Richtigkeit der Angaben des Servers, mit dem Sie verbunden sind, von einer *unabhängigen Instanz* bestätigt. Vertrauen Sie nicht einer Adresse, bei der der (scheinbare) Adressinhaber gleichzeitig der Zertifikationsaussteller ist. Im Zweifelsfall können Sie sich auch bei Ihrem Kreditinstitut 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, z. B. die Aufforderung zur PIN-Eingabe zu einem unerwarteten Zeitpunkt.

Kommentar: (56) Ende Seite 2
Kommentar: (57)
Kommentar: (58)
Kommentar: (59) (60)
Kommentar: (61)
Kommentar: (62)
Kommentar: (63) (64)
Kommentar: (65 – 67)
Kommentar: (68)
Kommentar: (69)
Kommentar: (70) (Blocksatz)
Kommentar: (71) Absatz
Kommentar: (72)
Kommentar: (73)
Kommentar: (74)
Kommentar: (75)
Kommentar: (76)
Kommentar: (77) (78)
Kommentar: (79)
Kommentar: (80) (81)
Kommentar: (81 – 84)
Kommentar: (85)
Kommentar: (86)
Kommentar: (87)
Kommentar: (88)

Vortäuschen einer Vertrauensfunktion ist bei Hackern sehr beliebt, um an benötigte Informationen zu kommen: Hierzu gibt es zum Beispiel 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 Kreditinstituts zu aktualisieren. Der in der E-Mail angegebene Link führt dann aber zu einer **gefälschten Web-Seite** des Angreifers, der auf diesem Weg Ihre vertraulichen Zugangsdaten ausspäht. Achten Sie deshalb darauf, dass Sie Ihre vertraulichen Zugangsdaten ausschließlich auf der echten Web-Seite Ihres Instituts eingeben.

Regel 3: Gehen Sie sorgfältig mit sensiblen Daten und Zugangsmedien um

Schützen Sie immer 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 Ihre Festplatte ab. Diese könnte sonst an PCs, die nicht ausschließlich von Ihnen benutzt werden, wie zum Beispiel an Ihrem Arbeitsplatz, dazu führen, dass Dritte die von Ihnen gespeicherten Daten einsehen können. Auch spezielle Programme, die auf Ihren PC gelangt sind, könnten diese Dateien ausspähen und z. B. per E-Mail versenden. Wenn Sie zur Erhöhung der Sicherheit zusätzliche Hardware wie zum Beispiel einen Chipkartenleser mit PIN-Eingabetastatur verwenden, dann geben Sie die dafür vorgesehenen vertraulichen Daten nur dann ein, wenn Sie von dem Gerät dazu aufgefordert werden. Speichern Sie niemals Ihr Passwort für den

Kommentar: (89 – 91)
Kommentar: (92)
Kommentar: (93)
Kommentar: (94)
Kommentar: (95) (Ende Seite 3)
Kommentar: (96) (97)
Kommentar: (98)
Kommentar: (99)
Kommentar: (100)
Kommentar: (101)
Kommentar: (102)
Kommentar: (103)
Kommentar: (104 – 106)
Kommentar: (107)
Kommentar: (108)
Kommentar: (109)
Kommentar: (110)
Kommentar: (111)
Kommentar: (112 – 113)
Kommentar: (114)
Kommentar: (115 – 116)
Kommentar: (117)
Kommentar: (118 – 119)
Kommentar: (120)
Kommentar: (121)
Kommentar: (122)
Kommentar: (123)
Kommentar: (124 – 125)

Anwählvorgang ab. Dadurch 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 beweisen Sie, dass Sie berechtigt sind, an diesem PC oder mit diesem Programm zu arbeiten. Deswegen kommt es darauf an, dass Sie dieses Geheimnis mit niemandem teilen. Das bedeutet aber auch, dass Sie das Kennwort nirgendwo aufschreiben sollten und Sie sich ihr ganz individuelles und schwer zu erratendes Passwort ausdenken. Ein gutes Passwort ist acht bis zehn Stellen lang und besteht aus einer Kombination 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 Strategie stellt die Bildung des Passwortes aus den Anfangsbuchstaben eines Gedichtes oder Mottos dar. Durch Einfügen von Ziffern oder Sonderzeichen kann es noch weiter verfremdet werden. So kann z. B. „VinF&HnH“ etwa für „Vorsicht ist nicht Furcht und Hast nicht Heldenmut“ stehen. Ändern Sie das Passwort, wenn Sie Grund zur Annahme haben, dass irgendjemand Ihr Passwort erfahren haben könnte.

Kommentar: (126 – 127)
Kommentar: (128 – 130)
Kommentar: (131)
Kommentar: (132)
Kommentar: (133 – 134)
Kommentar: (135)
Kommentar: (136) Ende S. 4
Kommentar: (137)
Kommentar: (138)
Kommentar: (139)
Kommentar: (140)
Kommentar: (141 – 142)
Kommentar: (143)
Kommentar: (144 - 145)
Kommentar: (146)
Kommentar: (147 – 148)
Kommentar: (149)
Kommentar: (150 – 151)
Kommentar: (152)
Kommentar: (153)
Kommentar: (154 – 155)
Kommentar: (156 – 157)

Regel 5: Setzen Sie nur Programme aus vertrauenswürdiger Quelle ein

Kommentar: (158 – 160)

Laden Sie nur Programme aus dem Internet auf Ihre Festplatte, deren Quelle Sie als **seriös** betrachten können und prüfen Sie, ob 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. Öffnen Sie deshalb solche Anhänge nicht, wenn Ihnen Inhalt oder Absender unbekannt sind. Speichern Sie den Anhang 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 Audio-Empfang oder zum Darstellen von 3D-Welten in Ihren Web-Browser einbinden wollen. Solche Plug-Ins können zusätzliche, unkontrollierbare SICHERHEITSLÜCKEN eröffnen.

Kommentar: (161)
Kommentar: (162)
Kommentar: (163 – 164)
Kommentar: (165 – 166)
Kommentar: (167)
Kommentar: (168)
Kommentar: (169 – 171)
Kommentar: (172 – 173)
Kommentar: (174)
Kommentar: (175 – 176)
Kommentar: (177)
Kommentar: (178)
Kommentar: (179 – 180)
Kommentar: (181) (Ende S. 5)

Regel 6: Nutzen Sie aktuelle Programmversionen

Kommentar: (182 - 184)

Nutzen Sie nur die aktuelle Version Ihres bevorzugten Internet-Browsers und des Betriebssystems. Denn nur die jeweils aktuellen Versionen 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 Patches oder Bugfixes sollten Sie schnellstmöglich installieren, um den PC vor den entdeckten Sicherheitslücken zu schützen. Informieren Sie sich deshalb **regelmäßig** über die neuesten Entwicklungen. Die meisten Hersteller unterhalten entsprechende Informationsdienste. Microsoft bietet beispielsweise einen Check an, der die Aktualität des Internet-

Kommentar: (185)
Kommentar: (186 – 187)
Kommentar: (188)
Kommentar: (189)
Kommentar: (190)
Kommentar: (191)
Kommentar: (192)
Kommentar: (193)
Kommentar: (194)
Kommentar: (195)

Explorers und des Windows-Betriebssystems überprüft und benötigte Patches zur Verfügung stellt.

Kommentar: (196 – 197)

Kommentar: (198 – 199 Absatz)

Regel 7: Führen Sie einen Sicherheitscheck auf Ihrem PC durch

Kommentar: (200 – 203)

Nehmen Sie sich einige Minuten Zeit, bevor Sie Online-Banking über Ihren PC durchführen, und machen Sie einen persönlichen Sicherheitscheck.

Kommentar: (204 – 205)

Kommentar: (206)

Aktivieren Sie die vorhandenen Sicherheitsmechanismen, mit denen der Zugriff auf Ihren PC eingeschränkt 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 zum Beispiel in einem Internet-Café der Fall ist, nicht genau wissen können, welche Programme im Einzelnen auf diesem PC ausgeführt werden. Auch die Tastaturen können manipuliert sein. Hundertprozentige Sicherheit können Sie hier dort erwarten. Wenn Sie Online-Banking zum Beispiel in einem Internet-Café durchführen, müssen Sie anschließend den Cache des Browsers löschen, damit nachfolgende Nutzer nicht Ihre besuchten Seiten und die von Ihnen gegebenenfalls eingegebenen Passwörter ansehen können.

Kommentar: (207)

Kommentar: (208)

Kommentar: (209)

Kommentar: (210)

Kommentar: (211 – 212)

Kommentar: (213)

Kommentar: (214)

Kommentar: (215 - 216 Ende S6

Kommentar: 217)

Kommentar: (218)

Kommentar: (219)

Kommentar: (220)

Regel 8: Aktivieren Sie die Sicherheitseinstellungen des Browsers

Kommentar: 221 – 223)

Aktivieren Sie die Sicherheitseinstellungen Ihres Internet-Browsers. Denn Ihre Sicherheit im Internet lässt sich erheblich 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 eigenständige Programme, die auf Ihrem PC ausgeführt werden und dort u. U.

Kommentar: (224)

Kommentar: (225)

Kommentar: (226)

Kommentar: (227)

Kommentar: (228)

Kommentar: (229)

Kommentar: (230)

unerwünschte Aktionen auslösen können (z. B. Passowortdatei per E-Mail versenden). Cookies legen Daten in ein ganz spezielles Verzeichnis auf der Festplatte ab, lesen aber **keine** anderen Daten aus. Entscheiden Sie sich im Zweifel gegen solche „Kekse", die eine fremde Web-Seite auf Ihrer Festplatte ablegt. Denn diese Daten könnten auch dazu genutzt werden, Benutzerprofile anzulegen.

Eine generelle Ablehnung von Cookies ist aber nicht in allen Fällen die beste Strategie. Lehnen Sie ein Cookie ab, können Sie möglicherweise einige Web-Angebote nicht nutzen. Wenn Sie die Datenpakete annehmen, erkennt Sie der Web-Server bei jeder Einwahl wieder. Dem Server ist es so möglich, und ein Nutzerprofil zu erstellen. Registriert wird beispielsweise, welche Suchbegriffe verwendet und welche Seiten angesteuert werden. Sind hierdurch 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 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 täglich werden neue Viren entdeckt, und es ist durchaus möglich, dass Sie sich bei einem Ausflug in die Online-Welt „infizieren". Ferner können grundsätzlich auch außenstehende Dritte auf Ihren PC zugreifen, solange Sie

online sind, da Ihr PC im Netz eine eigene Adresse hat und so von außen erreichbar ist.

Bei unzureichenden Sicherheitsmaßnahmen laufen Sie Gefahr, dass Unbefugte auf Ihren PC zugreifen könnten. Weiterhin können Hacker auch eine „Hintertür“ auf Ihrem PC einbauen und den PC so bei jeder Internet-Verbindung z. B. 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 ausschließlich bekannte oder autorisierte Verbindungen zulässt.

Im Handel gibt es darüber hinaus zahlreiche Programme, die Ihnen dabei helfen, das Sicherheitsniveau Ihres PCs zu heben, wie z. B. 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“. Zur bequemen Datensicherung können Sie zum Beispiel eine Wechselfestplatte, einen CD- oder DVD-

Kommentar: (268)
Kommentar: (269 – 271)
Kommentar: (272 – 273)
Kommentar: (274 – 275)
Kommentar: (276)
Kommentar: (277)
Kommentar: (278 – 279)
Kommentar: (280 – 283) Block
Kommentar: Ende Seite 8
Kommentar: (284 – 285)
Kommentar: (286)
Kommentar: (287 – 289)
Kommentar: (290 – 293)
Kommentar: (294)
Kommentar: (295)
Kommentar: (296 – 297)

Brenner oder ein Bandlaufwerk benutzen. Wichtig ist jedoch, dass Sie **regelmäßig** eine Sicherung der geänderten sowie der neu hinzugekommenen Daten vornehmen. Bewahren Sie Ihre Backups sicher, das heißt getrennt vom PC und geschützt vor dem Zugriff unbefugter Dritter, auf!

Allgemeine 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

Kommentar: (298)

Kommentar: (299)

Kommentar: (300)

Kommentar: (301)

Kommentar: (302 – 303)

Kommentar: (304 – 306)