Deutsches
Sicherheitsnetz e.V.

Studie zur Browsersicherheit 2008

veröffentlicht September 2008

0 Verzeichnisse

0.1 Inhaltsverzeichnis

Deutsches Sicherheitsnetz e. V.
Schauenburgerstraße 116
D-24118 Kiel

Telefon: 0431 530237-50
info@deutsches-sicherheitsnetz.de
Fax: 0431 530237-59

Kieler Volksbank eG
Kontonummer: 513 80 70 6
BLZ: 210 900 07

0.2 Abbildungsverzeichnis

Deutsches Sicherheitsnetz e. V.
Schauenburgerstraße 116
D-24118 Kiel

Telefon: 0431 530237-50
info@deutsches-sicherheitsnetz.de
Fax: 0431 530237-59

Kieler Volksbank eG
Kontonummer: 513 80 70 6
BLZ: 210 900 07

1 Zusammenfassung

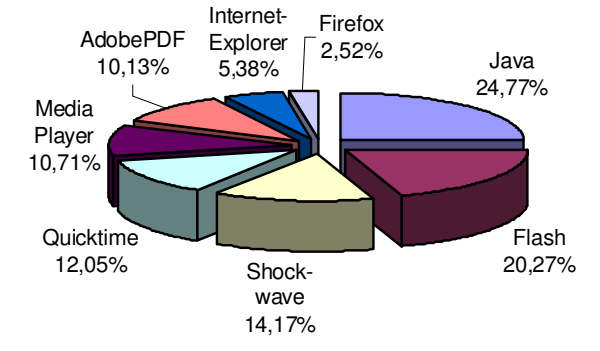
1.1 Motivation

Im Rahmen seiner kontinuierlichen Beobachtungen zur Sicherheit auf privaten PCs ist das Deutsche Sicherheitsnetz auf eine neue Methode gestoßen, wie PCs in privaten Haushalten mit schädlicher Software infiziert werden können - ohne dass der Nutzer etwas davon bemerkt. **Es zeigte sich, dass ein PC bereits durch das reine Betrachten von Bildern oder Videos angegriffen werden kann („Multimedia-Drive-by-Infektion“).**

1.2 Technik

Um diese Angreifbarkeit genauer zu analysieren, hat das Deutsche Sicherheitsnetz ein spezielles Testprogramm entwickelt. **Unter www.desine.de kontrolliert der kostenlose Online-Browsercheck sicherheitskritische Schwachstellen in den Video-, Audio und Dokumentformaten von Flash, Adobe-PDF, Quicktime und Microsoft.** Ist eine dieser Multimedia-Komponenten fehlerhaft programmiert, so kann ein Angreifer durch ein gefälschtes Video oder ein manipuliertes Bild den PC des Nutzers okkupieren.

1.3 Ergebnisse



Schwachstellen in Multimedia-Komponeneten und Browsern

Im Rahmen dieser Studie wurden 67.870 PCs in privaten Haushalten auf Multimedia-Sicherheitslücken hin untersucht. Über 63 % aller PCs sind über Multimedia-Komponenten im Browser angreifbar. Betroffen sind alle großen Hersteller von Multimedia wie Apple (Quicktime), Microsoft (Media Player), Sun (Java) oder Adobe (Flash, PDF). Dadurch wird fast jeder PC angreifbar, der nicht explizit auf die Sicherheit seiner Multimediakomponenten hin untersucht wurde. Für einen Angriff können manipulierte Videos und Multimediadateien eingesetzt werden. So wird es möglich, dass bereits durch das bloße Ansehen eines Videoclips oder das einfache Aufrufen einer Webseite, ein Spionageprogramm übertragen wird.

1.4 Der Verein

Das Deutsche Sicherheitsnetz e. V. hat sich zum Ziel gesetzt, die Internet-Sicherheit bei der privaten Computernutzung in Deutschland zu erhöhen. Hierzu bietet der Verein in Kooperation mit Banken, Sparkassen und Versicherungen einen PC-Pannendienst für jedermann an. Begleitend zu dieser Studie hat der Verein einen kostenlosen Browsercheck ins Netz gestellt, mit dem Multimedia-Sicherheitslücken erkannt werden können.

Deutsches Sicherheitsnetz e. V.
Schauenburgerstraße 116
D-24118 Kiel

Telefon: 0431 530237-50
info@deutsches-sicherheitsnetz.de
Fax: 0431 530237-59

Kieler Volksbank eG
Kontonummer: 513 80 70 6
BLZ: 210 900 07

2 Motivation

Vor etwa einem halben Jahr hat der Verein Deutsches Sicherheitsnetz e. V. eine umfangreiche Untersuchung zur Sicherheit von Personalcomputern in privaten Haushalten in Auftrag gegeben. Im Fokus dieser Untersuchung lag eigentlich die Schwachstellenanalyse der verschiedenen Windows-Betriebssysteme sowie der Anbindung an das Internet. Im Rahmen der Auswertungsarbeiten sind erste Hinweise aufgetaucht, dass im Kontext der Multimedia-Komponenten von Internet-Browsern ein ungeahnt großes Gefahrenpotenzial liegen könnte.

2.1 Anlass zur Sorge

Um das Vorhandensein von Schwachstellen innerhalb von Browser-Komponenten kurzfristig zu klären, hat das Deutsche Sicherheitsnetz e. V. bereits im Juli 2008 den Prototypen eines Online-Browserchecks seinen Mitgliedern zur Verfügung gestellt. Die ersten Untersuchungsergebnisse haben deutlich gemacht, dass etwa die Hälfte aller mit dem Internet verbundenen PCs über die Video- und Audio-Komponenten ihrer Internet-Browser angreifbar ist.

2.2 Plugins und Browser

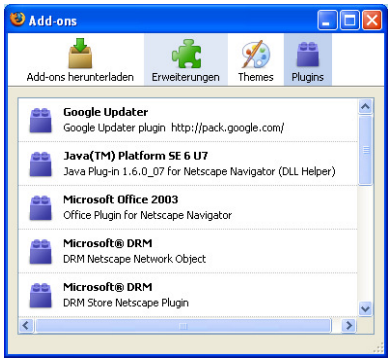


Abbildung 1 "Firefox Plugins"

Der Internet-Browser ist das Daten-Tor zum World Wide Web. Durch ihn müssen alle digitalen Informationen laufen. Das betrifft Musik, Videos, Texte und PDF-Dokumente. Damit ein Internet Browser mit möglichst vielen Multimedia-Formaten umgehen kann, bedient er sich zumeist so genannter Plugins oder auch Addins. Darunter versteht man kleine Programme, die innerhalb des Browsers ihren Dienst verrichten. Sie ermöglichen die Darstellung von Bildern, das Abspielen von Internet-Videos oder das anhören von Online-Musikstücken.

Wie jede Technik, lassen sich jedoch auch die Plugins innerhalb eines Browsers ausnutzen, um schädliche Programme oder Trojaner auf den PC zu laden.

2.3 Gefährdungspotential

Ist eine dieser Multimedia-Komponenten fehlerhaft programmiert, so kann ein Angreifer durch ein gefälschtes Video oder ein manipuliertes Bild den PC des Nutzers okkupieren. Betroffen sind aktuell alle großen Hersteller von Multimedia-Komponenten wie Apple (Quicktime), Microsoft (DirectX, Media-Player) und Adobe (Flash, PDF). Dadurch wird fast

Deutsches Sicherheitsnetz e. V.
Schauenburgerstraße 116
D-24118 Kiel

Telefon: 0431 530237-50
info@deutsches-sicherheitsnetz.de
Fax: 0431 530237-59

Kieler Volksbank eG
Kontonummer: 513 80 70 6
BLZ: 210 900 07

jeder PC angreifbar, der nicht explizit auf die Sicherheit seiner Multimediakomponenten hin untersucht wurde. Für einen Angriff können manipulierte Videos und Multimediadateien eingesetzt werden. So wird es möglich, dass bereits durch das bloße Ansehen eines Videoclips oder das einfache Aufrufen einer Webseite, ein Spionageprogramm übertragen werden kann. Dieser Umstand kann gar nicht deutlich genug betont werden: im Falle von Angriffen über fehlerhafte Browser-Komponenten muss der Nutzer nicht einmal mehr auf eine Datei oder ein Video klicken, es genügt das einfache Besuchen einer Seite, um die Infektion des eigenen PCs auszulösen.

2.3.1 Alle Browser sind betroffen

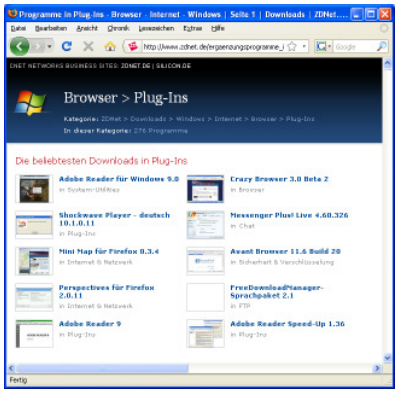


Abbildung 2 "Beliebteste Plugins bei zdnet.de"

Die technische Möglichkeit über Multimedia-Komponenten den PC anzugreifen, besteht derzeit bei allen Browsern vom Internet-Explorer über Firefox bis hin zu Opera, Safari und dem neuen Google-Browser Chrome. Ausgenommen sind nicht einmal die Browser auf Mobiltelefonen oder Spielkonsolen. Dieser Umstand kommt potentiellen Angreifern entgegen, da sie nicht mehr für jeden einzelnen Browser ein extra Angriffs-Programm schreiben müssen, sondern durch die Manipulation von Multimedia-Inhalten, die auf allen PCs gleich aussehen, ein universelles Tor zu jedem Computer finden.

2.3.2 Multimedia-Drive-by-Infektionen

Gerade im anbrechenden Web-2.0-Zeitalter sind interaktive Funktionen und Multimediainhalte jedoch die Voraussetzung für jedwede Kommunikation und Interaktion. Das Internet der Zukunft wird uns also noch mehr Plugins und noch mehr Multimedia bescheren, als dies heute bereits der Fall ist. Mit jeder zusätzlichen Video-Funktionen und jedem zusätzlichen Medien-Format steigen aber auch die Aussichten sich beim Besuchen einer manipulierten Internetseite mit einem Schadprogramm der zweiten Generation zu infizieren. Da diese Infektionen nicht mehr auf eine Interaktion des Benutzers angewiesen sind, werden sie im englischen Sprachgebrauch auch häufig als Drive-by-Infections, also Infektion im vorbeifahren bezeichnet. Bereits heute sind viele Schadprogramme bekannt, die über solche Mechanismen Schwachstellen im Browser und im Betriebssystem ausnutzen. Einen echten Boom könnte diese Technik erfahren, wenn die Angreifer sich professionell und massenhaft auf Schwachstellen in den Multimedia-Komponenten „einschießen“.

Deutsches Sicherheitsnetz e. V.
Schauenburgerstraße 116
D-24118 Kiel

Telefon: 0431 530237-50
info@deutsches-sicherheitsnetz.de
Fax: 0431 530237-59

Kieler Volksbank eG
Kontonummer: 513 80 70 6
BLZ: 210 900 07

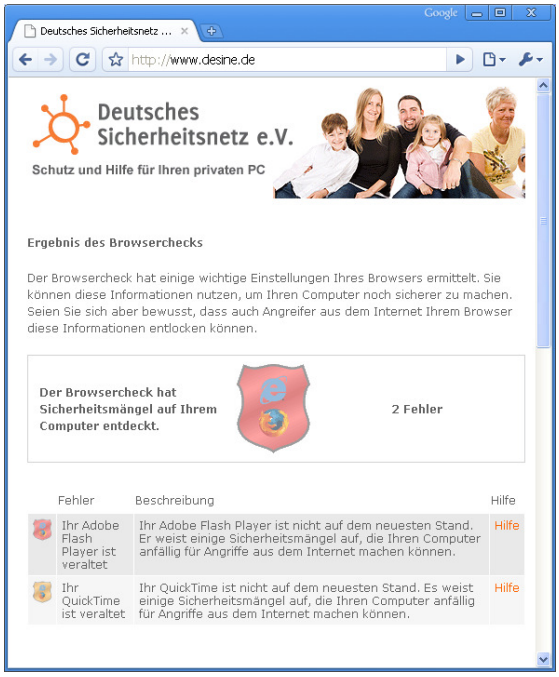


Abbildung 3 "Fehler bei Google Chrome"

Um hier eine Abgrenzung vorzunehmen: Die beschriebenen Technologien zur Ausnutzung von Multimedia-Schwachstellen sind tatsächlich vorhanden. Es gibt erste Schadprogramme, die Schwachstellen in Flash oder Fehler in PDF-Dokumenten ausnutzen. Es handelt sich allerdings noch nicht um ein Massenphänomen. Diese Studie fokussiert sich auf die potenzielle Möglichkeit zur Ausnutzung von Multimedia-Schwachstellen, sie sagt nicht aus, dass diese Technologien bei Kriminellen bereits heute massenweise im Einsatz sind. Um es ganz deutlich zu formulieren: Browser-Komponenten und Multimedia-Funktionen bieten für Kriminelle einen idealen Zugang auf den heimischen PC, das ist technisch unstrittig. In der tatsächlichen Verbreitung ist dieses Phänomen jedoch bis heute eher eine Randerscheinung.

2.3.3 Typische Verbreitungswege

Wer einen Computerschädling auf dem PC eines unbedarften Anwenders platzieren möchte, hat hierzu prinzipiell drei Möglichkeiten. Sehr verbreitet ist die Variante einer Infektion über Werbeeinblendungen. Die Kriminellen treten hierbei wie ein Werbepartner auf und bieten Betreibern von Foren und Portalen an, eine Einblendung ihrer Inhalte (zumeist als i-Frame) vorzunehmen. Über diese manipulierten Werbeeinblendungen wird dann versucht dem Besucher des Forums oder des scheinbar harmlosen Internetportals einen Computerschädling unterzuschieben. Ein zweiter Weg besteht in der Ausnutzung von typischen Tippfehlern, die man beim eintippen einer Internet-Adresse häufig macht. Vertippt man sich bei einem Buchstaben oder verwechselt z. B. den Buchstaben „O“ mit der Zahl „Null“, so kann es passieren, dass man auf speziell präparierten Seiten landet, über die Schadsoftware verbreitet wird. Die dritte und letzte Variante ist die Durchführung von Drive-by-Infektionen über bekannte, scheinbar vertrauenswürdige Internetseiten. Die Kriminellen greifen Schwachstellen auf dem Server des Seiten-Anbieters an und manipulieren dann den gesamten Internetauftritt so, dass den arglosen Besuchern schädliche Programme untergejubelt werden. Diese letzte Variante des Vorgehens ist vor wenigen Wochen zu zweifelhaftem Ruhm gelangt, als eine manipulierte britische Regierungsseite einen Trojaner tausendfach verbreitete.

Deutsches Sicherheitsnetz e. V.
Schauenburgerstraße 116
D-24118 Kiel

Telefon: 0431 530237-50
info@deutsches-sicherheitsnetz.de
Fax: 0431 530237-59

Kieler Volksbank eG
Kontonummer: 513 80 70 6
BLZ: 210 900 07

2.3.4 Gegenmaßnahmen

Konnte man bisher Hacker-Angriffe sehr effektiv durch Firewallsoftware blockieren, so ist der Angriff auf die Video- und Audio-Komponenten des Internet-Browsers kaum zu verhindern, denn wer alle Multimedia-Funktionen blockiert, kann auch das Internet in seiner heutigen bunten und vielschichtigen Art nicht mehr sinnvoll nutzen. Das Abschalten aller Video-, Grafik- und Audio-Funktionen führt dazu, dass eine Internetseite nur noch aus „schwarzem Text auf weißem Grund“ besteht - ohne Klänge, ohne Bilder und ohne Farben. Der größte Schaden, den die neuen Technologien anrichten liegt aber in der Verunsicherung des Internet-Nutzers. Denn die alte Regel „besuche nur vertrauenswürdige Seiten und Du bist immer sicher“ verliert hierdurch jede Berechtigung.

An dieser Stelle hilft einzig und allein das händische aktualisieren jeder einzelnen Multimedia-Komponente. Das deutsche Sicherheitsnetz hat für alle, die freiwillig am Test teilgenommen haben, eine Installations-Hilfe zusammengestellt, über die man fehlerhafte Plugins reparieren oder versäumte Aktualisierungen nachholen kann. Sowohl der Test als auch die zur Verfügung gestellten Downloads für das Schließen erkannter Sicherheitslücken stehen weiterhin jedem Nutzer auf der Internetseite des Vereins zur Verfügung.

Deutsches Sicherheitsnetz e. V.
Schauenburgerstraße 116
D-24118 Kiel

Telefon: 0431 530237-50
info@deutsches-sicherheitsnetz.de
Fax: 0431 530237-59

Kieler Volksbank eG
Kontonummer: 513 80 70 6
BLZ: 210 900 07

3 Technik

In dieser Studie wurden insgesamt 67.870 Personalcomputer in privaten Haushalten auf ihre Sicherheitseinstellungen hin untersucht. Die Untersuchung wurde mit Hilfe eines Online-Browserchecks direkt im Internet durchgeführt.

3.1 Testfeld

Im Zeitraum vom 15. August bis zum 15. September 2008 haben insgesamt 77.394 Internet-Benutzer die Seite des Deutschen Sicherheitsnetz e. V. im Internet besucht. Von diesen haben sich 67.870 dafür entschieden ihren eigenen Browser mit Hilfe des kostenlosen Online-Browserchecks zu überprüfen. Das Prüftool steht auch heute noch unter der Adresse www.desine.de zur Verfügung.

3.1.1 Voraussetzungen

Bei dem Online-Browsercheck handelt es sich um eine klassische JEE-Client-Server-Applikation, die der interessierte Nutzer über seinen Internet-Browser starten kann. Eine Installation von Software, Plugins oder ActiveX-Controls auf dem eigenen PC ist hierfür nicht notwendig. Die Applikation wird vollständig serverseitig ausgeführt und erfordert auf Clientseite lediglich ein funktionsfähiges Betriebssystem mit Internet-Browser und der Fähigkeit zum Umgang mit Java-Skript Funktionen.

3.1.2 Browserverteilung

Die folgenden beiden Grafiken zeigen die Browserverteilung der Besucher der Testseite sowie die Browserverteilung bei den tatsächlichen Testteilnehmern. Bei den Besuchern der Testseite ergibt sich ein typisches Bild mit einer deutlichen Dominanz des Internet-Explorers von über 70 % aller Besucher. Auf Platz zwei liegt der Firefox Browser mit 22 % gefolgt von Google Chrome, Opera und Safari. Interessant ist, dass die Browserverteilung der Personen, die letztendlich am Test teilgenommen haben, deutlich anders aussieht. Die hohe Dominanz des Internet-Explorers ist hier gebrochen. Fast auf Augenhöhe agieren Microsoft und der Konkurrent Firefox. Lag der Anteil der Besucher mit Opera-Browser noch bei 0,7% so liegt der Anteil der Testteilnehmer mit Opera-Browser bei beachtlichen 3,45%. Beides deutet darauf hin, dass das Testangebot zu einem hohen Anteil von technisch interessierten Besuchern wahrgenommen worden ist. Gerade bei technologieaffinen Menschen ist die Verbreitung von alternativen Browsern deutlich höher als beim Durchschnittsdeutschen.

Deutsches Sicherheitsnetz e. V.
Schauenburgerstraße 116
D-24118 Kiel

Telefon: 0431 530237-50
info@deutsches-sicherheitsnetz.de
Fax: 0431 530237-59

Kieler Volksbank eG
Kontonummer: 513 80 70 6
BLZ: 210 900 07

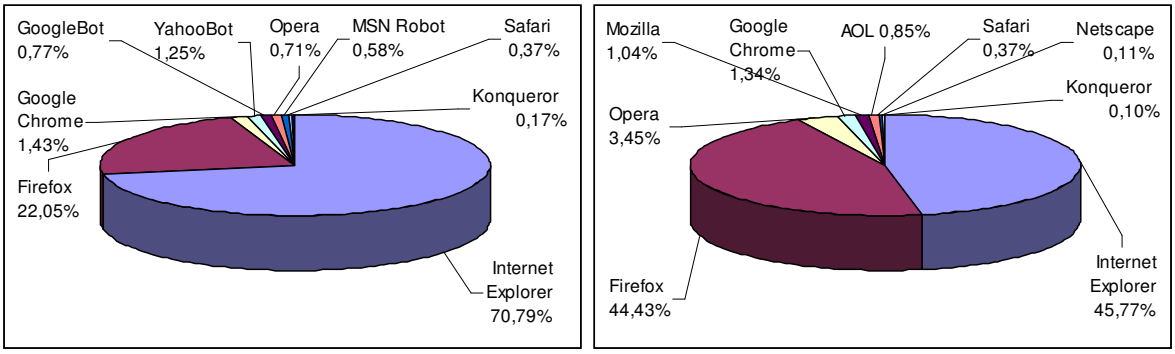


Abbildung 4 "Browserverteilung Besucher und Testteilnehmer grafisch"

Browserverteilung der Besucher	Anteil	Browserverteilung Testteilnehmer	Anteil
Internet Explorer	70,79%	Internet Explorer	45,77%
Firefox	22,05%	Firefox	44,43%
Google Chrome	1,43%	Opera	3,45%
YahooBot	1,25%	Google Chrome	1,34%
GoogleBot	0,77%	Mozilla	1,04%
Opera	0,71%	AOL	0,85%
MSN Robot	0,58%	Safari	0,37%
Safari	0,37%	Netscape	0,11%
Konqueror	0,17%	Konqueror	0,10%

Abbildung 5 "Browserverteilung Besucher und Testteilnehmer tabellarisch"

3.1.3 Betriebssystemverteilung

Die Verteilung der getesteten Betriebssysteme spiegelte deutlich die eigentliche Zielsetzung des Browserchecks wider: Den Test von Windows Betriebssystemen auf Sicherheitslücken innerhalb der Browser Architektur. Demzufolge lag der Anteil der getesteten Windows Betriebssysteme bei insgesamt 94 %. Der Löwenanteil von über 75 % geht hierbei auf das Betriebssystem Windows XP zurück, auf Platz zwei folgt Vista mit 16,5 %, die älteren Windows Betriebssysteme von Win2000 bis Win95 teilen sich die verbleibenden 2,7 %. Der Anteil von Linux/Unix Nutzern lag bei 1,37 % und damit noch knapp vor dem Anteil der Benutzer mit Macintosh Betriebssystem (1,13 %). Interessant ist hierbei dass mit insgesamt 0,2 % der Testteilnehmer auch mobile Betriebssysteme (iPhone, Nokia, Motorola, SonyEricson) und Spielkonsolen (Playstation3, Wii) getestet wurden.

Deutsches Sicherheitsnetz e. V.
Schauenburgerstraße 116
D-24118 Kiel

Telefon: 0431 530237-50
info@deutsches-sicherheitsnetz.de
Fax: 0431 530237-59

Kieler Volksbank eG
Kontonummer: 513 80 70 6
BLZ: 210 900 07

Betriebssystem	Anteil
Windows XP SP2/3	39,33%
Windows XP SP1	35,78%
Windows Vista	16,55%
Windows 2000	1,65%
Linux	1,37%
MacOS X	1,13%
Windows 98	0,58%
Windows 2003	0,25%
Windows Me	0,17%
Windows NT	0,03%
Symbian OS	0,02%
Windows 95	0,01%
FreeBSD	0,01%

Abbildung 6 "Verteilung der Betriebssysteme tabellarisch“

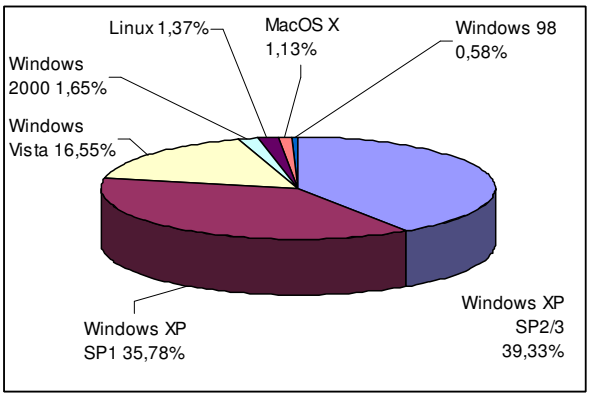


Abbildung 7 "Verteilung der Betriebssysteme grafisch“

3.1.4 Länderverteilung

Domain / Länder	Anteil
.net	42,55%
.de Deutschland	34,32%
.ch Switzerland	18,77%
.at Austria	1,75%
.com	1,73%
.nl Niederlande	0,16%
.fr France	0,09%
.be Belgien	0,08%
.it Italien	0,06%
.li Liechtenstein	0,06%
.lu Luxembourg	0,05%

Abbildung 8 "Domain / Länder Verteilung der Seitenbesucher“

Die Zuordnung der Besucher der Internetseite auf Länder erfolgte im Rahmen dieser Studie über die Analyse des so genannten Referers. Der Referer ist eine Dateninformation, die der Internet-Browser beim Besuch einer neuen Seite übergibt. Hierin wird angegeben, woher der Besucher ursprünglich gekommen ist. Die einzelnen Daten wurden bezüglich ihrer Herkunft ausgewertet. Hierbei wurde lediglich auf Domain-Ebene eine Entscheidung und Zuordnung zu den jeweiligen Herkunftsdomänen und den damit verbundenen Ländern aufgestellt. Da es sich um ein deutschsprachiges Testangebot handelte war zu erwarten, dass der überwiegende Anteil der Besucher aus den Domain-Regionen „.de„, also Deutschland, „.ch“ Schweiz und „.at“ Österreich herrührt. Internationale Domain-Kürzel wie „.com“ oder „.net“ konnte nicht nach Herkunftsländern aufgespalten werden.

3.1.5 Zugangsverteilung

Um nachzuvollziehen, inwieweit es sich bei den Testteilnehmern um typische Privatpersonen handelt, wurden die Daten der Internetprovider der Seitenbesucher mit protokolliert. Es ergab sich ein typisches Bild, wie es in Deutschland für die Internetnutzung in privaten Haushalten üblich ist. 44 % aller Nutzer hat über einen Internetknoten von T-Online

Deutsches Sicherheitsnetz e. V.
Schauenburgerstraße 116
D-24118 Kiel

Telefon: 0431 530237-50
info@deutsches-sicherheitsnetz.de
Fax: 0431 530237-59

Kieler Volksbank eG
Kontonummer: 513 80 70 6
BLZ: 210 900 07

auf den Test zugegriffen, an zweiter Stelle folgt Arcor, an dritter Stelle bereits ein Schweizer Internetanbieter.

Provider	Anteil
t-dialin.net	30,30%
t-ipconnect.de	14,35%
arcor-ip.net	8,28%
bluewin.ch	8,11%
pppool.de	3,83%
hispeed.ch	3,77%
alicedsl.de	3,54%
adslplus.ch	2,49%
versanet.de	2,27%
einsundeins.de	1,53%
ewe-ip-backbone.de	1,10%
netcologne.de	0,88%

Abbildung 9 "Provider Verteilung"

3.2 Prüfkriterien

Es wurden die Aktualisierungsstände der beiden am meisten verbreiteten Browser, Internet Explorer und Firefox, sowie der meistverbreiteten Browser-Plugins kontrolliert. Abgefragt wurde, ob die aktuell verfügbare Version des Browsers bzw. des Plugins mit dem getesteten Versionsstand des Browsers bzw. des Plugins übereinstimmte. Im Falle des nicht Übereinstimmens wurde geklärt, ob diese Differenz auf eine sicherheitskritische Lücke zurückzuführen ist. War dies der Fall, so wurde der Browser als angreifbar bewertet.

	2000	2005	2006	2007	2008e
Sicherheitslücken **Flash**/Plugin	1	1	6	9	11
Sicherheitslücken **Quicktime**/Plugin	0	17	19	37	36
Sicherheitslücken **Acrobat**/Plugin	1	9	6	6	20
Bekannte **Exploits** (Codeausführung)	0	25	30	34	57
Plug-ins für den **Internet-Explorer**	13	→			878
Plugins für den **Firefox**/NCP-Browser	108	→			2980
Quellen: National Vulnerability Database (nvd.nist.gov), Mozilla.org, zdnet.de					

Abbildung 10 "Übersicht zu kritischen Schwachstellen in Plugins"

3.2.1 Flash

Für das Flash-Plugin wurde die aktuelle Version 9.0.124.0 des Flash-Players über den

Deutsches Sicherheitsnetz e. V.
Schauenburgerstraße 116
D-24118 Kiel

Telefon: 0431 530237-50
info@deutsches-sicherheitsnetz.de
Fax: 0431 530237-59

Kieler Volksbank eG
Kontonummer: 513 80 70 6
BLZ: 210 900 07

gesamten Testzeitraum hinweg als sicher bewertet. Alle Versionen mit kleineren Ständen als 9.0.124.0 wurden als unsicher und angreifbar bewertet. Diese Beurteilung geht auf Einschätzungen des Warn- und Informationsdienstes des Bundesamtes für Sicherheit zurück, der in seinen CERT-Bund Meldungen CB-K08/0201 und CB-K08/0482 das Flash-Plugins als angreifbar und anfällig für Remote-Codeausführung bezeichnet. Auch das US-CERT benennt verschiedene Sicherheitslücken Schwachstellen in Flash (VU#159523, VU#758769, VU#730785, VU#451380) die geeignet sind schädliche Programme auf dem PC zu platzieren. Verschärfend kommt hinzu, dass für verschiedene Sicherheitslücken im Umfeld von Flash seit Ende Mai Exports bekannt sind, die tatsächliche Infektionen auf dieser Basis durchführen.

3.2.2 Quicktime

Für das Quicktime-Plugin wurde die aktuelle Version 7.5.5 über den gesamten Testzeitraum hinweg als sicher bewertet. Alle älteren Versionen mit geringeren Versionsständen als 7.5.5 sind momentan als unsicher und angreifbar zu bewerten (siehe auch CERT-Bund CB-K08/0333, CB-K08/0248, CB-K07/0861, CB-K07/0557).

3.2.3 Shockwave

Für Shockwave/Flash wurde über den gesamten Testzeitraum hinweg die Version 11.0.0.465 als sicher bewertet. Alle älteren Versionen wiesen über den Testzeitraum Sicherheitslücken und potenzielle Angreifbarkeit auf (Siehe auch CERT-Bund CB-K07/0058, US-CERT VU#395473, VU#298651).

3.2.4 Media-Player

Der Windows Media-Player in seiner Version 11 wurde als ausreichend sicher bewertet. Über den gesamten Testzeitraum hinweg wurden alle Versionen, die geringer als Version 11 ausfielen als Sicherheitskritisch eingestuft (siehe auch CERT-Bund CB-K08/0068, CB-K08/0508).

3.2.5 Java

Die Version 1.6.0_07 von SUN Java wurde über den gesamten Testzeitraum hinweg als sicher bewertet. Siehe hierzu auch CERT-Bund CB-K08/0030, CB-K08/0015, CB-K07/0776 sowie National Vulnerability Database CVE-2008-3440.

3.2.6 Acrobat PDF

Die Version 9.0 des Adobe Readers (ehemals Acrobat Readers) wurde über den Testzeitraum hinweg als aktuell und sicher bewertet. Ältere Versionen, hierbei insbesondere 7.0 und ältere Stände boten mehrere Möglichkeiten zur Remote-Codeausführung und damit

Deutsches Sicherheitsnetz e. V.
Schauenburgerstraße 116
D-24118 Kiel

Telefon: 0431 530237-50
info@deutsches-sicherheitsnetz.de
Fax: 0431 530237-59

Kieler Volksbank eG
Kontonummer: 513 80 70 6
BLZ: 210 900 07

zur direkten Infektion eines PCs durch PDF-Dokumente. Siehe hierzu auch CVE-2008-2641 und US-Cert VU#788019 sowie CERT-Bund CB-K08/0074, CB-K07/0882-1, CB-K07/0261, CB-K07/0024.

Achtung: die Möglichkeiten zur exakten Ermittlung des Versionsstandes des PDF-Plugins ist beim Internet-Explorer leicht eingeschränkt. So konnte bei diesem Browser lediglich eine Versionsnummer „7 oder höher“ ermittelt werden, unabhängig davon ob der tatsächliche Versionsstand 7.0, 7.1 oder 7.5 ist. Um in jedem Fall dem Fehlurteil eines „False Positive“ zu entgehen wurden Browser-Systeme mit nicht eindeutiger Versionsnummer nicht als nicht mangelhaft bewertet. Die genannte Einschränkung betrifft nur den Internet-Explorer. Der Firefox Browser oder Opera wiesen diese Einschränkungen nicht auf.

3.2.7 Firefox Update

Zusätzlich zu Fehlern in den Plugins von Browsern wurden auch direkte Sicherheitslücken der Browser selbst beurteilt. Für den Fall, dass die aktuelle Version des Firefox-Browsers unter 3.0.1 bzw. zu Beginn der Testreihe unter 3.0 / 2.0.16 lag, wurde eine Angreifbarkeit bedingt durch Veralterung des Browsers vorausgesetzt (CERT-Bund CB-K08/0410, CB-K08/0409, CB-K08/0388, CB-K08/0226).

3.2.8 IE Update

Zusätzlich zu Fehlern in den Plugins von Browsern wurden auch direkte Sicherheitslücken der Browser selbst beurteilt. Für den Fall, dass die aktuelle Version des Internet-Explorers unter 7.0 (bei Windows Vista), unter 7.0 (bei Windows XP SP2/SP3) und unter 6.0 bei Windows XP und XP SP 1 lag, wurde eine Angreifbarkeit bedingt durch Veralterung des Browsers vorausgesetzt (CERT-Bund CB-K08/0339, CB-K07/1024 und National Vulnarability Database CVE-2008-3014, CVE-2008-3013, CVE-2008-3012 sowie US-Cert VU#516627).

Achtung: die Möglichkeiten zur exakten Ermittlung des Versionsstandes des Internet-Explorers war durch den im Rahmen dieses Test verwendeten Java Skript Code leider eingeschränkt. Um für die Testteilnehmer keine Instabilitäten zu verursachen, konnten im Bereich des Internet-Explorer-Testings nur die Hauptversionsnummern (5.0, 5.5, 6.0, 7.0 und 8.0) erkannt werden. Die tatsächliche Fehlerrate aufgrund von Versionsunterschieden wird also deutlich höher liegen, als in diesem Testfeld angegeben.

3.3 Eingesetzte Audit- und Testroutinen

Die Browserversionen wurden ermittelt über die Identifikation, die ein Browser bei jedem Seitenaufruf schickt (User-Agent).

Deutsches Sicherheitsnetz e. V.
Schauenburgerstraße 116
D-24118 Kiel

Telefon: 0431 530237-50
info@deutsches-sicherheitsnetz.de
Fax: 0431 530237-59

Kieler Volksbank eG
Kontonummer: 513 80 70 6
BLZ: 210 900 07

Die Plugin-Versionen wurden zumeist über Clientseitigen JavaScript- bzw. VBScript (IE)-Code ermittelt. Hierfür wurden Browserspezifische Erkennungsroutinen verwendet, die in dem Browser ausgeführt wurden. Ihr Ergebnis (die ermittelte Plugin-Version) wurde zum Test-Server geschickt, wo sie anhand der Datenbank der unsicheren Versionen bewertet wurde. Alle Einzelergebnisse wurden gesammelt und dem Testteilnehmer nach Abschluss des Gesamttests präsentiert.

Aufgrund der Vielzahl der möglichen Kombinationen von Browsern-, Betriebssystemen sowie der darauf aktiven Plugin-Kombinationen konnte nicht für jede exotische Interkombination die vollständige Korrektheit der Abfrageroutinen garantiert werden. Dies betrifft insbesondere mobile Endgeräte und Spielekonsolen sowie nicht-Windows-Systeme und Browser mit einem Verbreitungsgrad von unter 1%. Statistisch ist diese Auswirkung also unbedeutend, im Einzelfall jedoch zu diskutieren.

Plugins und Browser in bestimmten Versionen liefern bekanntermaßen fehlerhafte oder gar keine Angaben über ihre Version. So geben sich beispielsweise ältere Opera-Versionen bewusst als Internet Explorer aus, oder aber der Internet-Explorer selbst liefert in einigen Versionen für das PDF-Plugin nur die Angabe „Version 7 oder größer“ in solchen Fällen wurde im Zweifel zu Gunsten des getesteten PC Systems entschieden und die Angreifbarkeit negiert.

3.4 Datenschutz

Im Rahmen der Überprüfung wurden keine personenbezogenen Daten gesammelt oder ausgewertet. Die Durchführung der Studie erfolgte im strengen Einklang mit den einschlägigen gesetzlichen Vorgaben des Bundesdatenschutzgesetzes. Aus Dokumentationszwecken wurden bei jeder Nutzung statistische Daten gespeichert. Hierzu gehörte die Art und Zahl der Fehler auf den getesteten PCs. Diese Daten stellen keine durch das Datenschutzrecht besonders zu behandelnden Daten dar, sie dienen nur statistischen Zwecken. Eine Speicherung der IP-Adresse fand nicht statt. Der vom Deutschen Sicherheitsnetz eingesetzte Computercheck ist durch das offizielle deutsche Datenschutz Gütesiegel juristisch und technisch zertifiziert (Prüfnummer #1-01/2005 bis 2009).

3.5 Selber Testen

Wer seinen eigenen Computer kostenlos auf die in dieser Studie überprüften Sicherheitslücken kontrollieren möchte, kann dies jederzeit auf den Internetseiten des Deutschen Sicherheitsnetz (www.desine.de) machen. Klicken Sie einfach auf unser Angebot „Browsercheck“ und machen Sie gratis den Test.

Deutsches Sicherheitsnetz e. V.
Schauenburgerstraße 116
D-24118 Kiel

Telefon: 0431 530237-50
info@deutsches-sicherheitsnetz.de
Fax: 0431 530237-59

Kieler Volksbank eG
Kontonummer: 513 80 70 6
BLZ: 210 900 07

Abbildung 11 "Startseite Deutsches Sicherheitsnetz e. V."

Deutsches Sicherheitsnetz e. V.
Schauenburgerstraße 116
D-24118 Kiel

Telefon: 0431 530237-50
info@deutsches-sicherheitsnetz.de
Fax: 0431 530237-59

Kieler Volksbank eG
Kontonummer: 513 80 70 6
BLZ: 210 900 07

4 Ergebnisse

Die Ergebnisse lassen sich grob in vier Bereiche unterteilen. Zunächst sind hier Plugin- und klassische Browserfehler zu nennen. Also Angriffsmöglichkeiten die auf Fehler innerhalb der Multimedia-Komponenten zurückgehen und solche, die sich gegen den Browser selber richten. Bei den letztgenannten klassischen Browser-Sicherheitslücken hat sich die Studie auf die beiden Hauptakteure Internet-Explorer und Mozilla-Firefox beschränkt. Der Abschnitt Einzeluntersuchungen widmet sich der Fragestellung welcher Browser oder welches Betriebssystem am wenigsten anfällig ist. Den Abschluss bilden die Analyseergebnisse für Nicht-Windows-Systeme beziehungsweise von exotischen Konfigurationen, wie sie auf Mobiltelefonen oder Spielkonsolen vorzufinden sind.

4.1 Plugin- und Browserfehler

Plugin	Fehler	Anteil
Java	21.119	24,77%
Flash	17.279	20,27%
Shock-wave	12.081	14,17%
Quicktime	10.272	12,05%
Media Player	9.132	10,71%
AdobePDF	8.640	10,13%
IE Fehler	4.588	5,38%
FF Fehler	2.150	2,52%
Summe der Fehler	85.261	100,00%

Besucher der Seite	77.394	
Durchgeführte Audits	67.870	
Fehlerhafte PCs	43.317	**63,82%**

Abbildung 12 "Plugin-Fehler tabellarisch“

Untersucht wurden die Versionsstände der Plugins für alle gängigen Browsersysteme. Im Einzelnen waren dies: Adobe Reader (ehemals Acrobat Reader), Apple Quicktime, Adobe Flash bzw. Shockwave, Sun Java VM, Microsoft Media Player. Bei insgesamt 67.870 untersuchten PCs wurden 78.523 angreifbare Plugins auf 43.317 bemängelten PCs gefunden. Zieht man 6.738 reine Browserfehler in diese Betrachtung mit ein, so ergibt sich eine Quote von circa zwei Fehlern pro PC. Mit jeweils über zwanzig Prozent relativem Anteil waren Java (24,77 %) und Flash (20,27 %) die häufigsten Fehlerquellen. Mit einigem Abstand folgten die Plugins von Shockwave (14,17 %) und die des Microsoft Media Players (10,71 %). In diesem Test belegte Adobe PDF mit etwas über zehn Prozent aller getesteten Systeme zwar den rühmlichen letzten Platz, allerdings ist dieser Umstand wohl eher der nur eingeschränkten Möglichkeit zur Detektion auf IE-Systemen, als der tatsächlich geringen Fehlerzahl dieses Plugins zu verdanken.

Bei den direkten Browser Fehlern hat sich diese Studie auf die beiden am weitesten verbreiteten Systeme beschränkt. Untersucht wurden lediglich Schwachstellen und Sicherheitslücken des Internet-Explorers und von Mozilla-Firefox. Mit 4.588 (IE) bzw. 2.150 (FF) liefern die beiden in Summe lediglich 7,9 % der insgesamt detektierten Angriffsmöglichkeiten. An dieser Stelle wird deutlich wie hoch das Potenzial von Angriffsmöglichkeiten ge-

Deutsches Sicherheitsnetz e. V.
Schauenburgerstraße 116
D-24118 Kiel

Telefon: 0431 530237-50
info@deutsches-sicherheitsnetz.de
Fax: 0431 530237-59

Kieler Volksbank eG
Kontonummer: 513 80 70 6
BLZ: 210 900 07

gen Browser-Plugins im Vergleich zu klassischen Angriffen gegen den Browser selbst ist. Die automatischen Updatemechanismen der Browser tragen sicherlich zu diesem guten Ergebnis bei.

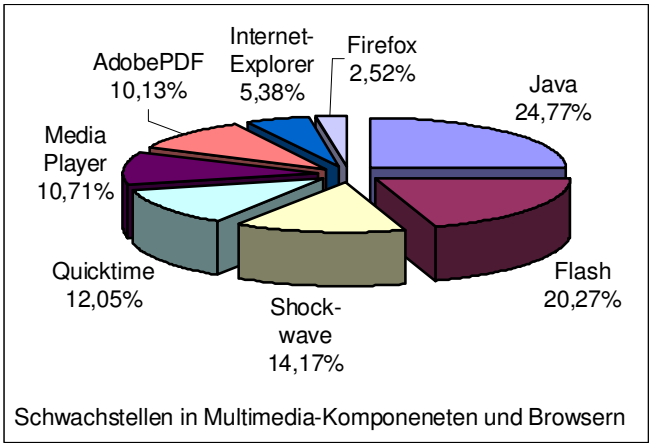


Abbildung 13 "Plugin-Fehler grafisch“

Das Fazit der Untersuchung ist, dass deutlich mehr als 60 % aller untersuchten PCs über den Browser oder Multimedia-Komponenten innerhalb des Browsers direkt angreifbar sind. Berücksichtigt man an dieser Stelle die Tatsache, dass nach Abschluss eines Browserchecks jedem Testteilnehmer die Möglichkeit zum Reparieren der gefundenen Sicherheitslücken geboten wurde, so sollte man davon ausgehen, dass ein großer Teil der mangelhaften getesteten Teilnehmer dieses Angebot auch wahrgenommen hat. Nach der Reparatur ist es nur menschlich einen zweiten Test zu starten, um zu kontrollieren, ob die Reparatur erfolgreich war. Unterstellt man bei zumindest jedem vierten Teilnehmer ein solches Vorgehen, so erscheint es wahrscheinlich, dass der tatsächliche Prozentsatz an angreifbaren PC-Systemen eher bei 75 oder 80% Prozent aller PCs im Internet liegt. Ein weiterer Hinweis, der diese These stützt ist der Umstand, dass das Testfeld aus einer größeren Zahl technologieaffiner Nutzer bestand, als dies auf normalen Internetseiten der Fall ist. Wenn jedoch bereits die Technik-Freaks derart große Probleme mit angreifbaren Media-Komponenten haben, spricht einiges dafür, dass die Verbreitung solcher Sicherheitslücken beim Durchschnitts-Surfer noch höher liegt.

4.2 Einzeluntersuchungen

Die folgenden Untersuchungsergebnisse stellen die Fehlerverteilungen aufgeschlüsselt nach den jeweils eingesetzten Browsern und Betriebssystemen gegenüber. Zielsetzung ist es zu erfahren, ob und inwieweit es einen Sicherheitsunterschied bei der Verwendung eines bestimmten Betriebssystems oder eines bestimmten Browsers, bezüglich der Angreifbarkeit der Multimedia-Komponenten gibt.

4.2.1 Browservergleich

Aus der Tabelle erkennt man deutlich, dass ältere Browsersysteme anfälliger sind als neuere. Spitzenreiter mit einem Wert von über 80 % ist der inzwischen deutlich in die Jahre gekommene Netscape-Browser. Dicht gefolgt vom AOL-Browser, der sich in über 70 % aller Fälle als angreifbar erwies.

Deutsches Sicherheitsnetz e. V.
Schauenburgerstraße 116
D-24118 Kiel

Telefon: 0431 530237-50
info@deutsches-sicherheitsnetz.de
Fax: 0431 530237-59

Kieler Volksbank eG
Kontonummer: 513 80 70 6
BLZ: 210 900 07

Browser	Fehleranteil
Netscape	80,26%
AOL	71,88%
Safari	63,49%
Mozilla	58,33%
Opera	53,25%
Internet Explorer	53,03%
Firefox	53,03%
Konqueror	46,97%
Google Chrome	35,09%

Abbildung 14 "Fehlerverteilung bei Browsern“

Der Safari Browser liegt mit circa 63 % Fehlern genau im Durchschnitt des gesamten Testfeldes. Mit Fehleranteilen zwischen 53 % und 58 % liegen die drei derzeit verbreitetesten Browsersysteme Internet-Explorer, Firefox und Opera deutlich unter dem Durchschnitt von 63,8 % und können somit als sicherer als der Durchschnitt gelten. Ebenfalls auf der sicheren Seite liegt der auf Unix Systemen sehr verbreitete Browser Konqueror sowie der neue Google Chrome Browser. Gerade bei Chrome sollte man jedoch berücksichtigen, dass dieses Browser System kaum veraltete Plugins aufweisen kann, weil der Browser erst seit wenigen Wochen am Markt ist. Die Zahl der Altinstallationen ist somit gewissermaßen prinzipbedingt gleich Null.

4.2.2 Betriebssystemvergleich

Betriebssystem	Fehleranteil
Windows NT	95,45%
Windows 98	86,77%
Windows 2000	83,05%
Windows Me	77,88%
Windows XP SP1	70,42%
Windows 95	66,67%
Windows 2003	65,88%
Linux	64,05%
Windows XP SP2/3	62,49%
MacOS X	60,65%
Windows Vista	49,13%
Symbian OS	7,69%

Abbildung 15 "Fehlerverteilung bei Betriebssystemen“

Bei den Betriebssystemen ist die Situation ähnlich. Auch hier sind alte Systeme deutlich stärker angreifbar als Neuere. Mit einer Fehlerrate von über 90 % wird das Feld von dem inzwischen mehr als betagten Betriebssystemen Windows NT angeführt, dicht gefolgt von Windows 98 und Windows 2000 mit Fehleranteilen von über 80 %. Erst ab Windows XP werden die Fehlerraten deutlich besser, liegen aber erst auch bei der Verwendung von Service Pack 2 und 3 unter dem Durchschnitt. Erst mit Windows Vista gelingt es die Fehlerrate auf unter fünfzig Prozent zu drücken. An dieser Stelle sei noch kurz auf die Exoten im Testfeld hingewiesen: die Angreifbarkeit der Linux Systeme ist natürlich nur theoretisch gegeben. Zwar lassen sich die verwendeten Plugins auch im Konqueror-Browser ausnutzen, allerdings ist der Schadcode, der ursprünglich für Windowssysteme programmiert wurde hier natürlich nicht wirksam. Gleiches gilt auch für das Macintosh Betriebssystem Mac OS X. Die Angreifbarkeit würde in beiden Fällen voraussetzen, dass man Schadcodes speziell für diese Betriebssysteme entwickelt, was aufgrund der ähnlich hohen Zahl von Schwachstellen innerhalb des Browsers problemlos möglich wäre, aufgrund der extrem schwachen Verbreitung dieser Betriebssysteme bisher jedoch durch Internet Kriminelle in nicht messbarer Anzahl gemacht worden ist. Eine ech-

Deutsches Sicherheitsnetz e. V.
Schauenburgerstraße 116
D-24118 Kiel

Telefon: 0431 530237-50
info@deutsches-sicherheitsnetz.de
Fax: 0431 530237-59

Kieler Volksbank eG
Kontonummer: 513 80 70 6
BLZ: 210 900 07

te Sonderrolle nimmt Symbian OS ein. Dabei handelt es sich um ein typisches Betriebssystem das auf Mobiltelefonen und Kleincomputern verwendet wird. Es lag bisher nicht im Fokus dieser Untersuchung die Sicherheit von mobilen Endgeräten zu kontrollieren, allerdings haben diese mit ihren immer stärker werdenden Fähigkeiten im Internet zu surfen die gleichen Schwachstellen und Angriffspunkte ihrer großen PC-Brüder geerbt. Dazu noch einige Anmerkungen im folgenden Abschnitt.

4.3 Mobiltelefone und Spielkonsolen

Browser	Anteil
Internet Explorer	45,767%
Firefox	44,431%
Opera	3,448%
AOL	0,849%
Mozilla	1,043%
Google Chrome	1,344%
Safari	0,371%
Netscape	0,112%
Konqueror	0,097%
Seamonkey	0,057%
Rippers	0,055%
Iceweasel	0,041%
iPhone	0,032%
Inktomi	0,019%
Nokia Handy	0,007%
SonyEricsson Handy	0,003%
Sony Playstation 3	0,003%
Motorola Handy	0,001%
Wii Web Browser	0,001%
Sonstige	2,318%

Abbildung 16 "Exoten“

Die nebenstehende Tabelle zeigt den kompletten Überblick der im Rahmen dieser Studie getesteten Browser. Im Unterschied zu den vorangegangenen Daten sind hier auch Browser mit Verbreitungs-Anteilen von unter 0,1 % enthalten. Aus diesen Daten wird ersichtlich, dass neben dem Testen von PCs in privaten Haushalten auch einige Teilnehmer ihre privaten Handys und Spielkonsolen mit dem Browsercheck getestet haben. Diese technische Möglichkeit dessen war nicht so vorgesehen, erscheint aber im Nachhinein verständlich, da viele der modernen mobilen Kleingeräte inzwischen über voll funktionelle Browser und Internet Zugänge verfügen. Insgesamt wurden 46 mobile Endgeräte über den Testzeitraum hin getestet. In den Fällen, in denen die Browser Konfiguration und die eingesetzten Plugins denen von PC Systemen glichen, konnte auch die prinzipielle Angreifbarkeit von mobilen Endgeräten ermittelt werden. In 14 Fällen konnte die Aussage getroffen werden, dass, geeigneten Schadcode vorausgesetzt, über Multimedia-Komponenten auch Mobiltelefone und Spielkonsolen angreifbar sind. Dieser Umstand lässt für die nähere Zukunft eine neue Dimension von Sicherheitsrisiken für private Haushalte ahnen, die sowohl das private Wohnzimmer (Spielkonsole) als auch die direkte private Umgebung (Handy) betreffen. Das Deutsche Sicherheitsnetz wird prüfen, inwieweit mit neuem Testapplikationen zukünftig auch dieser sehr spezielle Kreis von Endgeräten überprüft werden kann.

Deutsches Sicherheitsnetz e. V.
Schauenburgerstraße 116
D-24118 Kiel

Telefon: 0431 530237-50
info@deutsches-sicherheitsnetz.de
Fax: 0431 530237-59

Kieler Volksbank eG
Kontonummer: 513 80 70 6
BLZ: 210 900 07

5 Ausblick

5.1 Kostenloses Hilfsangebot für jedermann

Computerviren und Datenspione werden immer dreister. Der Schutz des Computers wird immer komplizierter und ist ohne Hilfe kaum noch zu bewältigen. Für alle technischen Laien hat das Deutsche Sicherheitsnetz deshalb eine Reihe von Sicherheitslösungen zusammengestellt, die besonders schnell und einfach helfen. Ein wichtiges Augenmerk war hierbei die Anforderung, dass bei Sicherheitspannen am PC auch ein kompetenter Ansprechpartner aus dem technischen Kundendienst zur Verfügung steht. So bietet das Deutsche Sicherheitsnetz inzwischen einen PC-Pannendienst für jedermann, der sowohl Professionelle Schutzsoftware und eine kostenlose Telefon-Hotline als auch die Reparatur von infizierten PCs durch einen Techniker umfasst. Die verschiedenen Sicherheits-Angebote entnehmen Sie bitte unserer Internetseite:

www.desine.de

Deutsches Sicherheitsnetz e. V.
Schauenburgerstraße 116
D-24118 Kiel

Telefon: 0431 530237-50
info@deutsches-sicherheitsnetz.de
Fax: 0431 530237-59

Kieler Volksbank eG
Kontonummer: 513 80 70 6
BLZ: 210 900 07

6 Der Verein

Das Deutsche Sicherheitsnetz e. V. (Desine, www.desine.de) hat sich zum Ziel gesetzt, die Internet-Sicherheit bei der privaten Computernutzung in Deutschland zu erhöhen. Hierzu bietet der Verein in Kooperation mit Banken, Sparkassen und Versicherungen einen PC-Pannendienst für jedermann an. Wer mitmacht, erhält nicht nur Zugang zur neuesten Sicherheitssoftware, sondern bei einem PC-Sicherheitsproblem auch konkrete technische Hilfestellung „ohne wenn und aber“.

Deutsches Sicherheitsnetz e. V.
Schauenburgerstraße 116
24118 Kiel
Tel. 0431 530 237-50
E-Mail: info@deutsches-sicherheitsnetz.de
Web: www.deutsches-sicherheitsnetz.de

Deutsches Sicherheitsnetz e. V.
Schauenburgerstraße 116
D-24118 Kiel

Telefon: 0431 530237-50
info@deutsches-sicherheitsnetz.de
Fax: 0431 530237-59

Kieler Volksbank eG
Kontonummer: 513 80 70 6
BLZ: 210 900 07