Deutsches Sicherheitsnetz

Studie zur PC-Sicherheit 2008

veröffentlicht am 4. Juni 2008

Zusammenfassung

Das Deutsche Sicherheitsnetz e.V. hat in den vergangenen fünf Monaten über 225.000 PCs in privaten Haushalten auf Sicherheitslücken und Angreifbarkeit aus dem Internet untersucht. Gestützt auf eine Analyse der Coronic GmbH wurden in über zehn Prozent der Computer Schwachstellen sowie direkt angreifbare Sicherheitslücken entdeckt. Die Zahl der gefundenen Fehler lag bei Windows XP mit 12% deutlich über der Fehlerrate von Windows Vista mit nur 5,5%. Ältere Betriebssysteme wie Windows 98 / Me / 2000 wiesen Fehlerquoten von über 20% auf, die teilweise direkt für einen Angriff missbraucht werden könnten. Von allen gefundenen Fehlern wurden circa 20% als schwerwiegend eingestuft (Trojaner, Schadsoftware, freie Dienste), weitere 25% gehen auf direkte Sicherheitslücken im Betriebssystem oder im Browser zurück und circa 55% aller Fehler verteilen sich auf mittelschwere Fehler und potentiell angreifbare Dienste auf dem PC, die durch offene Ports bedingt sind.

Fehlerklasse	#	%
Schwere Fehler	4.539	18,1%
Direkte Sicherheitslücken	6.381	25,4%
Mittelschwere Fehler	3.542	14,1%
Potenziell angreifbar	10.659	42,4%
Summe	25.121	100,0%

Untersucht wurden 225.213 privat genutzte PCs von denen 25.121 (11,2%) Fehler und potenzielle Sicherheitslücken aufwiesen.

Motivation

Im letzten Jahr hat die Zahl der Personalcomputer in Deutschland mit 46 Millionen registrierten Geräten erstmals die Zahl der zugelassenen Pkw überstiegen. Das Internet ist vom Tummelplatz für Computerfreaks und Wissenschaftler zum Online-Medium für alle Deutschen geworden. Eine Bestellung bei Amazon, eine Überweisung im Online-Banking und das Ummelden der Wohnung via Internet sind heute genauso einfach wie Autofahren. Leider hat der große Erfolg der Online-Geschäftsprozesse auch seine Schattenseiten: Mit jedem umgesetzten Euro und mit jedem online bestellten Artikel wird der private PC mehr und mehr zum Lieblingsziel von Computerkriminellen und Trickbetrügern.

Fragt man die Hersteller von Sicherheitssoftware, so gibt es natürlich für jeden Computerschädling ein geeignetes Sicherheitspaket, für jeden Virus einen Antivirus und für jede Sicherheitslücke den passenden Sicherheitsflicken. Trotzdem nimmt die Zahl der Datendiebe und der ausspionierten PCs weiter zu.

© 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

Vor diesem Hintergrund schätzen immer mehr Internetnutzer ihre persönliche Sicherheit im Internet als sehr schlecht ein. Laut Emnid halten heute schon über 50% der Internetnutzer das Netz für unsicher. Die Ursache hierfür sind zumeist keine direkten grundsätzlichen Sicherheitsbedenken gegenüber den Anbietern von Shops und Angeboten im Internet, sondern eher ein persönliches Unbehagen, das man seinem eigenen PC entgegenbringt. Ziel der Studie war es herauszufinden, ob diese mangelnde "Gefühlte Sicherheit" am eigenen PC tatsächlich durch technische Probleme am privaten PC begründet ist.

Das Deutsche Sicherheitsnetz hat daher über 225.000 privat genutzte Internet-PCs auf ihre Sicherheitseinstellungen und ihre Angreifbarkeit über das Internet überprüft.

Technik

Die einzelnen PCs wurden dazu direkt über das Internet einer Reihe von verschiedenen Einzeltests, den so genannten Prüfpunkten, unterzogen. Jeder dieser Prüfpunkte gab Aufschluss über einen speziellen Sicherheitsaspekt des getesteten PCs. Es wurden ausgewählte, technisch direkt oder indirekt nachweisbare Sicherheitsprobleme von Windows PCs und Internet-Browsern überprüft. Die Prüfung eines einzelnen PCs dauerte je nach Netzwerkverbindung zwischen 40 und 90 Sekunden.

Die Prüfpunkte unterteilten sich technisch in verschiedene Bereiche. Ein vor

geschalteter TCP-Porttest erkannte, welche Kommunikationstore (Ports) in den getesteten PCs oder den vorgeschalteten DSL-Routern offen waren. In einem zweiten Schritt wurden aktive Dienste hinter diesen Ports gesucht. Mit einer kontaktlosen Netzwerkanforderung (Null Session) wurde versucht, eine Verbindung zu den Diensten herzustellen, um so ihre Verfügbarkeit und Angreifbarkeit zu ermitteln. Parallel dazu wurden die Version des eingesetzten Browsers, sein Aktualisierungsstand und die Sicherheitseinstellungen abge-

© 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

fragt.

Alle Testergebnisse wurden online durch einen Live-Computercheck gewonnen, den der Internetnutzer direkt mit seinem Browser starten kann. Die Benutzung des Computerchecks steht jedem interessierten Nutzer auf den Seiten des Deutschen Sicherheitsnetz e. V. frei. Die Benutzung des Computerchecks ist an keinerlei technische Voraussetzungen gekoppelt, es muss zur Teilnahme keine Software installiert oder konfiguriert werden, ein einfacher Mausklick auf den Startknopf reicht aus.

Hilfe für fehlerhafte PCs

Allen Internet-Nutzern, an deren PCs Sicherheitsmängel oder konkrete Schwachstellen auftraten, wurde der Fehler ausführlich beschrieben. Für jeden Teilnehmer bestand danach die Möglichkeit anhand einer einfachen und verständlichen Schritt-für-Schritt-Anleitung die erkannte Schwachstelle wieder zu reparieren.

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).

Ergebnisse

Insgesamt wurden in den vergangenen fünf Monaten von Januar 2008 bis Mai 2008 genau 225.213 PCs von privaten Internet-Nutzern auf ihre Sicherheitseinstellungen und Schwachstellen überprüft.

Als wesentliches Ergebnis wurde festgestellt, dass über zehn Prozent aller getesteten Windows PCs teilweise gravierende Sicherheitslücken aufgewiesen

© 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

haben.

Einige dieser Sicherheitslücken waren schwerwiegend und mussten mit einer roten Ampel (Schadsoftware, angreifbare Dienste, veraltete Software mit Sicherheitslücken) bewertet werden. Der größte Teil der Sicherheitslücken wurde mit einer gelben Ampel bewertet. Es handelt sich hierbei meist um potentielle Lücken aufgrund von Browserfehlern oder offenen Ports, die jedoch mit genügend kriminelle Energie auch für einen Angriff missbraucht werden könnten.

Die folgende Tabelle zeigt eine Übersicht der verschiedenen Betriebssysteme, die auf den getesteten PCs zum Einsatz kamen. Die einzelnen Spalten zeigen die Häufigkeit des jeweiligen Betriebssystems in absoluter und prozentualer Anzahl sowie die Fehlerhäufigkeit in absoluter und prozentualer Anzahl.

Prüfergebnis: Fehlerzahl nach Betriebssysteme				
Betriebssysteme	***Fehlerzahl***		***Testzahl***	
Windows 98/Me	2.214	23,07%	9.598	4,26%
Windows 2000	2.240	24,90%	8.997	3,99%
Windows XP	8.249	13,62%	60.577	26,90%
Windows XP SP2	9.123	10,67%	85.464	37,95%
Windows Vista	3.295	5,44%	60.577	26,90%
Summe	25.121	11,15%	225.213	100,00%

Zunächst fällt auf, dass die Fehlerzahl direkt mit der Aktualität des betreffenden Betriebssystems verbunden ist. Neuere Betriebssysteme weisen in der tatsächlichen Bedrohungslage weniger Lücken und Anfälligkeiten auf als Ältere. Nicht berücksichtigt in dieser Darstellung ist der Effekt, dass die Angreifer natürlich immer nur das Betriebssystem attackieren, das die größte Markt-Dominanz aufweist. Besonders neue oder eher exotische Betriebssysteme und Softwareversionen stehen meistens nicht im Fokus der Angreifer. Diese Systeme sind also nicht per se sicherer, sondern werden nur weniger stark attackiert.

Eingesetze Browser	
Browser	***%***
Internet-Explorer	61,93%
Firefox	29,78%
AOL	3,55%
Opera	2,18%
Safari	0,62%
Mozilla	0,54%
Mozilla/4.0	0,46%
Netscape	0,41%
SeaMonkey	0,16%
Konqueror	0,12%
Andere	0,24%

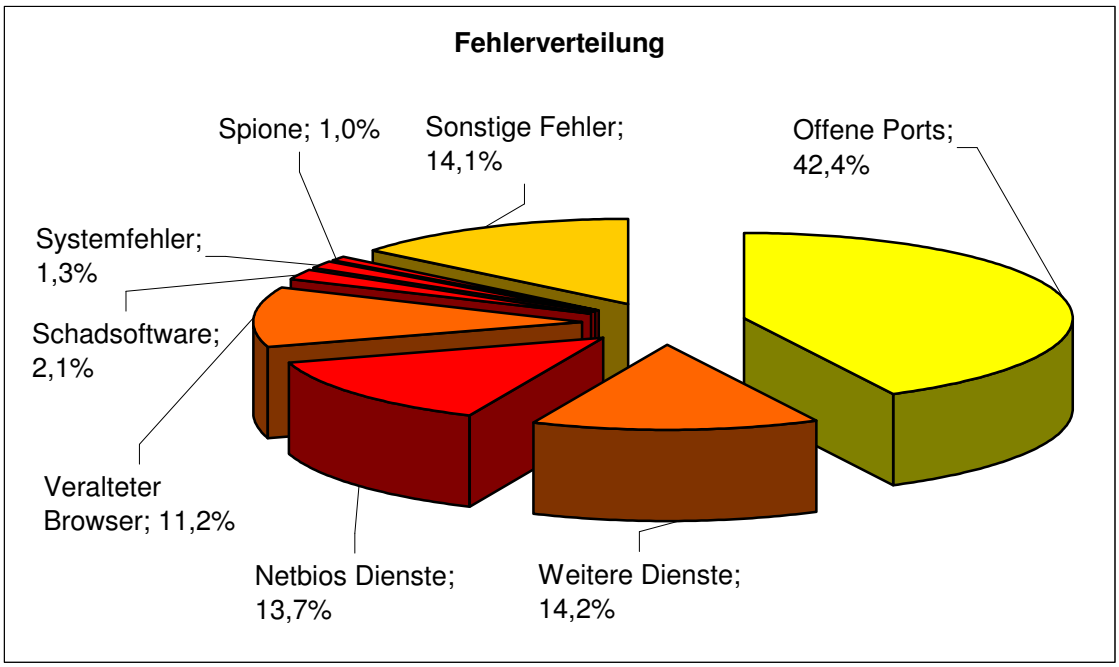
Gerade in puncto Angreifbarkeit kommt den eingesetzten Internet-Browsern eine enorme Bedeutung zu. Der Browser, als wesentliches

© 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

Mittel der Internet-Kommunikation stellt von jeher ein ideales Ziel für Angreifer dar. Auch bei den Internet-Browsern gilt das Gleiche wie bei den Betriebssystemen - der jeweils am stärksten verbreitete Browser wird auch am stärksten angegriffen. In dem hier durchgeführten Test haben circa 60% der Internet-Nutzer den Internet-Explorer der Firma Microsoft als Browser eingesetzt. Mit 29% Prozent lag der Firefox-Browser auf Platz zwei. Alle anderen Browser sind mit deutlich unter 5% in Deutschland nur Randphänomene. An dieser Stelle sei bereits darauf hingewiesen, dass sich das Deutsche Sicherheitsnetz in seiner nächsten Studien der Angreifbarkeit von Internet-Browsern gesondert widmen wird. Interessierte Testteilnehmer finden am Ende dieses Berichts eine kleine Vorschau auf die kommenden Prüfszenarien.



Bei den gefundenen Fehlern handelt es sich um Sicherheitslücken und Konfigurationsfehler verschiedener Art.

Den größten Teil aller gefundenen Sicherheitslücken machen offene Ports in den getesteten Betriebssystemen aus. Ports sind gewissermaßen die Kommunikationstore der Computer. Steht eines offen, ist es wie eine unverschlossene Tür, durch die Angreifer eindringen könnten.

Einen zweiten großen Bereich, der den privaten PC verwundbar macht, machen aktive Dienste aus. Ein Computerdienst stellt einem anderen Gerät (z.B. einem

© 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

Computer, Drucker, …) gewisse Funktionen auf dem heimischen PC zur Verfügung. Ist ein solcher Dienst nicht hinreichend abgesichert, so kann er als Einfallstor für Angreifer oder Viren dienen. Die größte Dienst-Schwachstelle auf den getesteten PCs war der so genannte Netbios-Dienst, gefolgt von weiteren Windows Diensten, die über den Port 445 kommunizieren.

Der dritte Fehlerbereich geht auf veraltete Browser, fehlende Updates in Betriebssystemen und Systemlücken innerhalb der PCs zurück. Besonders hervorzuheben ist hierbei, dass immer noch über ein Prozent der getesteten Computer direkt über relativ alte Systemfehler wie RCP-, ASN- oder PnP-Lücken potenziell angreifbar wäre. In circa einem Prozent der Fälle hat sich ein Verdacht auf Kommunikation von Schädlingsprogrammen ergeben.

Jetzt 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.deutsches-sicherheitsnetz.de) machen. Klicken Sie einfach auf unser Angebot „Computercheck“ und machen Sie gratis den Test.

Ausblick

Die Analyse der Verbreitungswege aktueller Trojaner und Schädlingsprogramme hat gerade in den letzten Wochen gezeigt, dass der Internet-Browser mehr und mehr zum primären Angriffsziel der Internet-Kriminellen geworden ist.

Die Verbreitung von Schad-Programmen über die verschiedenen Internet-Browser geschieht über zwei unterschiedliche Wege. Der einfachste Weg ist die Verteilung von Schädlingen über manipulierte Internetseiten, die die Kriminellen selber betreiben. Der zweite Weg ist komplizierter, aber auch effizienter. In diesem Fall versuchen die Angreifer Internetseiten seriöser Firmen zu übernehmen. Ist dies geschehen, werden die vormals harmlosen Internetseiten scheinbar seriöser Firmen durch die Angreifer manipuliert. Diese manipulierten Internetseiten versuchen dann allen späteren Besuchern ein Schad-Programm unterzujubeln.

Vor diesem Hintergrund sind die Aktualität des Browsers und der Schutz der einzelnen Browser-Komponenten von grundlegender Bedeutung für die Sicher-

© 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

heit der kommenden Monate und Jahre.

Das Deutsche Sicherheitsnetz e.V. wird daher in den kommenden Wochen einen groß angelegten Browsercheck durchführen, dessen Ziel es ist, die unterschiedlichen Schwachstellen und Angriffspunkte innerhalb des Browsers und seiner Unterprogramme zu identifizieren.

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 Sicherheits-Pannen am PC auch ein kompetenter Ansprechpartner aus dem technischen Kundendienst zur Verfügung steht. Die verschiedenen Sicherheits-Angebote entnehmen Sie bitte unserer Internetseite:

www.deutsches-sicherheitsnetz.de

Deutsche Sicherheitsnetz e.V.

Das deutsches Sicherheitsnetz e.V. (www.deutsches-sicherheitsnetz.de) hat sich zum Ziel gesetzt, die Sicherheit der Internet-Computernutzung in Deutschland zu erhöhen. Der Verein bietet in Kooperation mit verschiedenen Volksbanken Raiffeisenbanken sowie Sparkassen einen PC-Sicherheitsdienst für jedermann an. Vereinsziel ist der weitere Ausbau des Sicherheitsniveaus, um die Internet-Nutzung und den privaten PC von Gefahren zu befreien.

Weitere Informationen:

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