DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 89194 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

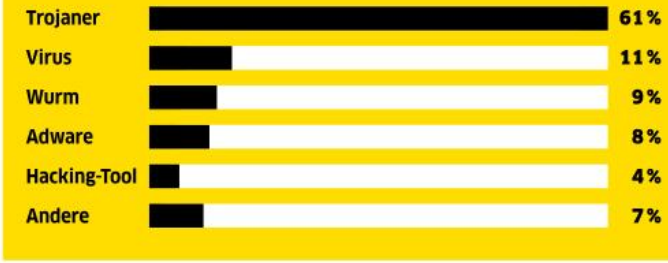
NSA rät zum Upgrade auf Windows 7

Der US-Geheimdienst NSA rät in einer offiziellen Stellungnahme zum Wechsel auf Windows 7. Laut Ratgeber ist das aktuelle Microsoft-System durch Sicherheitsfeatures wie die Benutzerkontensteuerung besser gegen Angreifer geschützt. Außerdem sollte die automatische Update-Funktion aktiviert werden. Als Textverarbeitung sollte Office 2010 zum Einsatz kommen, denn die XML-Dateiformate würden eine Manipulation der Files schwierig machen.

INFO: nsa.gov

DIE TOP-VIREN-GEFAHREN

Trojaner machen laut Panda Security mehr als die Hälfte aller Malware-Infektionen weltweit aus



NEUE SICHERHEITSRISIKEN

ADOBE READER UND ACROBAT

Über eingebettete Flash-Inhalte in PDFs können Angreifer Schadcode auf den PC spielen. Die Hacker nutzen manipulierte Webseiten oder in PDF eingebettete Word- und Excel-Dokumente für den Angriff.

LÖSUNG | Da die Attacken bereits „in the wild" stattfinden, also bereits im Internet auftauchen, hat Adobe ein außerplanmäßiges Update für den Adobe Reader und Adobe Acrobat herausgebracht.
Info: adobe.de

MICROSOFT POWERPOINT

Am vergangenen Patchday wollte Microsoft mit einem Update für PowerPoint eigentlich mehrere Lücken schließen. Doch das Update brachte die Anwendung vereinzelt zum Absturz – ob sich dadurch Schadcode aufspielen lässt, ist bislang unklar.

LÖSUNG | Microsoft bietet einen Hotfix an, der nicht nur die Abstürze behebt, sondern auch die Schwachstelle schließt.
Info: microsoft.de

APPLE ITUNES

Hacker können über eine Man-in-the-Middle-Attacke einen Bug im WebKit der iTunes-Windows-Version ausnutzen, um Schadcode auf den Computer aufzuspielen.

LÖSUNG | Apple hat den Fehler mit der Version 10.2.2 behoben – in der Ausgabe für Mac ist die Schwachstelle nicht vorhanden.
Info: apple.de

Quelle CHIP 7/2011

Vertrauen Sie den Websites, die Sie regelmäßig besuchen? Malware-Entwickler hoffen darauf, denn zeigt der Browser auf einer bekannten Seite eine Warnung an, glaubt kaum ein User an einen Virus – und ignoriert die Warnung. Dass dieses Vertrauen gefährlich ist, zeigen Angriffe auf renommierte Seiten, wie zuletzt im April. Rund 500.000 Websites wurden Opfer einer Attacke, die gefährlichen Schadcode in die Seiten einschleuste – darunter auch einige Podcasts auf iTunes.

Auch in anderen Fällen setzen die Malware-Entwickler gezielt auf die Arglosigkeit der User. Neben dem Dauerbrenner Phishing-Mail konzentrieren sich Angreifer zurzeit besonders auf zwei Wachstumsmärkte: soziale Netzwerke und Smartphone-Apps. Noch immer glauben nur wenige User, dass Postings ihrer Facebook-Freunde gefährlich sein können. Doch täglich tauchen neue Attacken auf, die es auf die persönlichen Daten der User abgesehen haben. Und auch die Zahl der Apps im App-Store und besonders im Android Market, die Handydaten ausspähen oder User abzocken, nimmt rasant zu.

Andererseits konfrontieren Browser und Betriebssystem den User immer wieder mit eigentlich harmlosen Warnungen, hinter denen mancher einen Virenbefall vermutet: Geblockte Websites, Fehlalarme des Virenscanners, Windows-Meldungen. Die Unterscheidung, wo tatsächlich ein Virus lauert und wo nicht, ist schwierig. Wer an den richtigen Stellen und mit den passenden Tools sucht, findet die Lösung aber schnell.

Echter Virus: So tarnen sich Malware und Abzocker

GEHACKTE WEBSITES Angreifer nutzen vermehrt seriöse Seiten, um Malware zu verbreiten. Jüngstes Beispiel: Der erwähnte Angriff auf rund eine halbe Million Websites, der als LizaMoon-Attacke bekannt wurde. Per SQL Mass Injection haben Hacker Code in die Seiten eingefügt, der automatisch zu einer Seite weiterleitete, die die Malware gehostet hat. Die meisten dieser Weiterleitungen führten zur Domain lizamoon.com – daher der Name. Eine ähnliche Attacke er-

wischte im Juni letzten Jahres etwa 114.000 Seiten. Genau wie damals visierte der LizaMoon-Angriff Seiten an, welche die Microsoft-Server-Plattform IIS und die Content-Entwicklungstechnologie ASP.net nutzten. Die Malware-Fakete auf den Zielseiten der Redirects suchen dabei gezielt nach ungepatchten Lücken im Browser, den Plug-ins oder in Windows selbst. Oft sind das Trojaner, die Daten ausspionieren oder Rogueware-Programme (siehe unten).

► Selbst wenn der Browser oder der Virenscanner eine Warnung anzeigt, rechnen User auf bekannten Seiten selten mit einem Angriff. Man würde ihn auch kaum bemerken, da er meist im Hintergrund ausgeführt wird. Daher sollten Sie immer den Virenscanner, den Browser und dessen Plug-ins aktualisieren, um Sicherheitslücken so gut wie möglich zu stopfen. Mit dem Firefox-Add-on NoScript regeln Sie zudem die Ausführung aktiver Elemente und blockieren eingebettete Skripte. Manchmal ist aber nicht die Seite selbst das Problem, sondern per iFrame auf der Seite eingefügte Inhalte. Gehen Sie daher nach der Installation von NoScript über das Icon neben der URL-Zeile zu »Einstellungen | Eingebettete Objekte« und aktivieren Sie dort die Funktion »<IFRAME> verbieten«.

Hacker hebeln neuen Browserschutz aus

An aktuellen Sicherheitstechnologien der Browser sollten sich Hacker die Zähne ausbeißen – jetzt sind sie geknackt

Möchten Sie mehr wissen?

Ein **0-Day-Exploit** ist schädlicher Programm-Code, der eine noch nicht geschlossene Sicherheitslücke ausnutzt. Die Bezeichnung „0-Day-Exploit" bezieht sich auf die Zeitspanne, die dem Software-Hersteller bleibt, um die Schwachstelle zu beheben, bevor Dritte sie für Angriffe ausnutzen. Es sind null Tage.

PDF-Viren verstecken sich

Da die bekannten PDF-Viren von den meisten Virenwächtern mittlerweile problemlos erkannt werden, haben sich die Virenprogrammierer eine neue Tarnung für ihre Schädlinge einfallen lassen. Sie nutzen den für Bilder im PDF vorgesehenen JBIG2-Decoder. Dem speziell für Monochrom-Bilder gemachten Algorithmus ist es offenbar egal, welche Art von Daten hinter den Nullen und Einsen stecken. Er komprimiert also Bilder ebenso wie Viren-Code. Antiviren-Software rechnete bislang nicht mit der zusätzlichen Maskierung. Die Sicherheitslücke ist in aktuellen Versionen von Adobes *PDF-Reader* geschlossen.

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 89194 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Angriffsziel Java

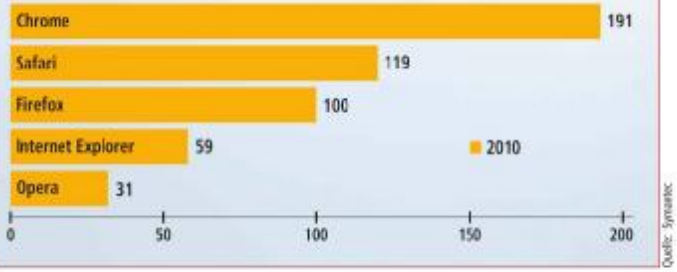
Im ersten Quartal 2011 dominierten Gdata zufolge Schädlinge die Malware-Top-10, die es auf Sicherheitslücken in Java oder Javascript abgesehen hatten. Anwender sollten deshalb Patches umgehend einspielen. Ein Check auf www.java.com/de/download/installed.jsp zeigt, ob das Java auf Ihrem PC aktuell ist.

www.gdata.de

Java: Ein Online-Check zeigt, ob die Version mit den neuesten Patches installiert ist

Chrome hat die meisten Lücken

Googles Chrome war im Jahr 2010 der Browser mit den meisten aufgedeckten Sicherheitslücken. Insgesamt entdeckten Sicherheitsexperten darin 191 Schwachstellen. In Apples Safari fielen 119 Sicherheitslücken auf, in Firefox 100.



com! Das Computer-Magazin 7/2011

com! Das Computer-Magazin 1/2010

AKTUELLE WARNUNG

Lücke im Flash-Player

Kriminelle haben über eine Sicherheitslücke im Flash-Player von Adobe unter anderem die Besucher der Website von Amnesty International infiziert.

Laut der Security-Firma Armorize schöpfte von 42 Virenscannern keiner Verdacht, da es sich um eine neue Drive-by-Cache-Attacke handelte (http://blog.armorize.com): Der Schädling wurde beim Besuch der Website zunächst als Flash-Datei im Browser-Cache abgelegt, ohne ausgeführt zu werden. So schlug die Verhaltensüberwachung nicht Alarm. Später aktivierte in den Flash-Player eingeschleuster Code ein Spionageprogramm. Den gepatchten Player 10.3.181.14 gibt es unter **http://get.adobe.com/de/flashplayer**

Schwere Flash-Lücke: Amnesty.org verbreitete einen Schädling

SICHERHEITSLÜCKEN

VLC Media Player

Version 1.1.9 des VLC Media Players schließt zwei gefährliche Lücken in der Verarbeitung von Videodateien. Die Schwachstellen machen ältere VLC Media Player anfällig für manipulierte Webseiten oder infizierte Dateien der Formate MP4 und S3M. Dabei kann schon der Besuch einer präparierten Website zur Infektion des PCs führen.

Noch keinen Patch gab es zu Redaktionsschluss für eine als hochkritisch eingestufte Schwachstelle, die in VLC 1.1.9 entdeckt wurde, aber auch frühere Versionen betreffen könnte. Verwundbar wird VLC durch die Verwendung der „libmodplug"-Bibliothek für das Abspielen von Musikdateien.

www.videolan.org,
http://secunia.com/advisories/44412

VLC Media Player 1.1.9: Schließt zwei schwere Sicherheitslücken, lässt eine offen

Angriff gegen Hotmail

Kriminelle verschicken fingierte E-Mails des Facebook-Sicherheitsteams an Nutzer des Webmail-Dienstes Hotmail. Bereits die Voransicht der E-Mail soll ausreichen, um ein bösartiges Skript auszuführen.

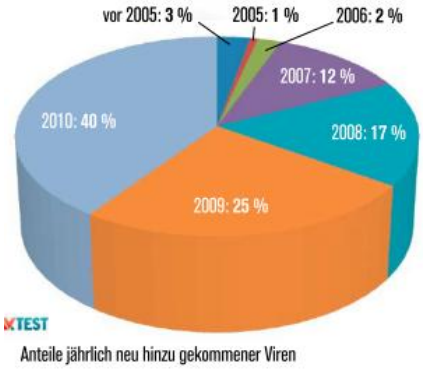
http://de.trendmicro.com/de

Jeder dritte Europäer kämpft mit Computerviren

Die EU-Statistikbehörde Eurostat hat Ergebnisse mehrerer Befragungen von EU-Bürgern ausgewertet. Danach soll durchschnittlich jeder Dritte mit Computerviren zu kämpfen haben. Vor allem Menschen in Bulgarien (58 Prozent), auf Malta (50 Prozent) und in der Slowakei (47 Prozent) sollen von Problemen mit PC-Viren betroffen sein. Die wenigsten Geschädigten gibt es laut Eurostat in Österreich (14 Prozent), Irland (15 Prozent), Finnland (20 Prozent) und Deutschland (22 Prozent). Etwa 84 Prozent der Befragten setzen eine Sicherheitslösung ein. In Deutschland sind es 88 Prozent, Spitzenreiter sind die Niederländer mit 96 Prozent. **http://pcwelt-praxis.de/Z4B**

Virenflut: 50 Millionen Schädlinge gesammelt

Im letzten Jahr ist durschnittlich alle zwei Sekunden ein neuer Virus entdeckt worden. Das Magdeburger Testinstitut AV-Test hat mitgeteilt, es habe inzwischen über 50 Millionen verschiedene schädliche Dateien in der Sammlung. Allein im Jahr 2010 sind 20 Millionen hinzugekommen. In den 1980er Jahren waren die täglichen Zuwächse noch einstellig, im Jahr 2010 kamen pro Tag bis zu 55 000 neue Schädlinge hinzu. Ein Ende der Steigerung ist laut AV-Test nicht in Sicht. **www.avtest.org**



Anteile jährlich neu hinzu gekommener Viren

Viele Programme ohne Sicherheits-Updates

Der Sicherheitsdienstleister Secunia verzeichnete 2010 einen Anstieg der PC-Sicherheitslücken um durchschnittlich 71 Prozent gegenüber 2009. Dank der Update-Automatik von Windows sind nicht mehr Microsoft-Programme das Hauptproblem. Vielmehr wird die Software anderer Hersteller seltener aktualisiert, obwohl Updates im Internet zum Herunterladen verfügbar sind. Die Computernutzer seien mit einem Dutzend oder mehr Update-Mechanismen schlicht überfordert, meint Secunia. **http://secunia.com/**

Schädliche Werbebanner in ICQ

Anfang dieses Jahres haben Online-Kriminelle im beliebten Gratis-Plauderprogramm *ICQ* dubiose Werbebanner platziert, die nutzlose Antivirenprogramme anpriesen. Dazu gaben sie sich gegenüber den Werbebannervermarktern als Bekleidungs-Onlineshop aus. Um die Tarnung echt aussehen zu lassen, hatten sie eine entsprechende Internetseite betrieben. Inzwischen wurde ihnen das Handwerk gelegt.

Angriffsbaukästen für Internetseiten

Der Sicherheitsspezialist Symantec hat die Techniken von Virenbaukästen untersucht. Mit diesen lassen sich ohne jegliche Programmierkenntnisse virenverbreitende Internetseiten erzeugen, die jeden Besucher-PC automatisch infizieren. Sie nutzen dafür immer noch die ATL-Schwachstellen in Active-X-Programmen aus. **www.symantec.de**

Quelle: PC-Welt 4/2011

Zahl des Monats

27 Prozent

der Computerbesitzer in Deutschland haben laut einer Bitkom-Umfrage noch nie ein Sicherheits-Update für das PC-Betriebssystem oder eine Software installiert. Immerhin 62 Prozent der Befragten hatten aber nach eigenen Angaben schon einmal Viren auf ihrem PC. Offenbar sind sich die Computernutzer zwar über die Gefahren im Klaren, ignorieren sie aber.

Infiziert trotz Schutz

Jeder dritte Nutzer hat einen infizierten PC – obwohl er eine aktuelle Sicherheitssoftware einsetzt. Das ergaben Auswertungen des Dienstleisters Surfright auf der Basis von rund 490.000 Nutzern.

www.surfright.nl

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 89194 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Zahl der Botnetz-PCs steigt weiter

Die Zahl infizierter PCs, die Teil eines ferngesteuerten Botnetzes geworden sind, ist im Jahr 2010 gegenüber Vorjahr um das Sechsfache gewachsen. Den Spitzenwert gab es zu Weihnachten. Unter den zehn größten Botnetzen des Jahres 2010 seien sechs vollkommen neue, so das Sicherheitsunternehmen Damballa. *http://pcwelt-praxis.de/Z4r*

2010 Botnetz (Betreibergruppe)	Anteil infizierter Rechner	Position 2009
1 TDLBotnetA (RudeWarlockMob)	14,8%	–
2 RogueAVBotnet (FreakySpiderCartel)	5,7%	–
3 ZeusBotnetB (FourLakeRiders)	5,3%	–
4 Monkif	5,2%	5
5 Koobface A	4,8%	(nicht in Top 10)
6 Conficker C	2,8%	(nicht in Top 10)
7 Hamweq (GraySunGirls)	2,5%	–
8 AdwareTrojanBotnet (WickedRockMonsters)	2,2%	–
9 Sality	2,1%	(nicht in Top 10)
10 SpyEyeBotnetA (OneStreetTroop)	1,9%	–

Getarnte Viren in CSS-Internetdaten

Mit einer neuen Methode verstecken Kriminelle schädlichen Code in Internetseiten so, dass Antiviren-Programme ihn nicht finden. Ein Internetbesucher muss eine solche Seite nur im Browser öffnen, und schon ist der PC infiziert. Die Kriminellen nutzen dafür die CSS-Daten, die eigentlich nur für das Layout der Internetseiten vorgesehenen sind. Darin verstecken Sie etwa die nötigen Übertragungs-Scripte. Diese laden dann die Viren nach, die Sicherheitslücken auf den Computern der Surfer ausnutzen.