Warum braucht man Secunia?

Das Software-Aktualisierungs-Tool PSI untersucht die installierte Software und rät dann auch schon mal vom Einsatz eines Browsers ab. Die Bewertung "Nicht sicher zum Browsen" erscheint zum Beispiel, wenn Browser-Erweiterungen installiert sind, bei denen schwerwiegende Sicherheitslücken bekannt sind.

Auf nahezu jedem PC findet sich veraltete Software, die dessen Sicherheit gefährden kann. Besonders kritisch sind dabei Anwendungen, die beim Surfen im Internet aktiviert und deshalb von bösartigen oder kompromittierten Web-Seiten direkt attackiert werden können. Microsofts Update sucht zwar automatisch nach sicherheitsrelevanten Aktualisierungen – aber nur für die hauseigene Software. So kommt es, dass Adobe Reader, Flash und Java häufig nicht auf dem aktuellen Stand sind. Mit dieser Problematik beschäftigt sich auch der aktuelle Kommnentar Mein Wunschzettel für Windows 7: Updates für Alle auf heise Security.

Secunias Personal Software Inspector (PSI) nimmt einen anderen Weg als den im Kommentar vorgeschlagenen. Er untersucht das System und vergleicht die vorgefundene Software mit einer Datenbank bekannter Sicherheitsprobleme. Für die gefundenen Sicherheitsprobleme zeigt er dann auch, wie man sie beseitigen kann. Der Anwender nimmt dabei billigend in Kauf, dass Informationen über die installierte Software an den Sicherheitsdienstleister übertragen wird.

Beim ersten Ausprobieren zeigte die neue Funktion "Sicheres Browsing" der aktuellen Beta-Version noch einige Macken. So fand sie den installierten Firefox 1.0.6 überhaupt nicht. Die Bewertung des installierten Internet Explorer hing davon ab, ob man eine erweiterte Option aktiviert hat, mit der PSI auch Sicherheitsprobleme anzeigt, die nicht einfach zu beheben sind. In der Standardeinstellung blendet PSI diese aus und lässt sie dann offenbar auch nicht in die Bewertung einfließen. Das führt dann unter Umständen zu einer irreführenden Bewertung der Sicherheit des Systems beziehungsweise der eingesetzten Software. (ju/c't)

Quelle: http://www.heise.de/ct/Secunia-PSI-gibt-Empfehlungen-zu-sicherem-Browsing--/news/meldung/139534

Jede fünfte Windows-Anwendung mit ungepatchten Sicherheitslücken

Der Sicherheits-Dienstleister Secunia meldet in seinem Blog, dass über 20 Prozent der installierten Windows-Anwendungen nicht auf dem neusten Versionsstand sind und bekannte Sicherheitslücken aufweisen. Die Zahl stammt von dem seit über einem Jahr kostenlos angebotenen Personal Security Inspector (PSI), den zurzeit knapp 200.000 Anwender auf ihren Systemen installiert haben und der Mitte Dezember in einer neuen Version erschienen ist. Das Tool scannt die auf einem Rechner installierten ausführbaren Dateien und übermittelt Informationen darüber an einen Server von Secunia, der daraufhin veraltete Versionen mit bekannten Sicherheitslücken identifiziert.

Secunia versichert in seinem Privacy Statement, dass PSI keine persönlichen Daten übermittelt und dass die gewonnenen Informationen vertraulich behandelt und lediglich statistisch ausgewertet werden – zum Beispiel für Meldungen wie diese. Die jetzt registrierten 20 Prozent unsicherer Anwendungen lassen übrigens einen Trend zur Besserung erkennen: Noch im Mai 2007 waren es laut Secunia 28 Prozent. (bo/c't)

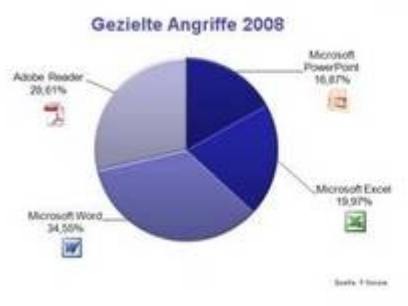
Quelle: http://www.heise.de/security/Jede-fuenfte-Windows-Anwendung-mit-ungepatchten-Sicherheitsluecken--/news/meldung/101174

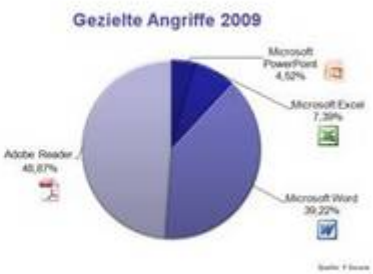
PDFs derzeit sehr beliebt bei Hackern

Von: Werner Veith

Dateianhänge sind für Hacker ein gutes Instrument für zielgerichtete Angriffe. Aktuell nehmen diese lieber PDFs als Word-Dokumente für ihre Attacken.

Um Nutzer mit Malware zu infizieren, sind Office-Formate wie Word, Excel, Powerpoint oder PDF (Portable-Document-Format) gut geeignet. In 2008 waren bei Dateianhängen Word-Dateien noch das beliebteste Mittel von Hackern, um Malware zu verteilen. In 2009 haben nach einer Untersuchung von F-Secure jedoch PDFs den Word-Dokumenten den Rang abgelaufen. Grund dafür sind zwei Schwachstellen in PDF-Javascript-Funktionen von Adobe. Der Security-Anbieter rät daher Javascript in Acrobat beziehungsweise Acrobat-Reader vollständig zu deaktivieren oder auf einen anderen PDF-Reader umzusteigen. Dies gilt, bis Adobe dafür einen Patch gebracht hat.





Gegenüber 2008 haben Angriffe über PDF-Dateianhänge in 2009 deutlich zugenommen.

Die hohe Anzahl von Angriffen über PDFs geht auf eine Schwachstelle bei Adobe zurück, die in den Javascript-Funktionen »getAnnots()« und »spell.customDictionaryOpen()« vorhanden ist. Über diese Schwachstelle führen Hacker Code remote aus. Dies passiert entweder bei gezielten Angriffen oder bei Drive-by-Downloads.

Knapp 50 Prozent der Angriffe erfolgten in 2009 bisher über PDFs. Dann kommen Word-Dokumente mit 39,22 Prozent. Gegenüber 2008 waren es hier 4,67 Prozent mehr. Bei PDFs waren es in 2008 nur 28,61 Prozent. Damit hat die Gefahr durch Word-Dokumente durch das PDF-Problem nicht abgenommen. Deutlich weniger für Angriffe wurden dagegen Excel- (7,39 Prozent) und Powerpoint-Dateien (4,52 Prozent) verwendet. In 2008 waren dies noch 19,97 beziehungsweise 16,87 Prozent.

Quelle: http://www.networkcomputing.de/pdfs-derzeit-sehr-beliebt-bei-hackern/

Überprüfung auf fehlende Patches

Der "Secunia Personal Software Inspector" (Secunia PSI) ermittelt, welche Programme auf dem eigenen PC noch nicht gegen aktuelle Sicherheitslücken gepatcht sind.

Foto-Show Secunia PSI

Nur für Privatanwender
Die Software prüft auf fehlende Updates von Programmen und Systembestandteilen wie beispielsweise Flash, Java, QuickTime, Skype, Firefox und Opera. Secunia PSI ist ausschließlich für Privatanwender zur kostenfreien Nutzung freigegeben.

Kauf-Empfehlung Kaspersky Anti Virus
Kauf-Empfehlung Avira AntiVir Premium

Sicherheitslücken schließen
Das Freeware-Tool durchstöbert die gesamte Festplatte und vergleicht die Versionsnummern der gefundenen Programme mit der eigenen Datenbank. Secunia PSI informiert Sie, falls Updates installierter Programme erhältlich sind. So können Sie Sicherheitslücken mit einer neuen Version schließen.

Kauf-Empfehlung Kaspersky Internet Security
Kauf-Empfehlung G-DATA InternetSecurity
Kauf-Empfehlung Avira Internet Security Suite

Ordner ausschließen
Die Download-Links der Programmme werden gleich mit angezeigt, so dass Sie alle wichtigen Programme schnell und einfach wieder auf den aktuellen Stand bringen können. Zahlreiche Feineinstellungen sind möglich. Beispielsweise lassen sich bestimmte Ordner oder Dateien von der Suche ausschließen. Das aktuelle Update erkennt neue Sicherheitslücken und bietet nun auch eine deutschsprachige Oberfläche.

Alternativen
Der Microsoft Baseline Security Analyzer macht sich auf die Suche nach Sicherheitslücken, fehlenden Patches sowie anderer ungenügender Sicherheitseinstellungen und Schwachstellen in Windows-Systemen. Die Patch-Sammlung WinFuture Windows Vista Update Pack enthält alle aktuellen Sicherheits-Patches, Updates und Hotfixes für Windows Vista. Norton 360 All-In-One Security sorgt für mehr Sicherheit auf Ihrem Rechner. Verbessert wurden vor allem der Schutz gegen Online-Identitätsdiebstahl und neue Gefahren wie Drive-by Downloads. Mit dem T-Online SicherheitsPaket treffen Sie Vorsichtsmaßnahmen gegen vielfältige Gefahren aus dem Internet wie Viren, Würmer, Hacker und unseriöse Dialer.

Fazit
Der "Secunia Personal Software Inspector" hält die wichtigsten Systemprogramme auf dem aktuellen Stand und schließt somit die gefährlichsten Sicherheitslücken.

Quelle: http://download.softwareload.de/Secunia-Software-Inspector/48973

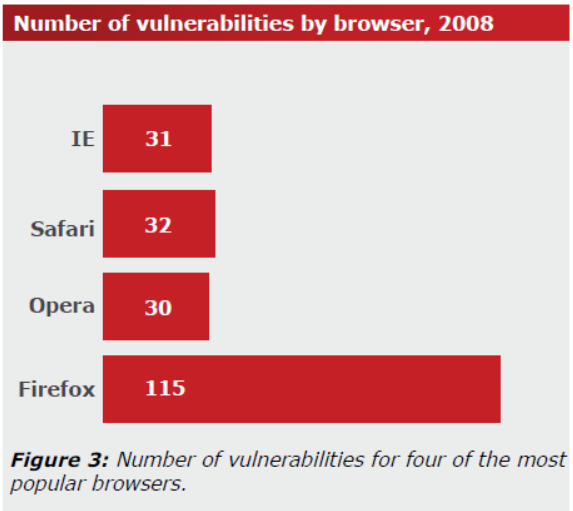


Figure 3: *Number of vulnerabilities for four of the most popular browsers.*

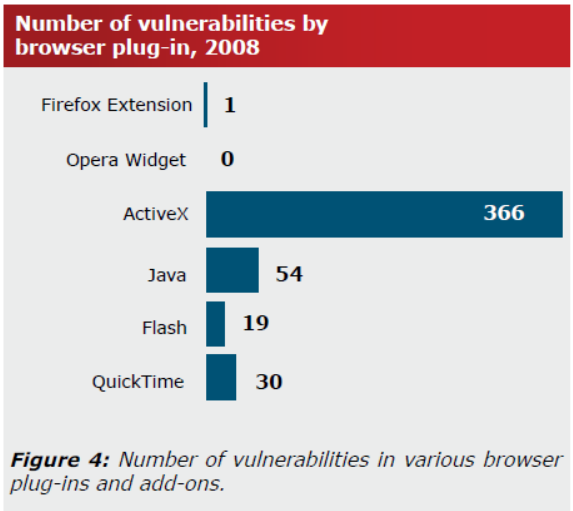


Figure 4: *Number of vulnerabilities in various browser plug-ins and add-ons.*

Software	Number of Installations,	percent insecure
Sun Java JRE 1.6.x/6.x	2,831,001	38%
Adobe Flash Player 9.x	2,389,661	34%
Adobe Reader 8.x	1,836,982	8%
Apple QuickTime 7.x	1,205,226	27%
Mozilla Firefox 2.0.x	544,384	14%
Sun Java JRE 1.5.x/5.x	473,783	97%
Mozilla Firefox 3.0.x	400,721	10%
Macromedia Flash Player 6.x	383,884	81%
iTunes 7.x	357,439	5%
Adobe Reader 7.x	297,827	15%

***Table 3**: Top ten most commonly detected applications based on the Secunia OSI in 2008.*

Secunia Advisory ID for disclosed vulnerabilities	Criticality	Disclosure date	Patching date	Number of days before patch release
Internet Explorer				
SA30857	Moderate	2008-06-26	2008-10-14	110
SA30851	High	2008-06-26	2008-10-14	110
SA30145	Not critical	2008-05-12	Unpatched	233
SA30141	Less critical	2008-05-14	Unpatched	231
SA29453	Less critical	2008-03-24	2008-06-10	78
SA29346	Less critical	2008-03-12	Unpatched	294
Mozilla Firefox				
SA32192	Not critical	2008-10-14	2008-13-11	30
SA32040	Not critical	2008-10-01	2008-12-26	86
SA28622	Less critical	2008-01-24	2008-02-08	15

This table considers only those vulnerabilities publicly disclosed without or prior to vendor notification.

The number of days unpatched are in red for those vulnerabilities that are still unpatched as of 31 December 2008.

***Table 5:** Window of exploitation for vulnerabilities publicly disclosed in IE and Firefox, 2008.*

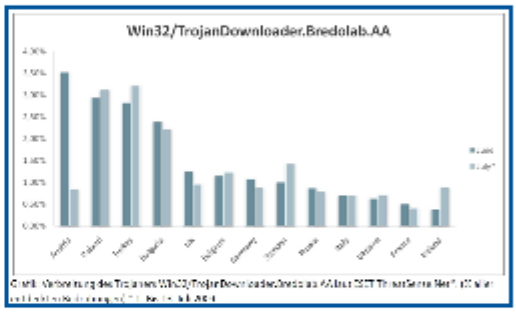
Quelle: http://secunia.com/gfx/Secunia2008Report.pdf

Neuer Trojaner Bredolab treibt in Europa sein Unwesen

Drucken Senden

Starke Verbreitung über PDF- und SWF-Dateien

Jena, 16.07.2009 – Der Sicherheitsspezialist ESET warnt vor dem neuen Trojaner Win32/TrojanDownloader.Bredolab.AA, der bereits europaweit zu den Top 10 Schädlingen zählt. Bredolab verbreitet sich über harmlos erscheinende PDF- und SWF-Dateien und lädt nach der Infektion des PCs weitere Schadsoftware aus dem Internet herunter. Die ESET-Experten raten dringend davon ab, PDF- und SWF-Dateien aus unbekannten oder verdächtigen Quellen zu öffnen. Im Zweifelsfall sollte der kostenlose ESET Online-Scanner für eine Überprüfung genutzt werden.



Durch das Öffnen einer infizierten Datei wird Bredolab aktiviert. Der Schädling nistet sich dann in den Systemdateien ein und wird bei jedem Bootvorgang des PCs automatisch gestartet. Ohne Wissen des Anwenders verbindet sich Bredolab sofort per HTTP-Verbindung mit einem Remote-Server. Von dort lädt er Adware, Spyware und weitere Schadsoftware herunter. Kriminelle können so ohne Probleme Passwörter und sensible Daten des Anwenders stehlen oder ihn mit Werbung bombadieren. Im schlimmsten Fall wird der eigene PC zum Teil eines Botnets und für den massenhaften Versand von SPAM oder Cyberattacken missbraucht.

Laut den Statistiken der ESET Virenlabors treibt Bredolab in ganz Europa sein Unwesen. In Tschechien und der Slowakei ist er der meistverbreitete Schädling. In Österreich, Polen und der Türkei rangiert er unter den Top 5. In Deutschland, England, Schweden, Belgien und Russland wird Bredolab unter den Top 10-Schädlingen geführt. Auch in zahlreichen weiteren europäischen Ländern verbreitet sich Bredolab rasant.

Win32/TrojanDownloader.Bredolab.AA gilt als besonders gefährlich, da er unterschiedliche Schadsoftware hinzuladen kann. Je später der Trojaner erkannt wird, desto mehr Malware muss auf dem infizierten PC vermutet werden. Dies erschwert eine vollständige Desinfektion des Rechners. Auch die Verbreitung über das als weniger riskant geltende PDF-Format macht den Schädling so tückisch.