www.chip.de

Die unsichersten Programme der Welt

Diese Software lebt gefährlich

Markus Mandau

Schädlinge brauchen verletzliche Programme, um den Rechner zu infizieren. Und davon gibt es jede Menge. CHIP Online nennt die Top 10 der unsichersten Anwendungen und sagt, wie Sie Angriffen auf Firefox, Office & Co. entkommen

Hai-Tauchen erlebt einen Boom. Immer mehr Touristen suchen den ultimativen Nervenkitzel – Auge in Auge mit dem Meeresräuber. Wer an einem solchen Event vor der Küste Südafrikas teilnimmt, steigt in einen Metallkäfig knapp unter der Wasseroberfläche und schießt von dort aus spektakuläre Urlaubsfotos – von weißen Haien, die mit blutigen Fleischstückchen angelockt werden.

Die neue CHIP: Jetzt am Kiosk.

Kein Teilnehmer einer solchen Veranstaltung würde auf die Idee kommen, ohne den Schutz des Käfigs ins Wasser zu steigen. Doch genau so verhalten sich viele Surfer, die im Internet unterwegs sind: Sie vernachlässigen wichtige Sicherheits-Updates und laden Hacker geradezu ein, auf ihren Rechnern herumzuschnüffeln. Der Sicherheitsdienstleister Trusteer hat die Software auf 2,5 Millionen Rechnern überprüft. Das Ergebnis: 80 Prozent aller User surfen mit veralteten und unsicheren Flash-Versionen. Für den Adobe Reader liegt der Wert sogar bei 84 Prozent. Da reicht der Besuch einer infizierten Website oder das Öffnen eines manipulierten Dokuments und die Malware nistet sich auf dem heimischen System ein.

Windows wird sicherer?

Da Windows mit jeder neuen Version umständlicher zu knacken ist, versuchen Hacker zunehmend, über unsichere Anwendungen auf fremde Rechner zu gelangen. Und ihre Chancen stehen gar nicht schlecht.

Die National Vulnerability

Database der USA, die der „Homeland Security“-Behörde angeschlossen ist, listet bis dato 38.571 Sicherheitslücken in Software-Produkten auf. Momentan kommen im Durchschnitt 19 pro Tag hinzu.

National Vulnerability Database: Diese US-Behörde check jeden Tag Software auf Sicherheitslecks.

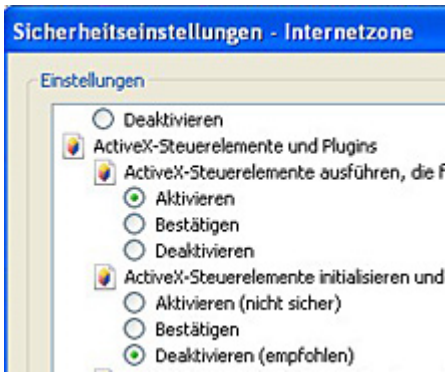
Viele Sicherheitslecks betreffen Software, mit denen der normale User wenig in Berührung kommt, etwa Suns Betriebssystem Solaris. Doch auch populäre Programme, die sich auf jedem Rechner finden, stehen in der Rangliste ganz weit oben. Umso wichtiger ist es, diese Programme durch Update-Tools immer aktuell zu halten oder – besser noch – sich nach sicheren Programmen umzusehen.

Die neue CHIP: Jetzt am Kiosk.

Doch bevor wir die Security-Lücken im Detail erläutern und sichere Software-Alternativen vorstellen, ist es noch dringlicher, einen Blick auf die Windows-Schnittstelle zu werfen, die seit Jahren für Ärger sorgt: ActiveX. Laut Bericht der IBM-Sicherheitsabteilung X-Force dominieren auch 2009 Webattacken über die ActiveX-Schnittstelle mit einem Anteil von 60 Prozent. Drei der fünf häufigsten Browserangriffe nutzen Lücken des Windows-Moduls.

ActiveX: Windows’ offene Wunde

ActiveX wurde 1996 in Windows implementiert, um Standardprogramme wie Internet Explorer, Media Player und Outlook, um neue Funktionen zu erweitern, wie etwa das ActiveX Control für QuickTime.



Internet Explorer: ActiveX läßt sich in den Internetoptionen abschalten.

Entwickelt zu einer Zeit, als das Internet noch kein so gefährlicher Ort war, gilt ein ActiveX-Plug-in allein durch seine Signatur als vertrauenswürdig. ActiveX-Komponenten, die sich als unzuverlässig erwiesen haben, kann Microsoft per Update durch einen Registry-Eintrag mit einem Killbit markieren und damit deaktivieren. Wenn Sie einmal selbst nachsehen wollen, welche Killbits auf Ihrem System gesetzt sind, finden Sie diese unter »HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Com patibility«. Gekennzeichnet wird das Killbit durch ein »Compatibility-Flag« mit dem Wert »0x00000400«.

ActiveX-Lücken wirken so schwerwiegend, weil betroffene Plug-ins dieselben Systemrechte haben wie die Programme, in denen sie laufen. Beispielsweise surft ein XP-Anwender mit dem

Internet Explorer normalerweise als Administrator, die ActiveX-Module haben also vollen Systemzugriff; in Vista und Windows 7 bietet die User Account Control zumindest einen grundlegenden Schutz – sofern sie eingeschaltet ist.

Jede infizierte Website kann Lücken in einem ActiveX-Plug-in nutzen. Dazu braucht sie nur dessen ID-Kennung und schon startet das unsichere Plug-in im Browser. Wer auf die Dienste von ActiveX verzichten kann, sollte es im Internet Explorer ausschalten. Sie finden die entsprechenden Einstellungen unter »Extras | Internetoptionen | Sicherheit | Stufe anpassen«.

Die neue CHIP: Jetzt am Kiosk.

Ende Juli haben sich die Probleme noch einmal vervielfacht: Zwei Lücken in der ATL-Bibliothek (Active Template Library), mit der ActiveX-Plug-ins programmiert werden, stellen das ganze System infrage. Prinzipiell muss nun jedes jemals erstellte Plug-in überprüft und unter Umständen neu programmiert werden.

Die eine ATL-Lücke ermöglicht einen Buffer Overflow, womit ein infiziertes Plug-in in andere Speicherbereiche schreiben kann, die etwa für Windows-Dienste reserviert sind. Die zweite Lücke umgeht das Killbit in der Registry und erlaubt so, unsichere Plug-ins ohne Wissen des Users zu aktivieren. Mittlerweile hat Microsoft für Outlook und den Media Player entsprechende Patches herausgegeben, die das Problem beheben. Zusätzlich können Anwender auch einen alternativen Browser einsetzen, der von sich aus keine ActiveX-Plug-ins ausführt.

Die Wahl des Webbrowsers entscheidet mittlerweile über die Sicherheit des Systems insgesamt. Laut IBM-Report sind die Hälfte aller sicherheitskritischen Lücken in Browsern zu finden – jedenfalls, was die Consumer-Produkte angeht.

Browser: Firefox ist voller Löcher

Jahrelang galt der Internet Explorer als unsicher. Kein Wunder, denn Microsoft hatte seinen Browser vernachlässigt, bis es fast schon zu spät war. Firefox profitierte davon und viele User wechselten zum Open-Source-Browser, weil sie ihn für vertrauenswürdiger hielten als den IE.

Inzwischen sehen die Dinge anders aus: Allein im Jahr 2009 sind für den Firefox über 80 Sicherheitslücken bekannt geworden. Damit steht der Browser einsam an der Spitze und bestätigt eine negative Tendenz auch im Vergleich zum Internet Explorer.


Sicherheitslücken: Jeder Browser hat seine Schwächen.

Die Anzahl der Firefox-Lücken steigt seit zwei Jahren stetig an, die des IE sinkt leicht. Trotzdem lässt sich mittels statistischer Daten nicht

unbedingt sagen, welcher der beiden Browser sicherer ist. Mozilla geht sehr offen mit den aufgetauchten Sicherheitslücken um, Microsoft hingegen verschweigt auch mal gerne die Probleme, die von Malware noch nicht ausgenutzt werden.

Deshalb lohnt für die Wahl des richtigen Browsers manchmal ein Blick in die Details: Die meisten Angriffe erfolgen heutzutage per Cross-Site-Scripting (XSS) und ähnliche Methoden. Dabei wird durch den Austausch eines HTML-Elements gefährlicher Inhalt in eine sonst vertrauenswürdige Website eingebaut. Die Browserfehler, die XSS ausnutzen, können vergleichsweise trivial sein. Bestes Beispiel dafür ist eine jüngst aufgetauchte Sicherheitslücke, mit der sich die SSL-Zertifizierung austricksen lässt. Eine kleine Modifikation der Adresse reicht völlig aus: Bei einem Klick auf einen Link nach dem Muster www.paypal.com/0.malware.org reicht vielen Browsern das gültige Zertifikat für Paypal aus, da sie die „0“ als Stoppzeichen interpretieren. Die eigentliche Domain kommt jedoch erst nach der „0“ – und auf der sitzt dann der Hacker.

Die neue CHIP: Jetzt am Kiosk.

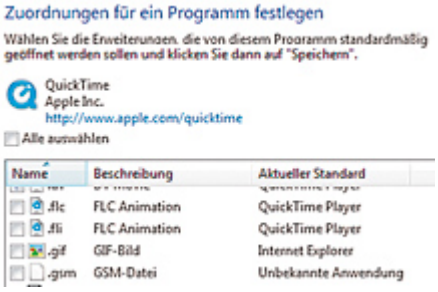
Firefox 3.5 lässt sich so nicht betrügen, der IE schon. Andererseits können Angreifer über den SSL-Trick die Update-Funktion von Firefox nutzen, um Malware auf dem System zu installieren. Das geht wiederum beim IE nicht, da Microsoft die Gültigkeit nicht nur per SSL checkt. Der User ist also bei beiden Browsern gefährdet.

Naheliegend wäre da der Griff zu alternativen Lösungen wie Apples Safari oder Google Chrome, bei denen der SSL-Trick auch nicht funktioniert. Doch leider stehen diese Browser in der Lückenstatistik ebenfalls weit vorne. Schuld daran ist oft die Webkit-Engine, die in beiden für die Verarbeitung von JavaScript zuständig ist. Man hat in ihr allein in diesem Jahr bisher über 30 Lücken gefunden. Beim Thema Sicherheit bleibt damit Opera als einzige Browserempfehlung übrig, zumal viele Lücken in Opera als nicht besonders schwerwiegend eingestuft werden.

Multimedia: Crash für Apple & Adobe

Der sicherste Browser nützt wenig, wenn wichtige Erweiterungen für Webinhalte angreifbar sind. Multimedia-Plug-ins wie QuickTime oder der Flash Player werden von Hackern gerne ins Visier genommen, denn sie sind auf fast allen Systemen zu finden.

Die Marktabdeckung des Flash Players hat laut Adobe mittlerweile 99 Prozent erreicht. Die Wahrscheinlichkeit für einen erfolgreichen Angriff ist hier also höher, als bei einem direkten Angriff auf den Browser, da selbst der Marktführer IE nur noch von rund 65 Prozent der User benutzt wird.



QuickTime: Für sämtliche Formate außer MOV sollten Sie QuickTime nicht als Standardplayer nutzen

Multimedia-Plug-ins sind häufig anfällig für Attacken, die einen Buffer Overflow erzeugen. Das Szenario ist eigentlich immer dasselbe: Der Surfer wird dazu verleitet, einen infizierten Video- oder Audiostream zu öffnen, der QuickTime oder Flash dazu bringt, über den reservierten Speicherbereich hinaus zu schreiben. Auf diese Weise lässt sich ausführbarer Code in das System einschleusen. Sicherheitslücken, die einen Buffer Overflow ausnutzen, werden deshalb immer als kritisch eingestuft. Kein Wunder, dass QuickTime mit 9,2 von 10 einen sehr hohen Durchschnittwert bei der Schwere der Sicherheitslecks hat.

Die neue CHIP: Jetzt am Kiosk.

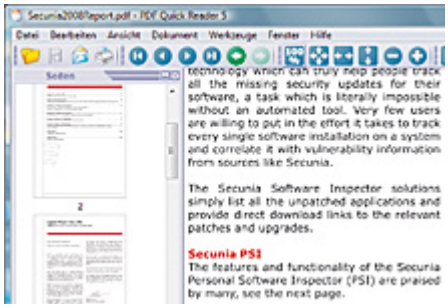
Leider lässt sich das Problem nicht eingrenzen, denn das Multimedia-Plug-in hat Schwachstellen über verschiedene Formate hinweg. Allein in diesem Jahr sind neben den üblichen MOV-Dateien beispielsweise auch AVI-Filme sowie Bilder im PSD-Format betroffen. Da sich QuickTime nicht komplett ersetzen lässt, bleiben Usern nur zwei Möglichkeiten: QuickTime deinstallieren oder so einstellen, dass das Plug-in nur noch MOV-Streams abspielt, denn für alle anderen Formate gibt es Alternativen.

Bei Adobe liegen die Dinge komplizierter, denn der Flash-Player ist das Standard-Plugin, um sich Filme online anzusehen. Wenn Sie auf bekannten Sites wie etwa YouTube surfen, kann Ihnen wenig passieren. Ansonsten haben Sie praktisch nur die Möglichkeiten, Flash im Browser zu deaktivieren oder über einen Filter Flash-Inhalte bei Bedarf zu blocken – das geht im Internet Explorer über das Plug-in IE7pro, bei Firefox mit dem Plug-in FlashBlock . Übrigens: Inzwischen prüft Firefox, ob eine veraltete Version des Flash-Players installiert ist und rät zu einem Update.

Adobe Reader: Gefährliche PDF-Skripte

Nach den Browsern geben laut dem X-Team von IBM die Office-Programme mit fast 30 Prozent die häufigsten Angriffsziele ab. Am stärksten betroffen ist der Adobe Reader, der PDF-Dokumente darstellt.

Denn im Adobe Reader stecken auch die anfälligen Flash-Bibliotheken. Darüber hinaus werden Flash-Animationen per ActionScript gesteuert. Fehler in dieser Sprache machen daher alle Adobe-Produkte anfällig bis hin zu AIR, einer Plattform für Webanwendungen.



PDF Quick Reader: Die Alternative zum unsicheren Adobe Reader.

Neuestes Beispiel ist das Heap Spraying mittels ActionScript. Heap Spraying wird hauptsächlich dazu genutzt, den Arbeitsspeicher mit sinnlosem Code aufzufüllen, Ziel ist letzten Endes ein Buffer Overflow. Heap Spraying mittels JavaScript ist bekannt, und für den Adobe Reader gibt es da eine einfache Lösung: Navigieren Sie über das Menü »Bearbeiten« in die »Voreinstellungen«, gehen Sie auf »JavaScript« und entfernen Sie das Häkchen vor »Acrobat

JavaScript aktivieren«. Eine entsprechende Vorgehensweise für ActionScript ist nicht möglich, denn die Flash-Funktionalität im Adobe Reader lässt sich nicht deaktivieren.

Die neue CHIP: Jetzt am Kiosk.

Wer als Anwender auf der sicheren Seite sein will, der sollte zu einem Ersatz für den Adobe Reader greifen wie etwa den PDF Quick Reader. Diese alternativen PDF-Leser können kein Flash darstellen und sind daher von dieser Lücke nicht betroffen.

Die Probleme mit dem Adobe Reader waren kurzzeitig so groß, dass der Virenschutzhersteller F-Secure von dessen Einsatz abgeraten hat. Mittlerweile hat Adobe reagiert und wie Microsoft einen festen Patch-Day für den Reader eingerichtet. Der für den Flash Player steht allerdings noch aus.

Microsoft Office: Zahlreiche Lücken

Microsoft Office ist dagegen nicht mehr so häufig das Ziel von Malware-Attacken, was aber nicht an fehlenden Sicherheitslücken liegt.

Zwei Dinge fallen bei den in diesem Jahr bekannt gewordenen Mankos auf: Sie sind alle als schwerwiegend eingestuft, da infizierte Dokumente immer einen Buffer Overflow auslösen, und sie betreffen praktisch ausschließlich zwei Office-Module: Excel und PowerPoint. User können diesem Problem relativ leicht aus dem Weg gehen, indem sie Dokumente in diesen Formaten einfach nicht öffnen, wenn sie im Internet angeboten werden.

MS Office: Zahlreiche Lücken.

Die neue CHIP: Jetzt am Kiosk.

Für Experten und Anwender, die es genau wissen wollen, bietet Microsoft das Tool OffVis in einer Beta-Version an. OffVis öffnet Office-Dokumente, zeigt sie in Hex-Code an und bildet ihre innere Struktur mit den eingebundenen Elementen ab. Zusätzlich identifiziert OffVis sogar Schädlinge, die bekannte Sicherheitslücken ausnutzen.

All diese Maßnahmen nützen natürlich herzlich wenig, wenn Anwender wichtige Sicherheits-Updates gar nicht erst aufspielen. So tauchen in letzter Zeit vermehrt infizierte PowerPoint-Dokumente auf, die eine schon seit drei Jahren geschlossene Lücke ausnutzen, um einen Trojaner in das System einzuschleusen. OffVis kennt diesen Schädling, Ihr Office auch?

Top 5: Die meistgenutzten Browserlücken

Allen Browserlücken ist zweierlei gemein: Sie werden über die bekannten Exploit Toolkits der Malwareszene vertrieben. Und sie lassen sich durch Software-Updates schließen.

1. Microsoft MDAC ActiveX: Kennung: CVE-2006-0003
Das ist eine Lücke in den Microsoft Data Access Components, die für den Zugriff auf Datenbanken und Datenquellen genutzt wird. Dadurch kann der Angreifer die Sicherheitseinstellungen des IE umgehen.

2. MS Snapshot Viewer ActiveX: Kennung: CVE-2008-2463
Das ActiveX-Plug-in im MS-Office Snapshot-Viewer ermöglicht Remote-Zugriff auf den Rechner, um beispielsweise ein schädliches Skript zu hinterlegen.

3. Adobe Reader: Kennung: CVE-2007-5659
Ein präpariertes PDF verursacht einen Buffer Overflow im Adobe Reader und schleust darüber Malware auf den PC.

4. Microsoft Internet Explorer 7: Kennung: CVE-2009-0075
Der Aufruf einer präparierten Website ermöglicht das Ausführen von infiziertem Code über den Internet Explorer 7.

5. RealPlayer ActiveX: Kennung: CVE-2007-560
Ein Fehler im Datenbankmodul des Real Players erzeugt einen Buffer Overflow.