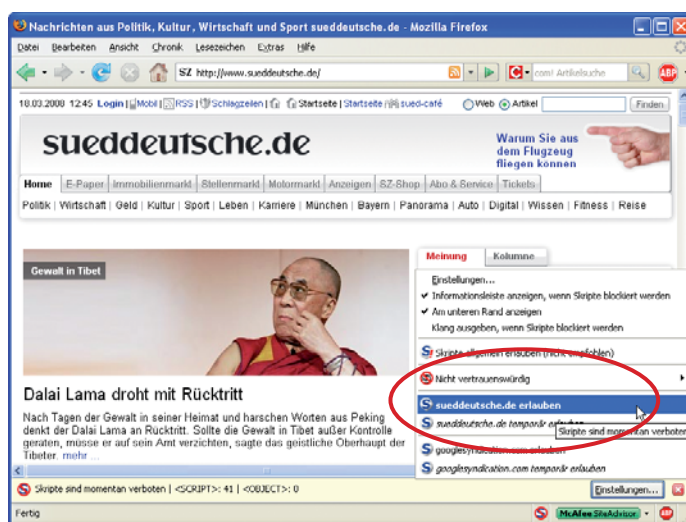


# Drive-by-Downloads: Infektion beim Surfen

Drive-by-Downloads nutzen Sicherheitslücken im Browser und installieren unbemerkt Schädlinge auf Ihrem Computer. So schützen Sie sich gegen die unsichtbare Gefahr beim Surfen.

Viele Anwender fühlen sich sicher, wenn sie einen Virens Scanner und eine Firewall installiert haben, mit Firefox surfen und Windows regelmäßig aktualisieren. Dabei gibt es eine zunehmende Bedrohung im Internet, bei der ein Computer bereits beim Besuch einer manipulierten Webseite mit einem Schädling infiziert wird – ohne dass der Anwender dies überhaupt bemerkt. Die Technik wird Drive-by-Downloads genannt.

Schädlinge, die sich über Lücken im Browser verbreiten, gibt es schon länger. Die Bedrohung durch Drive-by-Downloads hat jedoch in letzter Zeit enorm zugenommen. Google hat rund drei Millionen Drive-by-Download-Adressen in seinem Index gefunden. Im Schnitt versu-



Firefox-Erweiterung Noscript 1.5.2: Das Add-on blockiert Javascript. Sie sollten diese Technik nur auf seriösen Seiten erlauben (Bild B)

chen laut Google 2,5 Prozent aller geprüften Adressen, heimlich Schädlinge auf fremden PCs zu installieren. Außerdem verweisen 1,3 Prozent aller Suchergebnisse bei Google auf Drive-by-Download-Seiten. Das Risiko, versehentlich auf einer Webseite zu landen, die einen Trojaner oder ein Rootkit installiert, ist also groß.

Selbst wer nur vertrauenswürdige Webseiten besucht, ist nicht sicher. Die kriminellen Banden schleusen immer wieder Banner in große Werbenetze ein, die dann Schädlinge automa-

**Riskante Sites:** Adressen mit Raubkopien versuchen besonders oft, Schädlinge zu installieren (Bild A)

tisch verbreiten. Wie Sie sich trotzdem gegen Drive-by-Downloads schützen, lesen Sie im folgenden Artikel. Alle benötigten Programme finden Sie auf Heft-CD und -DVD in der Rubrik „Internet, Drive-by-Downloads“.

## Gefahr beim Surfen

Ein Drive-by-Download erfolgt in mehreren Stufen: Zuerst besucht der Surfer eine vermeintlich harmlose Seite. Dort wird ein Java-

script ausgeführt, das auf eine oder mehrere Sicherheitslücken im Browser abzielt. Ist das Skript erfolgreich, folgt der Download einer ausführbaren Datei auf den PC des Surfers. Dieser Downloader lädt dann weitere Schädlinge herunter.

Zur Verbreitung dienen nicht nur halbseidene Adressen (Bild A), sondern auch immer wieder seriöse Seiten. Letztere wurden entweder gehackt, oder es läuft auf ihnen ein manipuliertes Banner.

### ActiveX

ActiveX ist eine von Microsoft entwickelte Technik, mit der sich aktive Inhalte im Internet Explorer darstellen lassen. Da ActiveX über kein eigenes Sicherheitsmodell verfügt, verwenden Hacker die Technik besonders gern, um fremde PCs mit einer manipulierten Webseite zu infizieren.



**Steckbrief: Drive-by-Downloads – Infektion beim Surfen**

**Kompakt**

Drive-by-Downloads schleusen Schädlinge unbemerkt auf fremden PCs ein. Dazu nutzen sie Lücken im Browser oder in Add-ons.  
 Wegen verseuchter Banner sind auch seriöse Seiten nicht mehr sicher.  
 Noscript blockiert gefährliche Webskripts. Adblock Plus filtert manipulierte Banner aus.

**Inhalt**

- **Gefahr beim Surfen**
  - ActiveX S. 82
  - Javascript S. 83
  - Verseuchte Banner S. 83
- **Gefahr durch Software-Lücken**
  - Veraltete Software aktualisieren S. 84
- **Gefahr durch Downloads**
  - Gefälschte Seiten S. 84

**Weitere Infos**

- [www.virustotal.com](http://www.virustotal.com)  
Prüft verdächtige Dateien mit 32 Virensclannern
- <http://research.google.com/archive/provos-2008a.pdf>  
Google-Whitepaper zu Drive-by-Downloads
- [www.com-magazin.de/tipps/1601](http://www.com-magazin.de/tipps/1601)  
Phishing-Seiten mit Firefox blockieren

**Software-Übersicht**

Programm	Quelle	Seite
Adblock Plus 0.7.5.3 (Werbeblocker)	<a href="http://www.erweiterungen.de">www.erweiterungen.de</a>	83
Firefox 2.0.0.13 (Webbrowser)	<a href="http://www.mozilla-europe.org">www.mozilla-europe.org</a>	83
Noscript 1.5.2 (Skript-Blocker)	<a href="http://www.noscript.net">www.noscript.net</a>	83
Secunia PSI 0.9.0.1 (Update-Checker)	<a href="http://psi.secunia.com">http://psi.secunia.com</a>	84

Die -Programme finden Sie auf Heft-CD und -DVD in der Rubrik „Internet, Drive-by-Downloads“.

**Abschalten von Javascript.** Bei Firefox findet sich diese Funktion unter „Extras, Einstellungen ..., Inhalt“. Dann funktionieren viele Webseiten jedoch nur noch eingeschränkt.

Besser ist es, Javascript zu deaktivieren und auf vertrauenswürdigen Webseiten jeweils gezielt wieder einzuschalten. Das geht mit der Erweiterung Noscript 1.5.2 ([www.noscript.net](http://www.noscript.net), kostenlos), die Sie auf Heft-CD und -DVD in der Rubrik „Internet, Drive-by-Downloads“ finden.

Kopieren Sie die XPI-Datei auf Ihre Festplatte und ziehen Sie diese dann vom Windows-Explorer mit der Maus in ein Firefox-Fenster. Es öffnet sich ein kleines Fenster mit einem kurzen Countdown. Warten Sie einen Moment und klicken Sie dann auf „Jetzt installieren“. Mit „Firefox neustarten“ aktivieren Sie Noscript.

Auf jeder neu besuchten Webseite, die Javascript verwendet, blendet Firefox in Zukunft unten eine Leiste mit dem Hinweis „Skripte sind momentan verboten“ ein. Um Javascript auf dieser Seite zu aktivieren, klicken Sie rechts in der Leiste auf „Einstellungen...“ und wählen die Zeile mit der Adresse der gewünschten Webseite aus (Bild B). Firefox lädt die Adresse nun mit aktiviertem Javascript neu.

**Verseuchte Banner**

Es gibt zwei Möglichkeiten, ein gefährliches Skript auf einer fremden Webseite unterzubringen: Die klassische Methode ist, den Server zu hacken. Neuerdings verwenden die Kriminellen jedoch auch manipulierte Banner.

Moderne Werbe-Netzwerke vermieten nämlich meist einen Teil ihrer Kapazitäten an Partner weiter, welche die Werbeplätze in vielen Fällen ihrerseits wieder weiterreichen. Ein Team von Google-Forschern hat nachgewiesen, wie auf der Webseite eines dänischen Radiosenders ein Drive-by-Download-Banner eingeblendet wurde, das über eine Kaskade von sechs verschiedenen Werbenetzen auf der Seite landete.

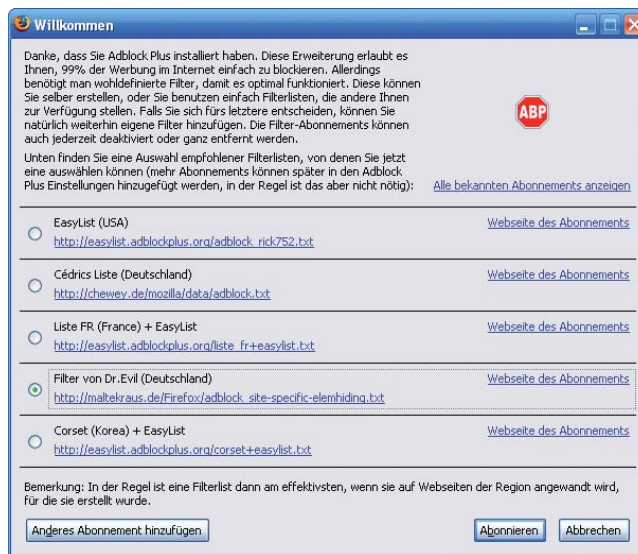
**So schützen Sie sich:** Das Add-on Adblock Plus 0.7.5.3 ([www.erweiterungen.de/detail/Adblock\\_Plus](http://www.erweiterungen.de/detail/Adblock_Plus), kostenlos) filtert Werbung aus, bevor sie von Ihrem Browser geladen wird. Ein manipuliertes Banner hat so keine Chance, Ihren PC zu verseuchen. ▶

**So schützen Sie sich:** Surfen Sie nicht mehr mit dem Internet Explorer. Installieren Sie stattdessen Firefox 2.0.0.13 ([www.mozilla-europe.org](http://www.mozilla-europe.org), kostenlos). Dieser Browser führt keine riskanten ActiveX-Komponenten aus und wird zudem erheblich häufiger und vor allem schneller aktualisiert als der Internet Explorer.

**Javascript**

Javascript ist eine häufig verwendete Skriptsprache, mit der sich Webseiten um zusätzliche Funktionen oder Effekte erweitern lassen. Kriminelle Banden setzen Javascript gezielt ein, um über Lücken im Browser oder in den darin installierten Add-ons Schadcode auf den PC des Anwenders herunterzuladen und dort auszuführen.

**So schützen Sie sich:** Die einfachste Methode, sich gegen gefährliche Webskripts zu schützen, ist das komplette



**Firefox-Erweiterung Adblock Plus 0.7.5.3:** Mit einem Filterabonnement aktualisiert sich der mächtige Werbeblocker automatisch (Bild C)

Sie finden die Erweiterung auf Heft-CD und -DVD in der Rubrik „Internet, Drive-by-Downloads“. Kopieren Sie die XPI-Datei in einen Ordner auf Ihrer Festplatte und ziehen Sie diese anschließend mit der Maus in ein Firefox-Fenster. Beim ersten Start fordert Sie das Add-on auf, ein kostenloses Filterabonnement auszuwählen. Markieren Sie die Liste von Dr. Evil und bestätigen Sie mit „Abonnieren“ (Bild C). Ab jetzt blockiert Firefox den Großteil der Internetwerbung.

Wie Sie mit Firefox und dem Add-on Siteadvisor Phishing-Seiten automatisch erkennen und blockieren, lesen Sie unter [www.com-magazin.de/tipps/1601](http://www.com-magazin.de/tipps/1601).

## Gefahr durch Software-Lücken

Viele Drive-by-Download-Seiten zielen auf Lücken in Programmen wie Adobe Reader oder Real Player, um sich heimlich auf einem PC einzuschleichen. Es ist deswegen wichtig, diese Tools immer auf dem aktuellen Stand zu halten.

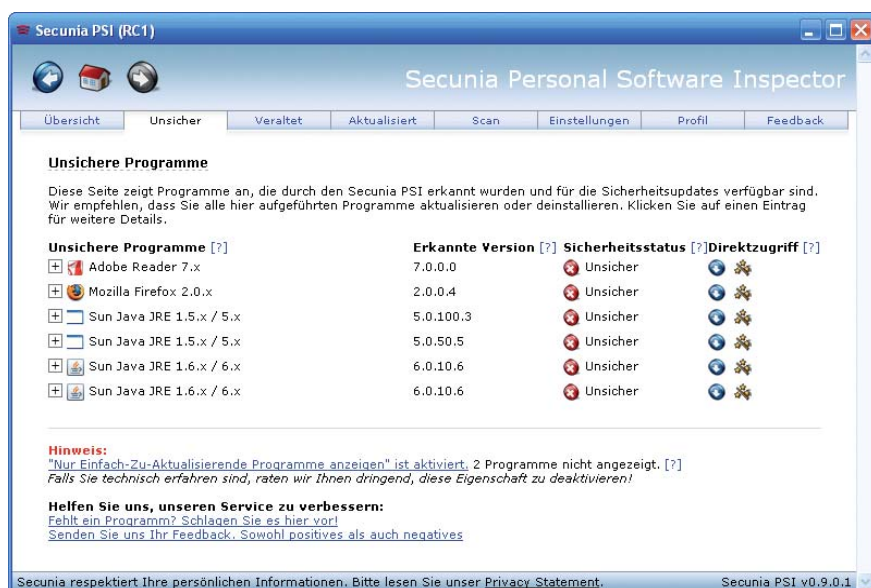


Riskante Seite: Die Screensaver auf dieser Webseite enthalten einen Trojaner (Bild E)

## Veraltete Software aktualisieren

Die Liste der Tools, die sich in den Browser integrieren und auf den meisten PCs installiert sind, ist lang. Zu den häufigsten gehören Adobe Reader, Real Player, Windows Media Player, Winamp, Flash und Java. Bei der Fülle an Tools ist es für die meisten Privatanwender nicht leicht, den Überblick darüber zu behalten, welches Programm dringend einer Aktualisierung bedarf.

**So schützen Sie sich:** Secunia PSI 0.9.0.1 (<https://psi.secunia.com>, kostenlos für Privatanwender) prüft die



Secunia PSI 0.9.0.1: Das Tool prüft installierte Anwendungen und zeigt wichtige Updates an (Bild D)

Versionsstände von Programmen, die auf Ihrem Computer installiert sind. Sie finden das Tool auf Heft-CD und -DVD in der Rubrik „Internet, Drive-by-Downloads“. Installieren Sie es und bestätigen Sie die Frage „Wollen Sie Secunia PSI (RC1) nun ausführen?“ mit „Ja“. Das Tool beginnt sofort damit, Ihren PC zu überprüfen und veraltete Software festzustellen.

Das Ergebnis zeigt Ihnen Secunia PSI mit einem kurzen Report. Klicken Sie auf „Betrachten Sie die unsicheren Programme“.

Sie sehen eine Übersicht, welche Programme aktualisiert werden sollten (Bild D).

## Gefahr durch Downloads

Eine weitere Gefahr lauert im Internet auf unvorsichtige Surfer: Webseiten mit kostenlosen Downloads, die versuchen, wie eine seriöse Seite auszusehen.

## Gefälschte Seiten

Vermeintlich harmlose Seiten bieten verseuchte Downloads an. Besonders häufig sind Webseiten, die ein fingiertes Sicherheits-Tool kostenlos anbieten, das in Wahrheit selbst ein Schädling ist. Aber auch mit kostenlosen Screensavern versuchen die Kriminellen, unvorsichtige Surfer hereinzulegen (Bild E).

**So schützen Sie sich:** Laden Sie neue Software nur von vertrauenswürdigen Quellen herunter. Bevor Sie ein neues Tool oder einen neuen Screensaver installieren, sollten Sie ihn von Virustotal ([www.virustotal.com](http://www.virustotal.com)) kostenlos prüfen lassen. Die Webseite checkt jede hochgeladene Software mit derzeit 32 unterschiedlichen Virenschaltern. Die Chance, dass dadurch ein Schädling erkannt wird, ist erheblich höher als bei einem einzelnen Virenschalter

Andreas Th. Fischer  
internet@com-magazin.de