

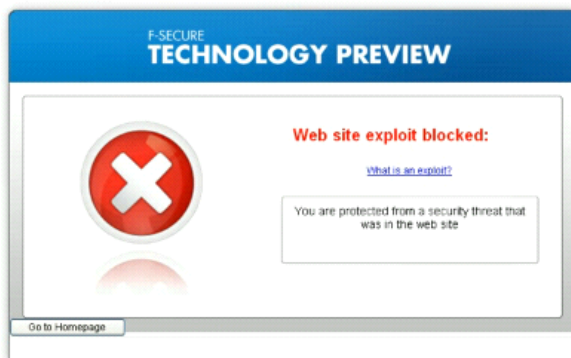
## „Zero Day“-Attacke auf ActiveX-Komponente

F-Secure meldet neue Sicherheitslücke im Internet Explorer

**München, 10. Juli 2009 – Benutzer vom Microsoft Internet Explorer surfen dieser Tage gefährlich. Die Experten von F-Secure haben eine weitere Sicherheitslücke im weltweit meistgenutzten Browser entdeckt. Dabei handelt es sich um eine Schwachstelle der Datei msvidctl.dll in der Microsoftanwendung ActiveX Video Controls. Es genügt dabei, lediglich die infizierten Internetseiten zu besuchen, per Drive-by-Download nistet sich die Malware dann auf dem Rechner ein und kann von Unbefugten per Remote-Zugriff ausgeführt werden.**

Microsoft arbeitet derzeit an einem Patch, hat aber mittlerweile bereits ein Security-Advisory zur Sicherheitslücke herausgegeben. Solange die Gefahr nicht gebannt ist, empfiehlt der Hersteller darin, ein Killbit zu setzen, das den Start der gefährdeten CLSIDs (ClassIDentifier) verhindert. F-Secure rät zwischenzeitlich eine andere Browseralternative oder den F-Secure Exploit Shield zu nutzen. Das kostenlose Tool von F-Secure bietet „Zero-Day“-Schutz gegen bösartige Exploits, die Sicherheitslücken in Browsern ausnutzen. Das Programm steht kostenlos zum [Download](#) bereit.

Die aktuelle Version des Exploit Shields ist zudem in der neuen [Internet Security Technology Preview \(ISTP\)](#) von F-Secure integriert. Die



Sicherheitsexperten nahmen den jüngsten Vorfall zum Anlass, um ISTP mit infizierten Internetseiten zu testen: Die Browsing Protection verhinderte den Exploit-Aufruf erfolgreich, noch bevor die Seite überhaupt aufgerufen werden konnte. Wie ISTP gegen „Zero Day“-Attacken vorgeht und was passiert, wenn einzelne Komponenten der Schutzmechanismen deaktiviert werden, demonstriert F-Secure in einem Video auf [YouTube](#).

### Kontakte für die Presse:

**Sandra Proske**  
F-Secure GmbH  
Zielstattstraße 44  
81379 München

Tel.: +49 89 787 467-22  
Fax: +49 89 787 467-99  
[sandra.proske@f-secure.com](mailto:sandra.proske@f-secure.com)  
[www.f-secure.de](http://www.f-secure.de)

**Berk Kutsal / Jürgen Rast**  
Trademark PR GmbH  
Goethestraße 66  
80336 München

Tel.: +49 89 444.467-461  
Fax: +49 89 444.467-479  
[f-secure@trademarkpr.eu](mailto:f-secure@trademarkpr.eu)  
[www.trademarkpr.eu](http://www.trademarkpr.eu)

# NEWS ALERT



„Zero-Day“-Attacken nutzen Schwachstellen in Programmen aus, so dass viele Softwarehersteller erst zum Zeitpunkt des Angriffs darauf aufmerksam werden. Diese Schwachstellen verhelfen Cyberkriminellen dazu, schädliche Software solange einzuschleusen, bis Softwareanbieter die jeweiligen Sicherheitslücken durch einen Patch beseitigen.

Als Drive-by-Downloads wird das unwissentliche Herunterladen von Software durch Anklicken einer Webseite bezeichnet. Die Webseite wird vom User oft auch dann noch als sicher empfunden, wenn sie längst von Cyberkriminellen gehackt wurde. Diese Art der Malwareverbreitung ist inzwischen sehr gebräuchlich, die Anzahl neuartiger Exploits steigt stetig.

## Über F-Secure

Innovation, Zuverlässigkeit und Schnelligkeit – diese drei Qualitäten haben F-Secure seit der Gründung 1988 zu einem der führenden IT-Sicherheitsanbieter weltweit gemacht. Heute vertrauen sowohl Millionen Privatanwender als auch Unternehmen auf die mehrfach ausgezeichneten Lösungen von F-Secure. Der effektive Echtzeitschutz arbeitet zuverlässig und unbemerkt im Hintergrund und macht das vernetzte Leben von Computer- und Smartphone-Nutzern sicher und einfach.

Die Lösungen von F-Secure sind als Service-Abonnement über mehr als 180 Internet Service Provider und Mobilfunkbetreiber weltweit zu beziehen. Die umfangreichen Partnerschaften machen F-Secure zum Marktführer in diesem Bereich. Seit 1999 ist das Unternehmen an der Börse in Helsinki notiert. Seitdem wächst F-Secure schneller als viele andere börsennotierte Mitbewerber.

Ständig aktuelle Informationen über die neuesten Viren finden sich im Weblog des „F-Secure Antivirus Research Teams“ unter der Internetadresse [www.f-secure.com/weblog](http://www.f-secure.com/weblog).