

## F-Secure Exploit Shield: Proaktiver Schutz gegen „Aurora“

München, 18. Januar 2010 – Microsoft steht dieser Tage vor einem massiven Problem – durch eine Sicherheitslücke (CVE 2010-0249) im Internet Explorer konnten Angreifer den manipulierten Schadcode „Aurora“ auf etliche Unternehmens-Netzwerke in China einschleusen. Dabei reichte es aus, infizierte Internetseiten zu besuchen, per Drive-by-Download gelangte die Malware dann auf die Rechner und konnte von Unbefugten per Remote-Zugriff ausgeführt werden. Weitere Vorfälle schließt F-Secure derzeit nicht aus. F-Secure Exploit Shield blockt „Project Aurora“ proaktiv im Vorfeld und verhindert den Aufruf weiterer gefährlicher Schadcodes.

Microsoft arbeitet derzeit mit Hochdruck an einem Patch. Solange die Gefahr nicht gebannt ist, raten die Sicherheitsexperten von F-Secure zwischenzeitlich eine andere Browseralternative oder den F-Secure Exploit Shield einzusetzen. Letzteres bietet „Zero-Day“-Schutz gegen bösartige Exploits, die Sicherheitslücken in Browsern ausnutzen. F-Secure Exploit Shield ist eine Komponente des Browsing-Schutz in [F-Secure Internet Security 2010](#).



Wie F-Secure Exploit Shield gegen „Zero Day“-Attacken vorgeht und was passiert, wenn einzelne Komponenten der Schutzmechanismen deaktiviert werden, demonstriert F-Secure in einem [YouTube-Video](#).

„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 Malware-Verbreitung ist inzwischen sehr gebräuchlich, die Anzahl neuartiger Exploits steigt stetig.

Detaillierte Informationen zu „Project Aurora“, weiteren Exploits und tagesaktuellen Ereignissen finden Sie im F-Secure Weblog unter <http://www.f-secure.com/weblog>.

### 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)

## 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 200 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).