

## Cyber Crime 2010: F-Secure mit aktueller Prognose

Die finnischen Sicherheitsexperten geben eine Vorhersage zur Internet-Sicherheit und die zu erwartenden Angriffe im kommenden Jahr.

**München, 16. Dezember 2009 – Kurz vor dem Jahreswechsel hat F-Secure die Internet-Bedrohungen der letzten 12 Monate analysiert und auf dieser Basis die 14 wichtigsten zu erwartenden Trends zusammengefasst.**

- 1) Windows 7 wird im kommenden Jahr Marktanteile hinzugewinnen. Windows XP wird dagegen unter 50% Marktanteil sinken. Diese Entwicklung wird die Internet-Sicherheit in wohlhabenden Ländern verbessern, in ärmeren Ländern werden sich dagegen „Malware-Ghettos“ bilden, sollten Cyber-Kriminelle ihre Anstrengungen auf die verbleibenden Installationen von Windows XP fokussieren. Ob sich die Angriffe auf Microsoft Windows allein konzentrieren oder ob im kommenden Jahr auch OSX und mobile Plattformen betroffen sein werden, bleibt abzuwarten.
- 2) Echtzeit-Funktionen von Suchmaschinen wie Google und Bing werden die Frequenz und Art der Attacken auf SEO-Tools beeinflussen.
- 3) Der 2010 FIFA World Cup wird eine große Anzahl an Trojanern, gefälschten Ticket-Shops, Spam, gehackten Online-Shops und DDoS-Angriffen hervorrufen. Schon einige Monate vor der Weltmeisterschaft im Juni wird mit SEO-Attacken zu rechnen sein. Und die südafrikanischen Mobilfunknetze werden eine Brutstätte für kriminelle Aktivitäten während der Spiele sein.
- 4) Ergebnisse von Internetrecherchen, die zu Angriffen des lokalen Rechners, der die Suche vorgenommen hat, führen, werden sich durch Techniken der Geo-Lokalisierung per IP-Adressen erhöhen. Sie werden auf Sprache, aktuelle Event News und sogar auf regionale Banken abzielen.
- 5) Auf Online-Banken zugeschnittene Trojaner werden 2010 verstärkt im Umlauf sein.
- 6) Die Angriffe auf iPhones werden zunehmen, möglich sind auch erste Angriffe auf die Betriebssysteme Android und Maemo. Denkbar ist auch eine Zero-Day-Sicherheitslücke eines groß angelegten Exploits.
- 7) Snowshoe-Spam-Angriffe werden sich erhöhen. Dabei handelt es sich um eine Technik, bei der die Spammer viele verschiedene IP-Adressen nutzen, um die Identifikation durch Spam-Filter zu erschweren, so dass zumindest ein Teil des Spams den E-Mail-Posteingang erreicht.
- 8) Ein großer DDoS-Angriff auf eine einzelne Nation ist wahrscheinlich.
- 9) Im Bereich des Möglichen scheint auch ein groß angelegter interner Angriff auf ein prominentes Ziel wie Google Wave.



### 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)

- 10) Als nahezu sicher gelten Angriffe auf soziale Netzwerke wie Facebook, Twitter, Myspace, LinkedIn, etc. Facebook hat bereits die 350 Millionen-Marke an Mitgliedern erreicht und es zeichnet sich derzeit keine Stagnation dieses Wachstums ab. Die Konzentration von Menschen und persönlichen Daten in derartigen Netzwerken ist sehr verlockend für Cyber-Kriminelle.
- 11) Da Internet-Suchmaschinen und soziale Netzwerke gemeinsam an sogenannten „social search results“ arbeiten, werden auch hier Angriffe auf die Optimierung dieser sozialen Suchmaschinen zu erwarten sein.
- 12) Da immer mehr Menschen über die Mobilfunknetze kommunizieren, wird sich die Anzahl der Zugriffe und Aktivitäten wie Banking, Spiele und Social-Networking im gleichen Maße erhöhen. Mit der wachsenden Popularität von Mobile-Banking und In-Game-Käufen wird die finanzielle Motivation stärker, solche Geschäfte auszuspionieren. Integrierte Social-Networking-Anwendungen veranlassen viele Handybesitzer, permanent online zu sein. Cyber-Kriminelle werden das Social Engineering nutzen, um diesen Trend zu ihrem Vorteil auszunutzen.
- 13) Angriffe im Zusammenhang mit Online-Spielen werden sich 2010 fortsetzen, solche Sites und Spiele sind besonders in der Asien-Pazifik-Region beliebt. Bisher werden sie allerdings noch nicht genug gesichert, das Problem wird durch die Tatsache verstärkt, dass viele Nutzer sehr jung und daher anfälliger für erfahrene Cyber-Kriminelle sind.
- 14) Datenbanken werden zunehmend gefährdet sein, da sie ein Ziel für maßgeschneiderte Angriffe sind. Cyber-Kriminelle haben mittlerweile die Mittel, gezielte Massen-Angriffe zu analysieren, zu planen und durchzuführen.



## 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).