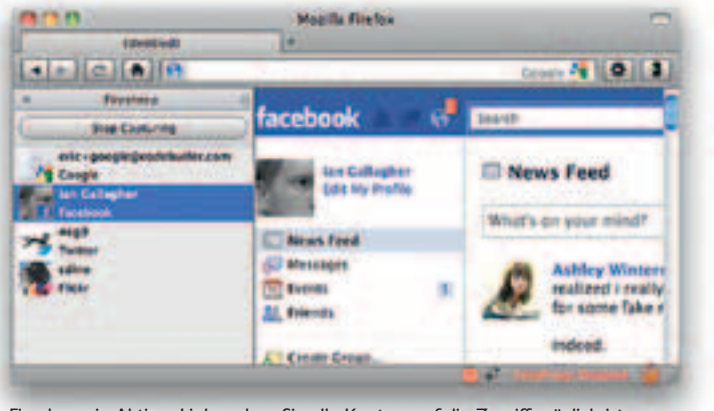
Bedrohung durch Session Hijacking

Gefährliche Sicherheitslücke: Firefox-Addon Firesheep

Seit einem Jahr können Sie mit einem Firefox-Addon namens „Firesheep“ Sitzungen von Nutzern des gleichen WLAN-Zugangs übernehmen – und so beispielsweise auf fremde Facebook-Konten zugreifen. Es gibt jedoch einfache Maßnahmen, mit denen sicheres Surfen möglich ist.

Eric Butler hatte im Oktober 2010 genug von den Entschuldigungen einiger Webseitenbetreiber, die unsichere Zugriffe zuließen. Da er wusste, wie gefährlich diese Sicherheitslücken sein können, programmierte er ein einfaches Tool namens Firesheep (1), mit dem es Menschen ohne Programmierkenntnissen möglich ist, so genanntes Session-Hijacking zu betreiben: Die meisten Webseiten verschlüsseln zwar Passwörter und andere Loginangaben mit TSL oder SSL, lassen dann aber unverschlüsselte Kommunikation über eine Session-ID zu. Diese Session-ID kann über einen ungeschützten WLAN-Zugang abgefangen werden – so dass ein Angreifer vorgeben kann, in ein bestimmtes Konto auf einer Webseite eingeloggt zu sein. Auf diese Weise hat der Angreifer letztlich auf der Webseite dieselben Rechte wie der eigentliche Benutzer.



Firesheep in Aktion: Links sehen Sie alle Konten, auf die Zugriff möglich ist.

Was Entwickler tun sollten

Butler wollte nicht ein Tool programmieren, mit dem jeder Sessions hijacken kann (obwohl er genau das getan hatte): Vielmehr wollte er Druck aufbauen, damit Entwickler sich endlich um die Sicherheit ihrer User kümmerten. Er sagte bei der Vorstellung des Tools: „Webseiten sind dafür verantwortlich, dass die Leute geschützt sind, die sich auf ihre Dienste verlassen. Sie haben diese Verantwortung zu lange ignoriert und nun müssen alle ein sicheres Internet verlangen. Ich hoffe, dass Firesheep den Usern hilft zu gewinnen.“ (2)

Hinweis

Zwei wichtige Tipps

Verbinden Sie sich immer über einen geschützten VPN-Zugang mit dem Internet. VPN-Zugänge können kostenpflichtig abonniert werden oder werden durch Firmen für ihre MitarbeiterInnen eingerichtet.

Zwingen Sie die verwendeten Browser, HTTPS zu verwenden (Firefox z. B. mit dem Addon HTTPS-Everywhere, Chrome mit KB SSL Enforcer).

Grundsätzlich geht es darum, dass Webseiten anstatt des HTTP-Protokolls das HTTPS-Protokoll verwenden, mit dem die Kommunikation zwischen User und Webseite komplett mit TSL verschlüsselt wird. Mittlerweile nutzen die meisten Webseiten (z. B. GMail) diese aufwendigere und leicht langsamere Möglichkeit; Facebook jedoch lässt weiterhin unverschlüsselte Apps zu.

Was Benutzer tun können

Die Bedrohung durch Firesheep zeigt aber gleichzeitig auf, wie unbedarft die meisten Menschen im Umgang mit sensiblen Daten sind. Die Privatsphäreneinstellungen von Facebook sind beispielsweise völlig überflüssig, wenn ganze Sitzungen übernommen werden können. Generell sollten öffentliche WLAN-Zugänge für sensible Daten nicht benutzt werden; private sollten mit WPA-Verschlüsselung gesichert sein (WEP ist unsicher) (3).

Autor ›› Links ›› Bild- und Quellennachweis

Philippe Wampfler

Ist Gymnasiallehrer und lebt in Zürich. Er bloggt über Medien, Digitales und Politik auf philippe-wampfler.com.

Link-Code	@@
Twitter-Hashtag	#wsm121-@@
Twitter-Account	kohlenklau