

Firesheep oder „Hacken“ für jedermann

Zuerst habe ich mich bei der Lektüre des aktuellen Print-Spiegels geärgert, dass jemand unwidersprochen dummes Zeug über das Internet verbreiten durfte. Der „Strafrechtler und Schufa-Ombudsmann [Winfried Hassemer](#): „Wer zwei Stunden im Internet surft, hinterlässt mehr Spuren als bei der Schufa.“ Nein. Stimmt nicht. Gar nicht wahr. Nur DAUs hinterlassen Spuren und erlauben Cookies und Javascript und [HTTP referrer](#). Aber so ist nun mal leider das Niveau der Diskussion. Es ist zum Heulen.

Unter der reißerischen Überschrift „Hacken für jedermann“ lesen wir auf S. 131 etwas über [Firesheep](#), „a Firefox extension that demonstrates HTTP session hijacking attacks“. Kein Wort darüber in Spiegel Offline, was diese Software macht, sondern nur dumpfe Panikmache: „Automatisch schnüffelt sie nach ungesicherten Verbindungen in der Umgebung, zum Beispiel um auszuspähen, der sich im Café über ein ungeschütztes WLAN bei Facebook angemeldet.“ Vermutlich kann man mit diesem „Hacker-Tool“ auch Verkehrsampeln ausstellen...

Warum sollte man jemanden warnen oder mahnen, der bei Facebook ohnehin die Hosen runterlässt und seine Daten in alle Welt verstreut (was war noch mal das Geschäftsmodell von Facebook?)... [Bruce Schneier](#) hat dazu das Nötige gesagt: „Basically, Facebook authenticates clients with cookies. If someone is using a public WiFi connection, the cookies are sniffable. Firesheep uses wincap to capture and display the authentication information for accounts it sees, allowing you to hijack the connection.(...) Protect yourself by [forcing the authentication](#) to happen over TLS. Or stop logging in to Facebook from public networks.“