

Clickjacking-Gefahr bei Chrome und Firefox

Auch Schutzfeature des Internet Explorer 8 unter Kritik

Viele Sicherheitsexperten haben derzeit das "Clickjacking", bei dem vermeintlich harmlose Klicks im Browser User ungeahnten Gefahren aussetzen, im Visir. So hat der indische Sicherheits-Forscher Aditya K Sood von SecNiche eine Lücke in Googles Browser Chrome entdeckt, die Nutzer einem Clickjacking-Risiko aussetzt. Auch die aktuelle Firefox-Version ist von dieser Schwachstelle betroffen. [Microsoft](#) wiederum war Anfang der Woche mit einem Clickjacking-Schutz für den kommenden Internet Explorer 8 (IE8) vorgeprescht, der bei Experten gemischte Gefühle auslöst. Fraglich bleibt allerdings, wie real die Bedrohung für User ist.

Verborgene Links

Beim Clickjacking werden User dazu gebracht, durch Klicks auf verborgene Links unerwünschte Aktionen zu setzen, beschreibt Sood. Der User klickt beispielweise auf einen sichtbaren Button, hinter dem auf einer für den Nutzer nicht sichtbaren Webseite ein ganz anderer Link versteckt ist. [Google](#) arbeitet Sood zufolge daran, die von ihm entdeckte Schwachstelle zu beheben. Allerdings scheint davon nicht nur Chrome betroffen. Auch die aktuelle Version von Firefox ist für Soods Variante des Clickjacking-Tricks anfällig, so Nishad Herath vom australischen Security-Consulting-Unternehmen Novologica gegenüber [ZDNet Australia](#). Sicher dagegen sind Herath zufolge der aktuelle Opera 9.63 und die neueste Vorabversion des IE8.

NoScript

Der Clickjacking-Schutz, den Microsoft mit der aktuellen Vorversion in seinen Browser integriert hat, stößt nur bedingt auf Enthusiasmus. "IE-Enthusiasten bekommen keinen magischen 'Out-of-theBox'-Schutz", meint Giorgio Maone, Entwickler des [Firefox-Plug-Ins NoScript](#) in seinem Blog. Er begrüßt zwar die Idee und kündigt auch an, Lobbying für eine kompatible Firefox-Umsetzung einer Schutzfunktion auf Basis des Tags im Header von Webseiten zu betreiben. Allerdings kritisiert er, dass es bereits eine wirksame und browserunabhängige Schutzlösung gibt - zumindest für Webmaster, die geschickt und vorsichtig genug sind, Microsofts Tag einzubauen. Denn ein bekanntes JavaScript könne ein Darstellen von Webseiten als Frame verhindern. Und vor Clickjacking-Angriffen mittels Browser-Plug-Ins böte das IE8-Feature keinen Schutz - dabei habe sich der Term "Clickjacking" ursprünglich speziell darauf bezogen.

Die Frage für Nutzer ist letztendlich, wie hoch die Bedrohung durch Clickjacking tatsächlich ist. "Soweit für uns ersichtlich, ist es noch kein großes Problem", meint Mikko Hyppönen, Security-Spezialist bei F-Secure, auf Nachfrage von presstext. Nach Google-Angaben gegenüber ZDNet Australia ist beispielsweise für die von Sood entdeckte Lücke kein Exploit in freier Wildbahn bekannt. "Clickjacking ist nur eine Maßnahme von vielen, um Nutzer auf andere Webseiten zu locken", [sagt wiederum Joe Pichlmayr, Geschäftsführer bei Ikarus Software](#), im Gespräch mit presstext. Verschiedene Tricks, die Links verstecken, habe es zwar seit einiger Zeit gegeben, doch eine wirklich große Verbreitung sei ihm nicht bekannt.

"Wenn man Scripts derart deaktiviert, funktioniert mehr als die Hälfte aller Webseiten nicht einwandfrei"

Das Plug-In NoScript wird von Firefox-Verfechtern oft als guter Schutz vor Skript-basierten Attacken inklusive Clickjacking angepriesen. Tatsächlich nutze er NoScript, wenn er beruflich gefährliche Webseiten erforscht, [so Pichlmayr](#). Für Durchschnittsuser ist NoScript jedoch nicht wirklich geeignet. "Wenn man Scripts derart deaktiviert, funktioniert mehr als die Hälfte aller Webseiten nicht einwandfrei", erklärt der Sicherheitsexperte. Gerade interaktive Inhalte des Web 2.0 leiden häufig. (pte)