

Das Like-Problem

Was Facebooks Gefällt-Mir-Buttons verraten

Jürgen Schmidt

Datenschützer warnen vor den überall auftauchenden Gefällt-Mir-Buttons von Facebook. Tatsächlich übermittelt er persönliche Daten, auch ohne dass man ihn angeklickt hat.

Immer mehr Web-Seiten bieten Ihren Lesern die Möglichkeit, durch einen Klick auf das "Gefällt mir"-Symbol ihre Facebook-Freunden auf eine interessante Seite aufmerksam zu machen. Von Spiegel Online über Bild.de bis hin zur Fan-Seite von Hannover 96 – überall begegnet man dem hochgestreckten Daumen.

Web-Sites versprechen sich mehr Sichtbarkeit und damit höhere Zugriffszahlen, die Anwender finden den Service ebenfalls praktisch. Datenschützer warnen allerdings, dass damit die Privatsphäre der Anwender gefährdet sei. Zum besseren Verständnis sei hier der technische Hintergrund der Problematik kurz erklärt.

Hier sind die eingebetteten iFrames eines Spiegel-Artikels mit einem blauen Rahmen markiert. Sie enthalten Code von Facebook beziehungsweise Twitter. Für den Like-Button bindet die Web-Seite einen sogenannten iFrame ein. Das ist eine kleine Mini-Seite innerhalb der Seite, deren Quelltext von Facebook selber stammt. Ruft man etwa eine Spiegel-Online-Seite auf, bettet diese sofort den Facebook-Frame ein – also bevor der Anwender auf "Gefällt mir" geklickt hat. Konkret führt etwa das Öffnen einer Spiegel-Online-Seite zu folgendem Aufruf des Browsers:

```
GET http://www.facebook.com/plugins/like.php?locale=de_DE&
href=http%3A%2Fwww.spiegel.de%2F...00.html... HTTP/1.1
Host: www.facebook.com
Referer: http://www.spiegel.de/.../0,1518,758141,00.html
Cookie: datr=12...f; lu=T...XQ; c_user=100...20; sct=13...539; ...
```

Dabei sendet der Browser an Facebook unter anderem als Referer die URL der gerade geöffneten Spiegel-Seite. Außerdem schickt er dem Facebook-Server auch das von ihm bereits früher gesetzte Cookie. Ist der Anwender gerade in einem anderen Fenster bei Facebook angemeldet, enthält das seine Sitzungs-ID. Damit kann Facebook diesen Aufruf der Spiegel-Seite einer konkreten Person zu ordnen.

Konkret kann Facebook also während Sie dort angemeldet sind beobachten, welche Web-Seiten Sie aufrufen, sofern diese einen solchen Like-Button oder andere Facebook-Elemente enthalten. Angesichts des Erfolgs des sozialen Netzwerks nimmt deren Zahl ständig zu. Und anders als Statistik-Server wie Google Analytics, die IVW oder auch die Server von Anzeigen-Dienstleistern, die mit anonymisierten Daten oder schlimmstenfalls IP-Adressen arbeiten, kann Facebook diese Daten direkt mit einer realen Person verknüpfen, deren Adresse und Freunde es kennt.

Auch wer nicht bei Facebook angemeldet ist, sendet Daten an deren Server. Auch wer nicht bei Facebook angemeldet ist, sendet auf Seiten mit aktiven Facebook-Elementen Daten an Facebook. So setzt Facebook bei jedem Aufruf der Web-Site ein Cookie mit einer Kennung wie E9dcTgVq3xnuDQAAFW47QTAZ, das zwei Jahre gültig ist. Da der Browser dieses Cookie bei jeder Verbindung mit einem Facebook-Server ungefragt mitschickt, könnte der Betreiber damit prinzipiell ein Profil erstellen, welche Web-Seiten der zu der Kennung gehörende Anwender aufgerufen hat. Und es wäre dann auch durchaus möglich, diese Kennung später – etwa beim späteren Anmelden bei Facebook – auch wieder einer Person zuzuordnen.

Angesichts der einschlägigen Erfahrungen, was die Daten und Privatsphäre der Mitglieder angeht, muss man auch davon ausgehen, dass die amerikanische Firma alle Daten, derer sie habhaft werden kann, auswertet und früher oder später zu Geld macht. Vergleichbare Informationen gehen übrigens auf vielen Web-Sites auch an Twitter oder Google.

Um das zu verhindern, kann man etwa in Firefox [Cookies von Drittanbietern](#) blockieren. Dann sendet der Browser bei eingebetteten Inhalten anderer Anbieter keine Cookies an den Server. Damit funktionieren allerdings außer dem Like-Button unter Umständen auch andere Site-übergreifende Funktionen nicht mehr. Um Datenschutz besorgte Web-Seiten-Betreiber müssen nicht völlig auf Facebook verzichten. Sie können statt ein iFrame einzubetten, einen einfachen Link einbauen, bei dem der Klick ein eigenes Facebook-Fenster öffnet. Dort kann Leser dann einen Kommentar erstellen und die Seite seinen Freunden empfehlen. Das ist nicht zwar ganz so komfortabel, aber es übermittelt erst dann Daten an Facebook, wenn der Anwender seine Bereitschaft dazu signalisiert hat. ([ju](#))

Auch auf heise online:

- [Facebook beschwert sich über datenschutzfreundlichen 2-Klick-Button \[2. Update\]](#)
- [2 Klicks für mehr Datenschutz](#)
- [Facebook & Co: 2 Klicks für mehr Datenschutz](#)
- [Behörden ziehen sich aus Facebook zurück](#)
- [Facebooks "Like"-Button im Visier deutscher Datenschützer](#)
- [Facebook-Spam](#)

7sep2011

<http://www.heise.de/security/artikel/Das-verraet-Facebooks-Like-Button-1230906.html>

Heise versus Facebook

Wenn der Button zwei Mal klickt

Der Computerverlag Heise unterwandert die Versuche von Facebook, an Daten von Nutzern zu kommen. Er tut es sehr geschickt - und Facebook ist machtlos.von Burkhard Schröder

BERLIN *taz* | Was ist das für eine Welt, in der Firmen "Gesichtsbuch" heißen und in der man sich darüber streitet, was wirklich geschieht, wenn man mit einem Finger ein handtellergroßes rundliches Gerät berührt? Um damit einen Pfeil auf einem Monitor so bewegen, dass dieser einem Unternehmen fernab in Kalifornien verrät, was man gestern im Internet getan hat?

Wer sich im World Wide Web bewegt, findet immer öfter kleine Facebook-Buttons. Facebook ist eine Website, die ihren Nutzern vorgaukelt, man hätte viele Freunde gefunden, wenn die ihre Kommentare zu dem abgeben, was man meint, der Welt über sich mitteilen zu müssen.

Diese Buttons simulieren und suggerieren direkte Demokratie: Die Surfer können mit einem Klick dokumentieren, ob ihnen das, was sie gerade gesehen haben, gefällt oder nicht und den Artikel an ihre virtuellen Kontakte weiterempfehlen. Facebook oder andere Firmen wie Twitter dokumentieren so das vermeintliche gesunde Surf-Empfinden.

In Wahrheit werden [Menschen ausspioniert](#), die sich zum Gefällt-mir-und-ich-empfehle-es-weiter-Klicken verführen lassen. Davon leben Datenkraken wie Facebook und Co. Den deutschen Datenschützern gefällt das nicht - sie warnen und mahnen, allerdings stehen sie angesichts des Herdentriebs des Homo sapiens auf verlorenem Posten. 750 Millionen Menschen können irgendwie nicht irren.

Mit simplem Trick

Der Computerverlag Heise stemmt sich gegen die Macht des Facebook-Faktischen und hat den [strittigen Button jetzt umgebaut](#). Wer etwas weiterempfehlen will und somit eine Nachricht an die "befreundeten" Menschen schickt, die in den so genannten "sozialen" Netzen aktiv sind, muss vorher nachdenken und der Datenspionage zustimmen.

Heise macht das mit einem simplen technischen Trick. Der ursprüngliche Facebook-Button zum Empfehlen liegt physikalisch nicht auf dem Rechner, der den Artikel anzeigt, den man soeben rezipiert hat. Er wird vielmehr von den externen Servern von Facebook eingebunden. Der Button tut nur so, als gehöre er zu der Website, die man gerade anschaut.

Facebook erhält nicht nur die Adresse - den uniform resource locator (URL) - der Website, die soeben benutzt wurde, sondern auch Informationen darüber, wer das gerade getan hat, falls diese Person bei Facebook angemeldet ist. Das "soziale" Netz kann so komplette Surf-Profile erstellen und diese mit Profit weiterverkaufen. Das ist die Geschäftsidee.

Heise jedoch hat einen eigenen Button gebaut. Der ist der Facebook-Grafik täuschend ähnlich, liegt aber auf den Heise-Rechnern. Erst bei einem zweiten Mausklick wird man mit den Facebook-Computern verbunden und setzt sich den Risiken und Nebenwirkungen aus. Dieses Vorgehen ähnelt dem [Double-Opt-In-Verfahren](#), das hierzulande vorgeschrieben ist, wenn jemand per SMS, Telefon oder E-Mail mit Werbung überschüttet wird. Die Endverbraucher müssen explizit zugestimmt haben. Wer erst "spammt" und dem "Opfer" mitteilt, es könne ja im nachhinein abbestellen, verstößt nach der aktuellen Rechtsprechung gegen das Gesetz gegen den unlauteren Wettbewerb.

Facebook gefällt nicht, dass der Heise-Verlag die Datenspionage unterläuft. Man drohte, es sei laut Platform Policies - den Geschäftsbedingungen des Unternehmens - untersagt, das strittige "Like"-Button zum Weiterempfehlen nachzuahmen. Heise hat jetzt den Button grafisch ein wenig verändert, so dass er nicht mehr mit dem "Like"-Original zu verwechseln ist. Facebook gab daraufhin zähneknirschend zu, dass diese Lösung zwar nicht ideal sei, man aber damit leben könne.

Artikel zum Thema

[Nicht mehr im Netzwerk: "Gefällt mir" gefällt nicht mehr](#)

[Weltgrößtes Online-Netzwerk: Facebook gibt ein wenig Kontrolle ab](#)

[Kommentar Facebook: Es geht aufwärts im Datenschutz](#)

[Sicherheit im sozialen Netzwerk: Facebooks Kopfgeldstrategie](#)

7sep2011

<http://www.taz.de/Heise-versus-Facebook!/77561/>