Bild: Rudolf A. Blaha

Tracker-Sperren

Firefox-Sicherheitskompendium, Teil 2

Zwei Add-ons gegen Website-übergreifendes Tracking: Decentraleyes vermeidet Anfragen an Content-Delivery-Netzwerke, indem es JavaScript-Code lokal bereitstellt. Und First Party Isolation sperrt die zu einzelnen Sites gehörenden Daten in Containern ein.

Von Mike Kuketz

JavaScript-Frameworks erleichtern Webentwicklern die Arbeit, weil sie häufig benutzte Funktionen bereitstellen. Viele Website-Betreiber binden diese Pakete daher in ihre Seiten ein. Häufig laden sie die Frameworks nicht aus ihrem eigenen Webspace, sondern über sogenannte Content Delivery Networks (CDNs) wie Google oder Cloudflare. Das spart Bandbreite und stellt sicher, dass die Frameworks schnell im Browser sind. Das Nachladen aus diesen Drittquellen übermittelt allerdings die IP-Adresse sowie weitere Informationen an die CDNs, mit denen sie Nutzer Site-übergreifend beim Surfen im Internet verfolgen können. Decentraleyes unterbindet das. Es hält aktuelle Versionen eines guten Dutzend JavaScript-Libraries lokal im Browser vor. Erkennt es den Versuch, solche extern gehosteten JavaScript-Ressourcen nachzuladen, kappt es den Verbindungsversuch und liefert das angeforderte JavaScript lokal an den Browser aus. Das beschleunigt nicht nur das Surfen, sondern schützt insbesondere die Privatsphäre. Der Kasten rechts beschreibt die Funktionsweise im Detail.

Fire and Forget

Unter dem Namen „Decentraleyes (von Thomas Rientjes)“ finden Sie das Add-on im Add-on-Verzeichnis in Firefox (siehe ct.de/yrqu). Nach der Installation zeigt es sich durch ein Icon in der Symbolleiste rechts oben neben der Adresszeile. Über eine Testseite (http://decentraleyes.org/test/) können Sie anschließend prüfen, ob das Add-on wie vorgesehen arbeitet. Als Rückmeldung sollten Sie „Decentraleyes is fully operational“ erhalten. Von Haus aus wird Decentraleyes mit den bekanntesten JavaScript-Ressourcen ausgeliefert, die häufig in Webseiten eingebunden werden – zum Beispiel jQuery oder Angular (siehe ct.de/yrqu). In zukünftigen Versio-

nen soll der Nutzer diese Ressourcen selbst erweitern können.

Ein Klick auf das Icon in der Symbolleiste bringt ein kleines Popup-Fenster zum Vorschein. Es zeigt Ihnen beim Besuch einer Webseite an, welche JavaScript-Ressourcen Decentraleyes lokal ausliefert. Über einen integrierten Zähler können Sie zudem ablesen, wie viele JavaScript-Ressourcen seit der Installation lokal bereitgestellt wurden.

Fortgeschrittene Nutzer, die das Nachladen von JavaScript von Fremdquellen über das bereits vorgestellte uBlock Origin vollständig unterbinden, müssen Ausnahmen definieren. Tun sie das nicht, wird das Nachladen von lokal bereitgestellten JavaScript-Ressourcen blockiert und der Vorteil von Decentraleyes geht verloren. Welche Ausnahmen Sie in uBlock Origin für Decentraleyes anlegen müssen, steht im Kasten „Ausnahmeregeln für uBlock Origin“.

First Party Isolation

Site-übergreifendes Tracking ist eine beliebte Technik der Werbe- und Marketingbranche, um die Webaktivität von Nutzern nachzuverfolgen. Erreicht wird dies zum Beispiel durch die Ablage von Drittanbieter-Cookies, die beim Besuch einer Webseite im Browser gespeichert werden. Werbenetzwerke nutzen diese Cookies anschließend, um den Nutzer auf unterschiedlichen Seiten wiederzuerkennen und ihm interessenbezogene Werbung einzublenden.

Anhand des fiktiven Werbenetzwerks Super-Ads möchten wir Ihnen zeigen, wie Site-übergreifendens Tracking mittels Cookies funktioniert (siehe Grafik S. 182): Beim Aufruf einer Website, zum Beispiel eines Nachrichtenportals (Website 1), wird im Browser ein neues Cookie (mit eindeutiger Kennung ID22321) von der externen Quelle „super-ads.com“ angelegt (1). Nach dem Besuch auf Website 1 surft ein Nutzer anschließend auf die Seiten eines weiteren Nachrichtenportals (Website 2), um dort ebenfalls ein paar Beiträge zu lesen.

Auch Website 2 arbeitet mit dem Werbenetzwerk Super-Ads zusammen, das nun erneut lokal im Browser ein Cookie ablegen möchte. Der Browser wird allerdings erkennen, dass bereits ein Cookie von der Quelle „super-ads.com“ existiert (2). Das Werbenetzwerk Super-Ads kann den Nutzer anschließend über die bereits vergebene Kennung ID22321 identifizieren beziehungsweise wiedererkennen (3). Mithilfe des Cookies kann Super-Ads nun feststellen (4), welche Beiträge der Nutzer auf den Nachrichtenportalen liest und kann ihm anschließend interessenbezogene Werbung einblenden. Überall dort, wo ein Site-Betreiber mit dem Werbenetzwerk zusammenarbeitet, kann es den Nutzer anhand der eindeutigen Kennung im Cookie wiedererkennen.

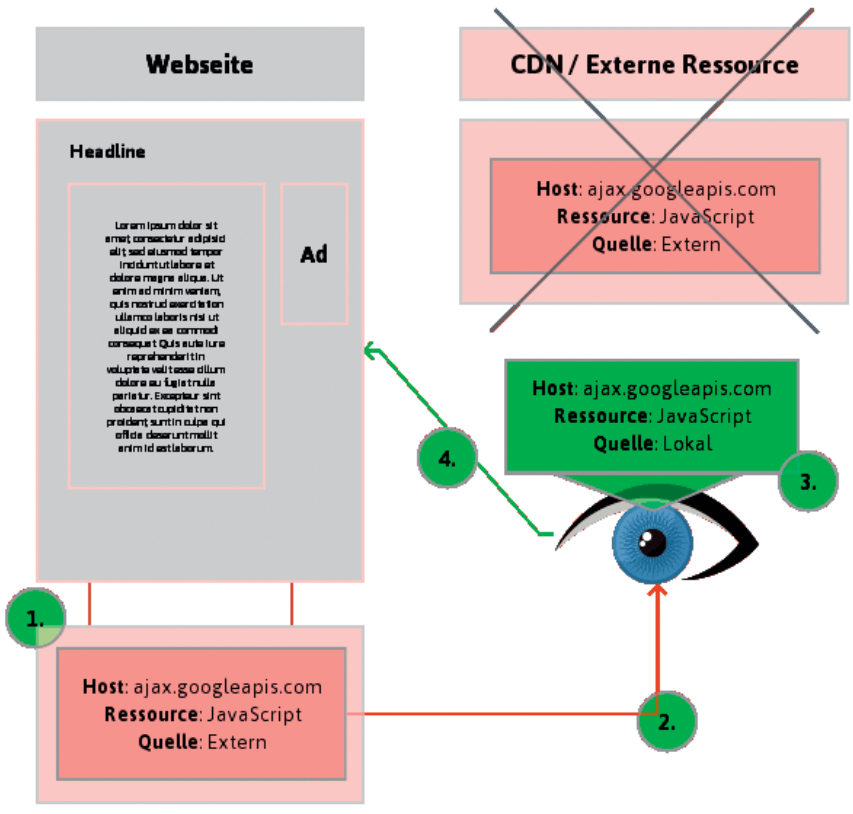
Das Firefox-Add-on First Party Isolation schützt vor diesem Site-übergreifenden Tracking mithilfe der Container-Verwaltung von Mozilla. Die Idee dahinter: Bestimmte Informationen, die der Browser beim Besuch einer Webseite ablegt, und mit denen sich der Nutzer tracken lässt, werden in einer isolierten Umgebung (Container) gespeichert. Zu diesen Surf-Daten zählen neben den Cookies auch Daten wie der Browser-Cache, TLS-Sessions und HSTS-Informationen.

Aktivieren sie First Party Isolation in Firefox, speichert der Browser die Surf-Daten in voneinander abgeschotteten Containern. Dieser Vorgang verlangsamt den Browser nicht, er ist für den Nutzer unsichtbar. Sie können sich das wie folgt vorstellen: Jede Domain, die Sie aufrufen, bekommt einen eigenen Container zugewiesen. Anschließend kann Web-Auftritt A niemals auf die Drittanbieter-Cookies von Web-Auftritt B zugreifen und umgekehrt, weil Firefox die Container für die Domains separat verwaltet. Das fiktive Werbenetzwerk Super-Ads kann Sie anschließend nicht mehr Site-übergreifend verfolgen.

Beim Aufruf von Website 1 legt es lokal im Browser erneut ein Cookie mit eindeutiger Kennung ID99234 von der externen Quelle „super-ads.com“ an (1). Nach dem Besuch auf Website 1 surft ein Nutzer anschließend auf Website 2, um dort eben-

Decentraleyes in Aktion

Beim Aufruf einer Webseite bindet der Betreiber externen JavaScript-Code (1) von der Quelle ajax.googleapis.com in den Kontext seiner Webseite ein. Firefox bearbeitet diese Anfrage und versucht eine Verbindung zur Quelle ajax.googleapis.com aufzubauen (2), um den Code von Google nachzuladen. Decentraleyes fängt diesen Verbindungsaufbau allerdings ab und stellt die JavaScript-Ressource lokal bereit (3). Im Anschluss lädt der Browser das JavaScript in den Kontext der Webseite (4) nach und führt es aus.



Ausnahmeregeln für uBlock Origin

Damit Decentraleyes und uBlock Origin reibungslos zusammenspielen, müssen Sie im Dashboard des Adblockers unter „Meine Regeln“ diese Regeln angeben:

```
* ajax.googleapis.com * noop
* ajax.aspnetcdn.com * noop
* ajax.microsoft.com * noop
* cdnjs.cloudflare.com * noop
* code.jquery.com * noop
* cdn.jsdelivr.net * noop
* yastatic.net * noop
* yandex.st * noop
* apps.bdimg.com * noop
* libs.baidu.com * noop
* lib.sinaapp.com * noop
* upcdn.b0.upaiyun.com * noop
* cdn.bootcss.com * noop
* sdn.geekzu.org * noop
* ajax.proxy.ustclug.org * noop
```

falls ein paar Beiträge zu lesen. Auch Website 2 arbeitet mit dem Werbenetzwerk Super-Ads zusammen, das nun erneut lokal im Browser ein Cookie ablegen möchte.

Aufgrund der First Party Isolation kann Super-Ads das bereits abgelegte Cookie nicht auslesen und wird für den Surf-Container der Domain von Website 2 ein neues Cookie (mit eindeutiger Kennung ID27219) anlegen (2). Versucht Super-Ads, den Nutzer seitenübergreifend wiederzuerkennen (3) (4), wird dies aufgrund der Container-Isolation nicht gelingen. Super-Ads kann zwar weiterhin feststellen, dass der Nutzer mit der Kennung ID99234 Artikel auf Website 1 liest (5). Das Unternehmen wird diese Information aber nicht mit der zweiten Kennung ID27219 (6) verknüpfen können. Aufgrund der First Party Isolation legt Firefox für jeden Surf-Container unterschiedliche Kennungen an, die das Wiedererkennen des Nutzers und damit das seitenübergreifende Tracking via Cookies verhindert. Praktisch: Die Session-Verwaltung vieler Websites funktioniert mit First Party Isolation weiterhin reibungslos.

Add-on oder about:config

Unter dem Namen „First Party Isolation (von freddyb)“ finden Sie das Add-on bei Mozilla. Nach der Installation zeigt es sich durch ein Goldfischglas-Icon in der Symbolleiste rechts oben neben der Adresszeile. Standardmäßig ist es nach der Installation aktiv – mit einem Klick auf das Icon deaktivieren Sie es. Anschließend ändert das Icon die Farbe in Orangerot.

First Party Isolation ist eine Funktion von Firefox. Um sie generell in Firefox zu aktivieren, ist die Installation des gleichnamigen Add-ons nicht zwingend erforderlich. Über about:config können Sie Parameter manuell setzen:

```
privacy.firstparty.isolate = true
```

Das Add-on hat allerdings den Vorteil, das Feature schnell ein- und ausschalten zu können. In seltenen Fällen kann dies notwendig sein, falls der Login zu einer Webseite durch First Party Isolation nicht möglich sein sollte. Dies kommt insbesondere dann vor, wenn die Webseite unterschiedliche Domains zur Anmeldung nutzt. Abhilfe schafft dann in vielen Fällen ein weiterer Parameter in der about:config, der den Schutz durch First-Party-Isolation etwas aufweicht:

```
privacy.firstparty.isolate.
  restrict_opener_access = false
```

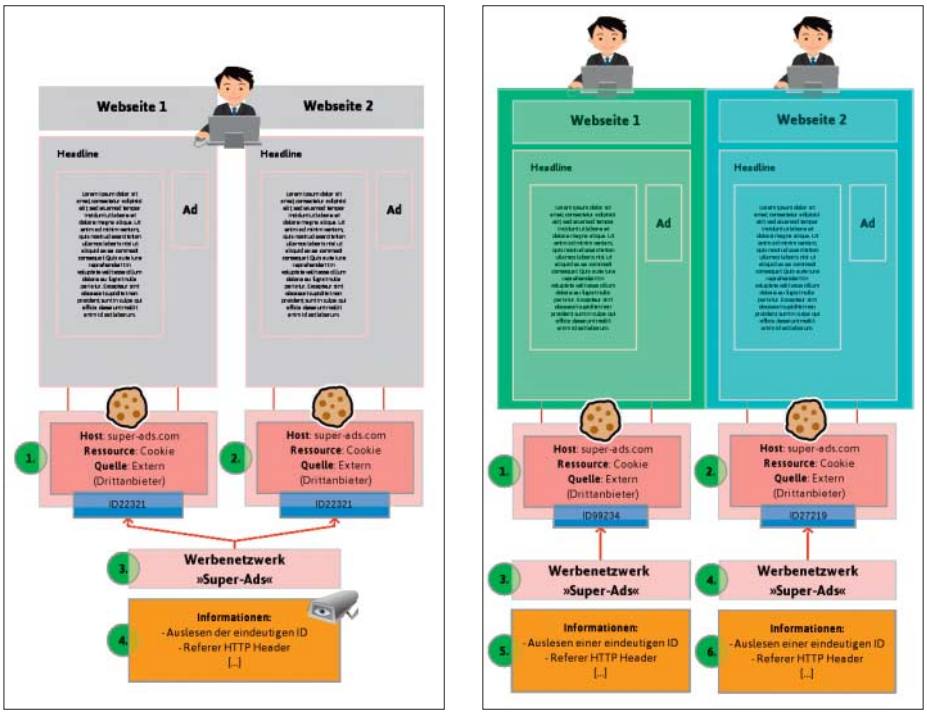
Drittanbieter-Cookies

Standardmäßig ist Firefox so eingestellt, dass der Browser Cookies von Drittanbietern akzeptiert. Trotz der Aktivierung der First Party Isolation dürfen Websites demnach auch weiterhin Cookies von Drittanbietern in ihrem Browser ablegen. Mit diesen Cookies kann man Sie dank First Party Isolation zwar nicht mehr Site-übergreifend verfolgen. Websites erkennen aber weiterhin, wann Sie eine Webseite aufrufen und welche Inhalte Sie dort ansehen.

Daher ist es generell empfehlenswert, die Annahme von Drittanbieter-Cookies zu verbieten. Öffnen Sie dazu die „Einstellungen/Datenschutz & Sicherheit“. Unter „Seitenelemente blockieren“wählen Sie „Benutzerdefiniert“ aus. Anschließend, stellen Sie die Auswahl unter „Cookies“ auf „Alle Cookies von Fremdanbietern (einige Websites funktionieren dann eventuell nicht mehr)“.

Auch wenn Sie Ihre Cookies selbst verwalten und First Party Isolation gegen das Site-übergreifende Tracking mit Cookies daher nicht benötigen, ist das Add-on nicht überflüssig: Neben dem Tracking via Cookies existieren noch weitere Techniken, gegen die das Container-Konzept schützt. Es ist daher empfehlenswert, das Add-on beziehungsweise die zugrunde liegenden Container dauerhaft aktiv zu lassen. *(jo@ct.de)* c't

Downloads und Infos: ct.de/yrqu



Sind die zu Websites gehörenden Daten in Container verpackt, lassen sich Cookies nicht mehr Site-übergreifend auslesen.