Browsen ohne Generve

Werbung blockieren, Tracking abwehren, Cookie-Hinweise loswerden

Bild: Sven Hauth

Inhalte geraten im Internet zur Nebensache, stattdessen dominieren meterlange Cookie-Dialoge, aufdringliche Reklame und ausufernden Tracking. Wer ohne solche Nervereien surfen will, muss zunächst verstehen, wie und wo seine Daten abfließen.

Von Jo Bager

Consent-Banner, auch Cookie-Banner genannt, sind die Geißel des modernen Webs. Kaum eine Webseite kann man noch „einfach so" abrufen. Stattdessen drängelt sich ein Dialogfenster in den Vordergrund, eine Art digitaler Türsteher. Und der lässt einen nur rein, wenn man sein Einverständnis gibt.

Wehe dem, der nicht auf den Button „Alles akzeptieren" klickt. Wer stattdessen genau erfahren möchte, wofür er eigentlich sein Einverständnis geben soll und die entsprechenden Einstellungen einzeln vornehmen will, der sollte Zeit mitbringen. Denn dann gilt es, ellenlange Erklärtexte durchzulesen und Dutzende oder Hunderte Einzeleinstellungen vorzunehmen.

Dabei erfüllen Consent-Banner eigentlich einen guten Zweck: Kein Website-Betreiber soll gemäß der Datenschutzgrundverordnung mit den Daten seiner Besucher einfach machen können, was er will. Stattdessen soll jeder Surfer eine informierte Entscheidung darüber treffen können, was mit seinen Daten geschieht. Und dafür muss er erklärt bekommen, was der Website-Betreiber mit seinen Daten zu tun beabsichtigt und dazu sein Einverständnis geben.

In der Praxis klicken Anwender die Consent-Banner aber meistens schnell weg und die Banner verfehlen ihr Ziel. Dabei versuchen viele dieser Consent-Banner, dem Besucher durch Tricksereien auf der Bedienoberfläche am Ende doch noch die für ihn ungünstigeren Einstellungen unterzujubeln. Die Datenschutzorganisation noyb jedenfalls sieht massenhaft Verstöße bei Cookie-Bannern, weshalb sie begonnen hat, bei Websites per Software-Roboter bessere Cookie-Dialoge anzumahnen.

Dieser Artikel erklärt die technischen Grundlagen der Cookies sowie anderer Techniken, mit den Sie getrackt werden, und welche Rolle Online-Werbung dabei spielt.

Bittere Kekse

Consent-Banner sind der Auswuchs eines schon länger währenden Kampfes gegen die Umtriebe der modernen Internet-Werbeindustrie. Um zu verstehen, worum es eigentlich geht und was dabei schiefläuft, muss man in der Vergangenheit und bei den Basics anfangen: den Cookies.

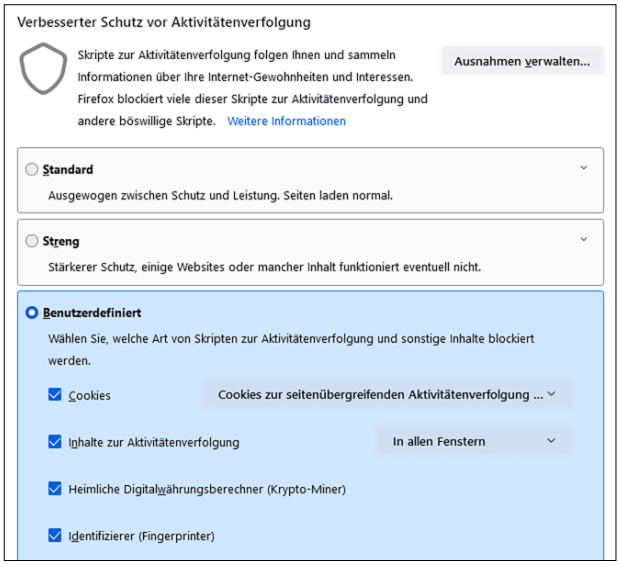
Cookies sind in den 90er-Jahren erfunden worden, um eine Schwäche des HTTP(S)-Protokolls wettzumachen, mit dem Browser Webseiten vom Server aufrufen. HTTP ist ein zustandsloses Protokoll. Das heißt, der Web-Server bearbeitet jede HTTP-Abfrage unabhängig von den vorhergehenden. So kann sich aber zum Beispiel ein Webshop nicht merken, welcher Kunde welche Artikel in den Warenkorb legt.

Cookies ergänzen diese Möglichkeit. Mit einem bestimmten HTTP-Header veranlasst der Webserver den Browser, einen Identifier zu speichern, der mit der Website assoziiert ist: das Cookie. Ruft der Browser eine weitere Seite von dem Server ab, der ein Cookie gesetzt hat, liefert er es mit. Damit kann der Server den Benutzer – genauer gesagt seinen Browser – wiedererkennen und den Seitenabruf mit früheren in Verbindung bringen.

Es gibt neben dem Warenkorb viele weitere nützliche Anwendungsfälle für Cookies. So können sich Webdienste damit merken, dass sich ein bestimmter Nutzer eingeloggt hat oder welche Einstellungen er bevorzugt. Stammt das Cookie von der Website, die man gerade besucht, spricht man von First-Party-Cookies. Problematisch sind erst die sogenannten Third-Party-Cookies, die man sich durch eingebettete Inhalte von Drittanbietern einhandelt.

Viele Webseiten enthalten zum Beispiel eingebettete YouTube-Videos oder Tweets. Betreiber großer Websites lagern Bilder und andere Mediendateien oft in sogenannten Content-Delivery-Netzwerken von Drittanbietern aus, die sich auf die schnelle Auslieferung solcher Inhalte spezialisiert haben. Viele Sites betten zudem Werbung von externen Anbietern in ihre Seiten ein. Auch Unternehmen, die Inhalte in Webseiten einbetten, können dort Cookies setzen.

Für solche Third-Party-Cookies gibt es ebenso viele legitime Anwendungen. So können Content-Delivery-Netzwerke mithilfe von Cookies ihr Load Balancing besser austarieren, was letztlich zu schneller ladenden Sites für den Surfer führt. Und mit einem Analytics-Dienst wie Google Analytics kann der Website-Betreiber



Browser, wie hier Firefox, blockieren zunehmend auch Tracking-Skripte.

die Datenströme auf seiner Site untersuchen und sie damit für jeden Besucher besser gestalten. Allerdings erfährt Google Analytics zu diesem Zweck jeden einzelnen Seitenabruf, was wiederum zulasten der Privatsphäre geht.

Ganz zuungunsten der Benutzer hat sich die Nutzung von Cookies auf dem Werbemarkt entwickelt, der ja eigentlich auch ein legitimes Mittel bietet, um Websites zu refinanzieren. Doch die Online-Werbebranche giert nach immer mehr Daten der Surfer.

Das hat damit zu tun, dass ein immer größerer Teil der Online-Werbung über Echtzeitmarktplätze des sogenannten Programmatic Advertising ausgeliefert wird. Dabei sollen Nutzer mit einem passenden Werbeprofil angesprochen werden und so nur Reklame zu Gesicht bekommen, die sie wahrscheinlich interessiert. Werbetreibende werten dazu mithilfe von Cookies aus, auf welchen Webseiten sich Nutzer welche Inhalte ansehen.

Dabei kommt großen Werbediensten zugute, dass sie regelrechte Netzwerke betreiben, die auf vielen Websites Werbung ausliefern. Mit ihren Cookies können sie Surfer daher Klick für Klick von Site zu Site verfolgen. Website-Betreiber blenden nicht selten Werbung mehrerer Werbenetze ein, liefern also die Daten ihrer Besucher gleich an mehrere Weiterverarbeiter.

Mit der Verarbeitung der so gewonnenen Informationen verdient eine riesige Marketing- und Adtech-Industrie ihr Geld. An der Weiterverarbeitung der Daten, die beim Abruf einer einzelnen Webseite anfallen, sind oft Dutzende Unternehmen beteiligt. Adtech-Anbieter versuchen aus den Daten Rückschlüsse über Alter, Geschlecht, Einkommenssituation, Hobbies und vieles mehr zu ziehen, um im Rahmen des „Predictive Behavioral Advertising“ jedem Surfer maßgeschneiderte Werbung präsentieren zu können [1].

Gar nicht super, Cookie!

Nicht nur HTTP-Cookies lassen sich dazu benutzen, um Benutzer bei ihren Streifzügen im Web zu tracken. So gut wie jede Technik, mit der Websites im Browser Inhalte speichern, hat das Potenzial dazu, Surfer wiedererkennbar zu machen. Man spricht dann auch von Supercookies. Mozilla zählt in seinem Blog ein knappes Dutzend Cache-Speicher auf, die dafür infrage kommen, zum Beispiel den Bilder- oder den Font-Cache.

In einer Anfang 2021 veröffentlichten Studie haben Forscher demonstriert, wie man sogar Favicons nutzen kann, um Browser zu identifizieren – die kleinen Logos der Websites, die in der Tab-Leiste und im Bookmark Manager angezeigt werden (siehe ct.de/yfxe). Das funktionierte selbst bei aktivierten Anti-Tracking-Maßnahmen, Inkognito-Modus und dem gezielten Löschen des Surf-Verlaufs.

Im Zweifelsfall muss man davon ausgehen, dass solche Methoden nicht lange theoretische Szenarien bleiben, sondern dass findige Werbeunternehmen sie ausnutzen, wenn die Browser ihnen die Möglichkeit dazu bieten. Der Hacker Samy Kamkar hat gezeigt, wie sich aus verschiedenen Speichertechniken auch ein sehr schwer zu löschendes Cookie bauen lässt: Sein „Evercookie“ nutzt mehrere Speichertechniken des Browsers. Löscht der Benutzer einzelne Elemente des Evercookies, stellt es diese aus den anderen wieder her (siehe ct.de/yfxe).

Verräterische Fingerabdrücke

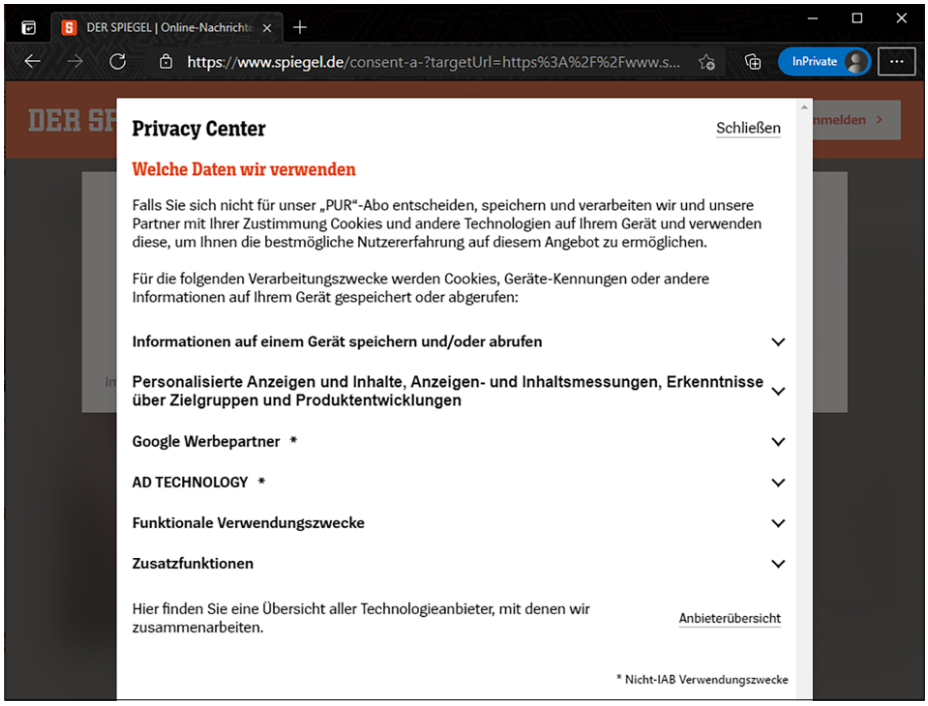
Kaum zwei PCs, kaum zwei Browser sind identisch konfiguriert. Werber machen sich das zunutze, um Surfer wiederzuerkennen, ohne einen Identifier speichern zu müssen. Der eindeutige virtuelle Fingerabdruck des Browsers genügt. Diese Technik nennt sich daher auch Browser Fingerprinting.

Schon beim Seitenabruf übermittelt jeder Browser Informationen, beispielsweise die eigene Versionsnummer, die Bildschirmauflösung, das Betriebssystem, installierte Plug-ins und Schriften. Daraus ergibt sich bereits ein Bild des Systems, auf dem der Browser läuft. Mit eingebettetem JavaScript lässt sich das beliebig verfeinern.

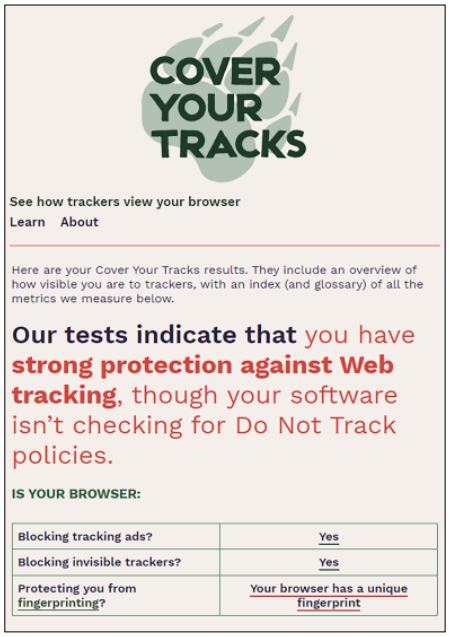
Besonders effektiv ist das sogenannte Canvas Fingerprinting. Unsichtbar für den Anwender lässt ein Skript den Browser Bilder oder Texte rendern. Diese sind so gestaltet, dass sich von Browser zu Browser kleine, messbare und eindeutig zuzuordnende Unterschiede im Layout ergeben.

Mittlerweile hat die Industrie Dutzende Techniken und Programmierschnittstellen gefunden, mit denen sich eindeutige Rückschlüsse auf den Browser ziehen lassen. Nach den Angaben des Anbieters FingerprintJS.com, der das Fingerprinting als Dienstleistung anbietet, eignet sich zum Beispiel das Web Audio API hervorragend dafür.

FingerprintJS.com sagt über sich selbst, dass es einzelne Browser mit einer Trefferquote von 99,5 Prozent wiedererkennen kann. Wenn Sie selbst herausfinden möchten, wie eindeutig der Fingerabdruck Ihres Browsers ist, finden Sie dazu unter amiunique.org und coveryourtracks.eff.org zwei Tests.



Eigentlich verfolgen Consent Banner ein hehres Ziel, in der Praxis nerven sie meist aber nur.



Wie eindeutig ist Ihr Browser wiedererkennbar? Bei Online-Tests wie hier „Cover your Tracks" können Sie das ausprobieren.

In einer Untersuchung der weltweit meistbesuchten 100.000 Sites aus dem Jahr 2020 haben Forscher zwar nur auf jeder zehnten Website Fingerprinting-Skripte gefunden. Die Technik ist laut der Studie aber umso verbreiteter, je beliebter eine Website ist. Unter den Top 1000 der Websites betrug der Anteil der Fingerprinter mehr als 30 Prozent.

Virtuelle Paravente

Auch wenn sich die Trackingfirmen immer neue Tricks einfallen lassen, sollten Sie nicht vor der Datengier der Konzerne kapitulieren: Browser haben verschiedene Schalthebel, mit denen Sie der Datensammelei einen Riegel vorschieben können. Für das Management von Cookies zum Beispiel gibt es schon seit langem Einstellungsmöglichkeiten. Sie können zum Beispiel Third-Party-Cookies pauschal blockieren lassen.

Aber das Ende der Third-Party-Cookies ist ohnehin besiegelt. Google hat angekündigt, aus dem Geschäft auszusteigen. Das Unternehmen will auch keine anderen Identifikationslösungen nutzen, die dazu genutzt werden können, einzelne Nutzer zu tracken. Wenn also selbst der Werbekonzern Google das Tracking mit Cookies einstellt, kann man davon ausgehen, dass diese demnächst allenfalls eine untergeordnete Rolle spielen werden.

Viel Ungemach können Sie zudem blockieren, wenn Sie JavaScript deaktivieren: Sowohl zum Setzen und Auslesen von Browserspeicher als auch für das Fingerprinting müssen Skripte laufen. Deaktiviert man JavaScript allerdings pauschal, funktionieren viele Sites nicht mehr richtig.

Gezielter lassen sich Skripte mit Werbe- und Inhalteblockern wie den Browsererweiterungen uBlock Origin und uMatrix aushebeln, die zum Beispiel Inhalte nur von bekannten Tracking-Domains ausfiltern. Browser übernehmen zunehmend solche Funktion zunehmend selbst.

Erst seit relativ kurzer Zeit setzen Browser zudem Containerisierung ein, um Tracking zu erschweren: Inhalte werden jeweils nur noch im Kontext der zugehörigen Domain gespeichert, und zwar auch die Inhalte von Partnern, etwa Werbetreibenden. Die können so zwar immer noch ihre Cookies setzen oder andere Dateien speichern. Die Sites können aber nicht mehr aus dem Kontext einer anderen Website darauf zugreifen und die Surfer also nicht mehr auf ihren Streifzügen verfolgen. Um es Werbetreibenden zu erschweren, eindeutige Fingerabdrücke zu erzeugen, setzen Browser zudem auf Verschleierung (obfuscation). Dabei geben sie nicht mehr von sich aus so viele Informationen über sich preis.

Doch wie gut schützt welcher Browser Ihre Privatsphäre? Im Beitrag ab Seite 18 klopfen wir Brave, Chrome, Edge, Firefox Opera, Safari und Vivaldi auf ihre Datenschutzfunktionen hin ab. Der Artikel ab Seite 22 erklärt, wie Sie Firefox so aufrüsten, dass er Ihre Privatsphäre bestmöglich schützt und gleichzeitig Nervereien wie Cookie-Banner unterdrückt.

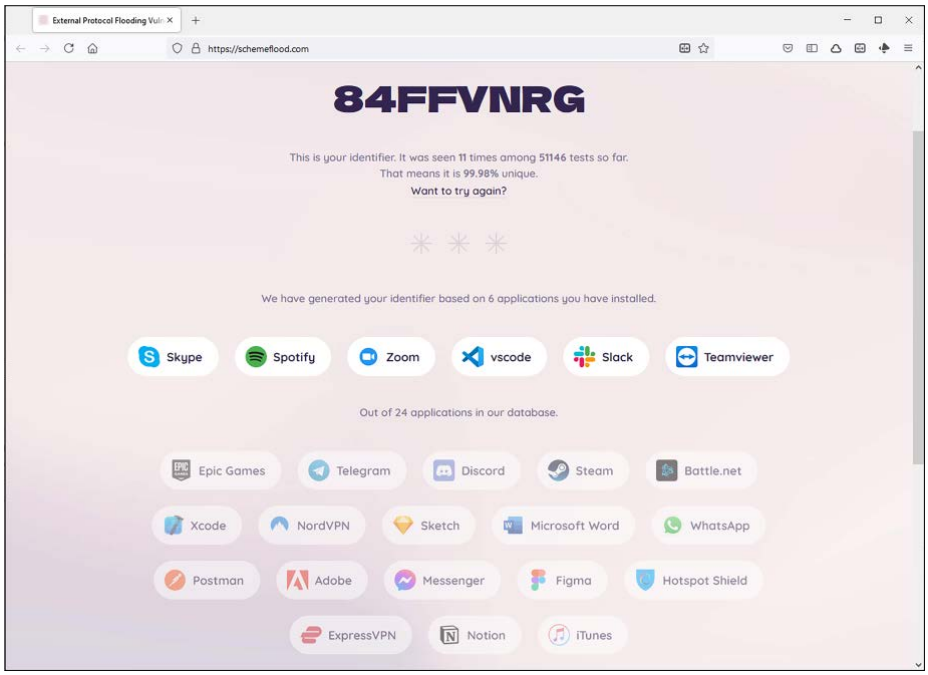
Das Ende der Third-Party-Cookies – die sogenannte Cookiecalypse – und Browser, die immer besser die Privatsphäre schützen, werden aber nicht verhindern, dass die Werbebranche Surfer auch in Zukunft trackt. Das Geschäftsmodell viel zu vieler Unternehmen hat mit der Aufbereitung von Nutzerdaten zu tun.

Also rüsten auch die Werbeunternehmen auf. An Stelle der Cookies werden also vermehrt andere Techniken treten, seien es andere Identifier, Fingerprinting – oder völlig neue Tricks. So herrscht derzeit ein heftiges Gezerre darum, welche Standards an Stelle der Cookies treten. Im Artikel ab Seite 28 geben wir einen Überblick. *(jo@ct.de)* c't

Literatur

[1] Torsten Kleinz: Gezerre um die Zukunft der Online-Werbung, Googles Cookie-Ausstieg: Streit um „Tracking Light", c't 8/2021, S. 28

Weiterführende Informationen:
ct.de/yfxe



schemeflood.com versucht einen Fingerabdruck anhand der installierten Anwendungen zu ermitteln.