Mein Browser – was verrät die Plaudertasche über mich?

Ein Skript zum Vortrag der studentischen Gruppe

der technischen Hochschule Lübeck (THL)

Mitglieder
Antje Hänzelmann (Stud. B.Sc. Medieninformatik - online)
Patrycja Magdalena Kupiec (Stud. B.Sc. IT Sicherheit – online)
Michael Georg Schmidt (Stud. B.Sc. IT Sicherheit - online)

Inhaltsverzeichnis

Vorab....3
1. Tests zum Datenschutz....3
2. Brave / Chrome / Edge / Firefox / Opera / Safari / Vivaldi....4
3. Browser Fingerprinting....4
4. Browser....5
    4.1 Brave....5
    4.3 Chrome....6
    4.4 Edge....6
    4.5 Firefox....7
    4.6 Opera....7
    4.7 Safari....8
    4.8 Vivaldi....8
5. Fazit....9
Quellen....10

Vorab

Dieses Skript versucht die wichtigsten Dinge im Zusammenhang mit der Nutzung von Browsern zu klären und vor allem zu erklären. Es ist in enger Anlehnung an die Artikelserie *Surfen ohne Nerverei und Tracking* aus der Zeitschrift *c‘t 14/21* entstanden.

Ergänzend sind am Ende unter der Überschrift *Quellen* Links und Hinweise zu deutlich weiterführenden Informationen beigefügt. Sollten dennoch Fragen offen bleiben oder sich gar neue Fragen ergeben, stehen wir Ihnen gerne jederzeit per

per *E-Mail* *mail@its-us.info*

oder via Threema

Patrycja Kupiec
Michael Georg Schmidt WYH86UFA

zur Verfügung.

wir hoffen, Ihnen hat der Vortrag gefallen und das Skript hilft Ihnen weiter.

Beste Grüße
Ihr ITS Us. Team
Wir erklären IT Sicherheit einfach

1. Tests zum Datenschutz

Browser verraten den Websitebetreibern von sich aus eine Menge an Daten. Welche das sind, können Sie mit Hilfe der folgenden Websites selber ausprobieren – und sich wundern, wie viele Daten von Ihnen in die Welt gehen.

Die *EFF (Electronic Frontier Foundation)* ist eine amerikanische Bürgerrechtsorganisation, die eine Website zur Verfügung stellt, die bewertet, wie *einzigartig* der Browsers von Nutzer:innen ist. Die Site trägt den Namen *amiunique.org*. Sie finden sie hier https://amiunique.org/

Auch von der EFF stammt die Seite *coveryourtracks*. Hier sehen Sie, wer Sie womit verfolgt. Testen können Sie das hier https://coveryourtracks.eff.org/results?&aat=1&fpi_whorls=%7B%22v2%22%3A%7B%22plugins%22%3A%22permission+denied%22%2C%22hardware_concurrency%22%3A8%2C%22audio%22%3A%2235.73833402246237%22%2C%22canvas_hash_v2%22%3A%22f139fb61b2b20249d81082f9012141dc%22%2C%22webgl_hash_v2%22%3A%2233dbdb28a8e5050332bc8f7473462c56%22%7D%7D.

Mit Hilfe der Site *browserleaks.com* können Sie hier https://browserleaks.com/ nachvollziehen, was Ihr Browser alles ausplaudert.

Gegen die Werkzeuge von *fingerprintJS*, die einen Fingerprint erstellen, ist noch kein Kraut gewachsen. Sie können es hier https://fingerprintjs.com/ selbst ausprobieren.

2. Brave / Chrome / Edge / Firefox / Opera / Safari / Vivaldi

Welchen Einfluss Cookies auf unsere Privatsphäre haben hängt auch vom benutzten Browser ab, denn die gehen ganz unterschiedlich mit Cookies und Datenschutz um.

Die Websitebetreiber und Werbetreibenden setzen vielfältige Methoden ein, um die Daten der Nutzer:innen zu erlangen. Ein Erfolg versprechendes Verfahren ist dabei das

3. Browser Fingerprinting

Dabei werten die Websites neben gesetzten Cookies auch Daten aus, wie die Konfiguration des Browsers, des genutzten Systems, installierter Programme, installierter Schriften und vielem mehr. Wer darüber mehr erfahren möchte, kann selbst Tests dazu durchführen.

Die *EFF* bietet dafür Websites an.
Die Site amiunique zeigt, wie *einzigartig* das eigene System ist. Während wir als Menschen stolz darauf sind, wenn wir einzigartig sind, ist dies bei Browsern weniger gut, denn so ist es deutlich leichter, uns wiederzuerkennen.
Zusätzlich bietet die EFF eine Website an, die anzeigt, mit welchen Daten wir verfolgt werden. Diese Site heißt *coveryourtracks.*
Bereits vier der hier aufgeführten *(Meta)Daten* reichen nachweislich aus, um Sie zu identifizieren. Wissenschaftlich nachgewiesen haben das *Yves-Alexandre de Monjoye et all*. In den *Quellen* finden sie noch einige weitere Hinweise auf Informationen zu Metadaten.

Vor allem lästig sind *Consent Banner*, die fragen die Nutzer:innen beim Aufruf einer Website immer, ob diese mit diversen Cookies einverstanden sind. Man sollte sich die Mühe machen, die *Optionen* oder *Einstellungen* anzusehen, denn hier kann man einiges an Spionageteilchen abschalten.

Eher unerwartet können auch *Favicons* zu den Bösewichten gehören, die Daten sammeln. Favicons sind die kleinen Bildchen, die Sie links neben der Adresse der aktuell aufgerufenen Website sehen. Sie können Daten speichern, obwohl *AntiTracking Maßnahmen* ergriffen wurden, der *Browserverlauf* gelöscht oder der *Incognito Mode* aktiviert ist. Dies gilt zum Glück nur für Ausnahmen und ist nicht der Regelfall.

Um einen *Browser Fingerprint* zu erzeugen sind *Audio APIs* sehr gut geeignet, um Nutzer zu identifizieren. Hierbei handelt es sich um Schnittstellen des Browsers für Audioausgaben.

Neben dem „normalen Browser Fingerprinting“ unterscheidet man auch zwischen *Canvas Fingerprinting* und dem Fingerprint der Firma *FingerprintJS.*

Canvas Fingerprints sind Codeschnipsel, die Bilder und Text für den Nutzer unsichtbar rendern, also so etwas ähnliches tun, wie eine Formatierung vorzunehmen. Je nachdem wie sich die betroffenen Inhalte verhalten, kann der Anwender feststellen, welchen Browser die Nutzer:innen einsetzen.

FingerprintJS ist eine Firma, die eine Schnittstelle für Websites anbietet, die mit *Java Script* Code herausfindet, um welchen Browser es sich handelt, den die Nutzer:innen gerade benutzen. Dies erkennt die Software mit einer Genauigkeit von 99,5 %, so der Hersteller.

4. Browser

Ein Browser ist das Programm mit dem Sie ins Internet gehen. *Brave* ist hier der Musterknabe, während *Edge (von Microsoft)* ein Browser ist, dem man lieber aus dem Weg gehen sollte, wenngleich er auf *Chromium*, also dem Unterbau von Googles Chrome basiert.

Im Einzelnen

4.1 Brave

Brave basiert auf *Chromium* und aktualisiert beim Aufruf des Browsers die Daten für Add-Blocker und unsichere Seiten. Dafür ruft er die Daten von *EasyList / Easy Privacy* und *uBlockOrigin* ab. Weitere Listen mit entsprechenden Daten können Nutzer:innen nachträglich selbst ergänzen. Zusätzlich überträgt Brave jedoch auch Diagnosedaten an die URL *b3a.brave.com*. Diese Daten sind vollständig anonymisiert. Sobald es mehr als vier Daten sind, die Brave hier überträgt, ist jedoch eine Deanonymisierung möglich. Sie können und sollten, diese Funktion daher deaktivieren.

Suchanfragen können über *DoH (DNS over HTTPS)* gesandt werden. Somit senden die Nutzer:innen ihre Anfragen verschlüsselt und es kann nicht jeder mitlesen, welche Anfragen die Nutzer:innen stellen.

Als *Standardsuchmaschine* ist *DuckDuckGo* voreingestellt. Dabei handelt es sich zwar um eine amerikanische Suchmaschine, jedoch verspricht sie, keine Daten der Nutzer zu speichern und keine Profile anzulegen. Allgemein gilt DuckDuckGo als Suchmaschine die vertrauenswürdig ist.

Brave ist Werbung gegenüber nicht ganz abgeneigt, wenn die Nutzer:innen damit einverstanden sind. Dieser zurückhaltenden Werbung mit dem Namen *Brave Rewards* müssen die Nutzer:innen explizit zustimmen. Der Sinn dahinter ist, dass Brave mit dieser Werbung Geld verdient. Die Nutzer:innen haben auch etwas davon, denn wenn sie zustimmen, sammelt Brave für sie Kryptogeld in einem integrierten *Wallet (digitale Geldbörse)*. Die „Einnahmen“ zahlt Brave monatlich in die Wallet ein.

Um zu überprüfen, ob Werbung am Brave Rewards Programm teilnimmt, sendet Brave an sein Mutterhaus gelegentlich einen vierstelligen Hash.

Für *privates Surfen* bietet Brave als einziger Browser einen integrierten *TOR Client* an, der es möglich macht das *Onion-Netzwerk* ohne weitere Installationen zu nutzen. TOR ist ein Browser, der ein weitestgehend anonymes Surfen ermöglicht (TOR = Tor Onion Router).

Bereits im Auslieferungszustand hat Brave eine Konfiguration, die gut vor Datenmissbrauch schützt. Sogar vor dem *Canvas Fingerprinting* bietet Brave einen Schutz. Gegen *FingerPrintJS* ist leider auch Brave machtlos.

4.3 Chrome

Chrome ist der Browser von *Google* dem *Chromium* zu Grunde liegt. Chrome ist nicht schlecht, aber sendet jede Eingabe in *Echtzeit* an Google, um den Nutzer:innen Vorschläge für ihre Suche zu unterbreiten. Das ist nicht so schön, weil Google damit umgehend die Eingaben speichert und dem Profil der Nutzer:innen zuordnen kann, auch wenn eine Eingabe wieder gelöscht wurde.

Chrome lädt Daten für *Add-Blocker* und *maliziöse Websites* nach. Im Browser ist *DoH* konfigurierbar. Die Funktion *Do not Track* ist ebenfalls aktivierbar, jedoch gilt dieses Projekt als gescheitert und wirkungslos.

Die *Standardsuchmaschine* von Chrome ist *Google*, das als Datenkrake bekannt ist.

4.4 Edge

Edge ist der schlechteste Kandidat dieser Reihe. Der Browser stammt von *Microsoft*. Mit dem *Internet Explorer* und eine ganze Zeit lang auch mit Edge hat Microsoft einen selbst entwickelten Browser betrieben. Seit einiger Zeit jedoch basiert Edge auf *Chromium* und ist damit performanter und weniger störanfällig als es die alten Versionen waren. Zusätzlich hat Edge damit die Möglichkeit alle Add-ons von Chrome zu nutzen.

Die *Standardsuchmaschine* von Edge ist *Bing*, die Microsoft eigene Suchmaschine. Bing überträgt in Echtzeit alle Eingaben an Microsoft. Das führt zur Vervollständigung von Profilen. Bedauerlich ist, dass diese Funktion sogar im privaten Modus, der sich hier *inPrivate* nennt, aktiv ist. Sie ist nicht abschaltbar. Nicht nur bei den Eingaben ist Microsoft so neugierig, sondern auch bei den aufgerufenen URLs. Das heißt, dass Microsoft ganz genau wissen will, welche Websites sich die Nutzer:innen angesehen haben.

Genauso ist die Funktion die *erforderliche Diagnosedaten* an Microsoft sendet, nicht abschaltbar. Hier stellt sich die Frage, weshalb Edge welche Diagnosedaten als erforderlich klassifiziert. Einige andere Browser nutzen ebenfalls *Chromium* als Basis und kommen ohne den Versand dieser Diagnosedaten zurecht.

Um dem *Tracking* zu entgehen müssen die Nutzer:innen den *strengen Modus* aktivieren, denn bei allen anderen Einstellungen ist diese Funktion recht

wirkungslos. Das hat System, denn Microsoft selbst überlädt neu aufgerufene Browser Tabs mit Werbung und Trackern der Anbieter *Tabula, Zemanta, ScorecardResearch.*

Erst mit Add-ons wie *Customize your new Tab Page (Neuer Tab – Seite personalisieren)* und *Tabliss* ist es möglich, dieser Unsitte Einhalt zu gebieten.

4.5 Firefox

Auch *Firefox* ist beim Start nicht stumm. Er nimmt Kontakt zur Adresse *detectportal.firefox.com/success.txt* auf. Diese Aktion kann man dem Browser allerdings leicht verzeihen, denn er überprüft auf diese Weise lediglich, ob eine Verbindung zum Internet besteht. Auch zu Google unterhält Firefox Beziehungen. Hier lädt er Bibliotheken von *Widevine* herunter. Widevine ist ein Tool, um angebotene Inhalte zu schützen. Insofern ist dieses Vorhaben durchaus lobenswert. Zusätzlich kontaktiert Firefox die Site *openh264.org*. Hier lädt Firefox Videocodecs herunter um möglichst viele Videoformate darstellen zu können. Nachteil hieran ist, dass Websitebetreiber dies zum *Browser Fingerprinting* missbrauchen können.

Um aufgerufene Seiten auf mögliche Schädlichkeit überprüfen zu können, lädt Firefox auch entsprechende Dateien von Google herunter. Die Überprüfung findet offline statt. Somit ist Google von der Information, welche Sites die Nuterz:innen aufgerufen haben, abgeschnitten.

Firefox bietet als einer von zwei Browsern (Opera hat dies auch) ein eingebautes *VPN (Virtual Private Network)* an. Da der gesamte Datenverkehr der Nutzer:innen über den Anbieter eines VPNs fließt, ist zwingende Voraussetzung für einen sinnvollen Einsatz dieses VPNs, dass man dem Anbieter trauen kann. Firefox bedient sich hierfür des Anbieters *Mullvad VPN* – https://mullvad.net/de/. Mullvad bietet seine VPN-Dienste zu günstigeren Preisen als Firefox an.

4.6 Opera

Opera scheint für und vermutlich von Werbung zu leben. Neben vielfältigen Links zu Onlineshops, die auf neu aufgerufenen Tabs erscheinen, lädt der Browser heimlich im Hintergrund die Add-ons *Rich Hint Agent* – ein Add-on, das zum *Cashbackdienst Dify* gehört und den *Aliexpress Observer* nach. Letzterer gehört zum Onlinehändler Ali Express, dem chinesischen Pendant von Amazon. Amazon ist aber auch vertreten, denn Opera bringt den *Amazon Assistent* von Haus aus mit.

Die heimlich nachgeladenen Add-ons bleiben für den Nutzer unsichtbar.

Die voreingestellte *Suchmaschine* ist Google. Google erhält auch in Echtzeit sämtliche Eingaben der Nutzer:innen, um Suchvorschläge zu generieren.

Angeblich macht sich Opera Sorgen um die Sicherheit der Nutzer:innen. Daher sendet der Browser sämtliche aufgerufenen URLs an *sitecheck.opera.com*.

Damit hat Opera die Möglichkeit viele Daten für umfangreiche Nutzerprofile zu sammeln.

Zumindest gibt sich Opera noch den Schein die Nutzer zu schützen, denn es verwendet eingebaute Add Blocker mit den Listen von *EasyList* und *NoCoin*.

Positiv zu vermerken ist, dass Opera ein integriertes *VPN (Virtual Private Network)* anbietet. Im Hinblick auf die anderen Besonderheiten von Opera ist jedoch Vorsicht in Bezug auf die Qualität dieses VPNs angeraten, denn der Anbieter eines VPNs „sieht“ den gesamten Netzwerkverkehr ins Internet und zurück.

4.7 Safari

Der Apple-Browser bewegt sich im Mittelfeld. Er verfügt über einen eingebauten Trackingschutz. Besonders ist hier, dass der Trackingschutz „lernt“ und seine Ergebnisse so im Laufe der Zeit immer besser werden.

Ruft man einen neuen Tab auf, begrüßen einen Unmengen an Werbelinks, die jedoch abschaltbar sind.

Als Suchmaschine hat Safari *Google* voreingestellt. Damit ist ein großer Datenkrake gleich mit an Bord. Sämtliche Sucheingaben gehen in Echtzeit an Google, um von dort Vorschläge für die Suche zu erhalten. Gleichzeitig schickt Safari diese Anfragen auch an *api-glb-eucla.snoot.apple.com*. Somit ist auch Apple gut darüber informiert, was seine Kunden interessiert. Die Weitergabe an Apple ist abschaltbar. Ist eine alternative Suchmaschine als Standard eingerichtet, wie beispielsweise *Startpage.com* oder *DuckDuckGo.com* erhält auch Google keine zusätzlichen Profilinformationen.

4.8 Vivaldi

Vivaldi erhält auch keine Empfehlung, denn seine Voreinstellungen sind zu werbelastig. Sie sind zwar abschaltbar, aber der Trackinkgschutz enthält eine Liste mit etlichen Werbepartnern von Vivaldi, denen Tracking damit automatisch erlaubt ist.

Die Möglichkeit Domains automatisch über HTTPS (DoH) abzurufen bietet Vivaldi nicht an. Dieses Kennzeichen sollte inzwischen jedoch Standard sein.

5. Fazit

Auf Grund dieser Eigenschaften sieht die Liste für Browserempfehlungen wie folgt aus:

1. Brave
2. Firefox
3. Safari
4. Chrome
5. Vivaldi
6. Edge und Opera

Passt man Firefox mit den erwähnten Add-ons an, könnte er sogar Brave an der ersten Stelle ablösen. Welche Add-ons das sind, erklären wir in unserem Workshop *Mein Browser – wie ich die Plaudertasche zum Schweigen bringe*.

Quellen

1. Add-on Canvas Blocker – Programmerweiterung für Firefox, um Canvas Fingerprinting zu vermeiden.
   https://addons.mozilla.org/de/firefox/addon/canvasblocker/
2. Add-on Firefox Multi Account Containers – Programmerweiterung für Firefox, um Websites einzelnen Containern zuzuordnen
   https://addons.mozilla.org/de/firefox/addon/multi-account-containers/
3. Add-on I don‘t care about cookies – Programmerweiterung für Firefox, um lästige Consent Banner weitgehend automatisch zu handhaben.
   https://addons.mozilla.org/de/firefox/addon/i-dont-care-about-cookies/
4. Add-on Firefox Multi Account Containers – Programmerweiterung für Firefox, die es den Nutzer:innen möglich macht, für unterschiedliche Anwendungsbereiche wie *Privat*, *Arbeit*, *Banking* und beliebiges mehr, *Container* anzulegen, so dass die Sites sich untereinander nicht mehr „sehen“ können.
   https://addons.mozilla.org/de/firefox/addon/multi-account-containers/
5. Add-on NoScript – Programmerweiterung für Firefox, die die Ausführung von Skripten verhindert. Ausnahmen sind konfigurierbar.
   https://addons.mozilla.org/de/firefox/addon/noscript/
6. Add-on für Chrome und Edge – Tabliss – entfernt Werbung
   https://tabliss.io/
7. Add-on Temporary Containers – Programmerweiterung für Firefox, die alle Websites, die die Nutzer:innen keinem Container zugeordnet haben, in einen *vorübergehenden* Container legen. Die dort abgelegten Daten löscht das Add-on nach 15 Minuten automatisch.
   https://addons.mozilla.org/de/firefox/addon/temporary-containers/
8. Add-on uBlockOrigin – Programmerweiterung für Firefox, ein ausgefeilter Blocker für Werbung.
   https://addons.mozilla.org/de/firefox/addon/ublock-origin/
9. amiunique – Website der amerikanischen Bürgerrechtsorganistaion EFF (Electronic Frontier Foundation), um festzustellen, wie leicht man über den eigenen Browser identifizierbar ist.
   https://amiunique.org/
10. Apple – Verwalten von Cookies und Websitedaten mit Safari auf dem Mac - https://support.
    apple.com/de-de/guide/safari/sfri11471/mac
11. Browser Leaks – Website, die zeigt, welche Daten der eigene Browser automatisch überträgt.
    https://browserleaks.com/
12. Browser Fingerprinting – eine Erkllärung, was *Browser Fingerprinting* ist.
    https://browser-fingerprint.cs.fau.de/
13. Browser Fingerprinting API – eine Erklärung wie Browser Fingerprinting über Schnittstellen funktioniert.
    https://fingerprintjs.com/

14 Building a privacy – first future for web advertising – Goolge erklärt Werbeverfahren, die vermeintlich Datenschutz konform sind
https://blog.google/products/ads-commerce/2021-01-privacy-sandbox/

15 Canvas Fingerprinting – Erklärung dieser besonderen Form des Fingerprintings
https://de.wikipedia.org/wiki/Canvas_Fingerprinting

16 Chip - Cookies akzeptieren oder nicht? Das sollten Sie tun – ein Artikel zu Cookies aus der Zeitschrift *Chip*
https://praxistipps.chip.de/cookies-akzeptieren-oder-nicht-das-sollten-sie-tun_42136

17 Codingkids.de - History Check: Was sind denn Magic Cookies? - Eine Erklärung zu Magic Cookies
https://www.codingkids.de/wissen/history-check-was-bitteschoen-sind-magic-cookies

18 Cookies – RFC 6265 – RFC = Request for Comments. Der Beginn eines Versuchs, Internettechniken zu standardisiern. Inzwischen ist RFC genau das.
https://datatracker.ietf.org/doc/html/rfc6265

19 Cookiebot.com – Cookie-Checker | Ist Ihre Webseite DSGVO- und CCPA-konform? - Test für Websitebetreiber:innen, auf Datenschutzkonformität
https://www.cookiebot.com/de/cookie-checker/?gclid=EAIaIQobChMI-9X6oMz88QIVFNayCh2FqAltEAAYAyAAEgKKqvD_BwE

20 Cortina-consult.com – Was sind Cookies? - Eine Erklärung, was Cookies sind
https://cortina-consult.com/was-sind-cookies/

21 c‘t 14/21 Surfen ohne Nerverei und Tracking (Artikelserie) – Grundlage dieses Skripts
https://www.heise.de/ct/artikel/c-t-14-2021-Der-Blick-ins-Heft-mit-Surfen-ohne-Nerverei-und-Tracking-6070723.html

22 coveryourtracks – Website der EFF (Electronic Frontierfoundation), die Tracking von Websites aufzeigt
https://coveryourtracks.eff.org/results?&aat=1&fpi_whorls=%7B%22v2%22%3A%7B%22plugins%22%3A%22permission+denied%22%2C%22hardware_concurrency%22%3A8%2C%22audio%22%3A%2235.73833402246237%22%2C%22canvas_hash_v2%22%3A%22f139fb61b2b20249d81082f9012141dc%22%2C%22webgl_hash_v2%22%3A%2233dbdb28a8e5050332bc8f7473462c56%22%7D%7D.

23 de Montjoye, Y.-A., Radaelli, L., Singh, V. K. & Pentland, A.. Science . Unique in the shopping mall:On the reidentifiability ofcredit card metadata. Ausführliche Informationen zu Metadaten.
https://science.sciencemag.org/content/sci/347/6221/536.full.pdf

24 Developer.mozilla.org – Set-Cookie – Informationen für Entwickler, zum Setzen von Cookies
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie

25 Die 6 gängigen Cookie Consent Tools im Vergleich – Vergleich von Tools, die Cookies auf Websites setzen
https://www.e-recht24.de/artikel/datenschutz/12495-cookie-consent-tools.html

26 DNS over HTTPS – Erklärung wie sichere Domainanfragen funktionieren
https://de.wikipedia.org/wiki/DNS_over_HTTPS

27 External Protocol Flooding Vulnerability – Erläuterung von Angriffsmöglichkeiten
https://schemeflood.com/

28 FingerprintJS – Anbieter ausgesprochen ausgeklügelten Fingerprintings
https://fingerprintjs.com/demo/

29 Fingerprinting the Fingerprinters: Learning to detect Browser Fingerprinting Behaviors – ein Versuch den Fingerprintern auf die Spur zu kommen
https://arxiv.org/abs/2008.04480

30 Firefox 85 cracks down on supercookies – Firefox wehrt sich ab Version 85 gegen Supercookies
https://blog.mozilla.org/security/2021/01/26/supercookie-protections/

31 Firefox 85 knackt Supercookies – Firefox wehrt sich ab Version 85 gegen Supercookies
https://blog.mozilla.org/press-de/2021/01/26/firefox-85-knackt-supercookies/

32 Firefox 86 introduces total cookie protection – Firefox 86 führt den “totalen” Cookieschutz ein
https://blog.mozilla.org/security/2021/02/23/total-cookie-protection/

33 Firefox Download – hier kann Firefox herunter geladen werden
https://www.mozilla.org/de/firefox/new/

34 Firefox Sicherheitskompendium – Anleitung um Firefox sicherer zu machen
https://www.heise.de/ct/entdecken/?volltext=sicherheitskompendium&sort=datum_auf&redautor=Mike+Kuketz

35 Flashcookies and privacy – Flashcookies und Privatsphäre
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862

36 Flashcookies and privacy II: Now with HTML5 and Etag – Flashcookies und Privatsphäre im Zusammenspiel mit HTML5 und Etags
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390

37 Gadotti, A., Houssiau, F., Rocher, L., Livshits, B. & de Montjoye, Y.-A.. Department of Comuting and Data Science Institute, Imperial College London, ICTEAM, Université catholique de Louvin. When the Signal is in the Noise: Exploiting Diffix's Sticky Noise. arxiv.org – Artikel über die hochgradige Anonymisierung von Datenbanken
https://arxiv.org/pdf/1804.06752.pdf

38 Gieselmann, H. 36. Chaos Communication Congress (2019, 29.12.). 36C3: Wie gängige Methoden zur Anonymisierung von Daten versagen – Nachweis, dass anonymisierte Daten keinesfalls anonym bleiben https://www.heise.de/newsticker/meldung/36C3-Wie-gaengige-Methoden-zur-Anonymisierung-von-Daten-versagen-4624450.html

39 Github – Evercookies – eine Bauanleitung https://github.com/samyk/evercookie

40 Github – Unified ID – Erklärung einer neuen Methode zur Werbung https://github.com/UnifiedID2/uid2docs

41 Google – Building a privacy-first future of web advertising – Google erklärt seine Vision von Werbung unter Wahrung der Privatsphäre https://blog.google/products/ads-commerce/2021-01-privacy-sandbox/

42 Google – Cookies in Chrome löschen, aktivieren und verwalten – eine Anleitung zur Handhabung von Cookies in Chrome https://support.google.com/chrome/answer/95647?hl=de&co=GENIE.Platform%3DAndroid

43 Gumm, D. / TH Lübeck "Metadaten sind strukturierte Daten, die Inhaltsdaten beigeordnet sind und etwas über diese aussagen."

44 Hayden, M. V. "We kill based on metadata." Wikipedia, Michael V. Hayden & Holland, M. / Heise Security – ein Beitrag in dem der ehemalige Direktor der CIA, später auch der NSA, erklärt, dass Amerika Menschen allein auf Basis von Metadaten tötet https://www.heise.de/newsticker/meldung/Ex-NSA-Chef-Wir-toeten-auf-Basis-von-Metadaten-2187510.html

45 heise security - Feature mit Bug: Microsoft Edge telefoniert besuchte Seiten nach Hause - https://www.heise.de/news/Feature-mit-Bug-Microsoft-Edge-telefoniert-besuchte-Seiten-nach-Hause-8980355.html

46 Here’s how to enable DoH in each browser, ISPs be damned – Anleitung, um DoH in jedem Browser zu aktivieren https://www.zdnet.com/article/dns-over-https-will-eventually-roll-out-in-all-major-browsers-despite-isp-opposition/

47 Hiller, A., Hakuna Metadata - Warum Metadaten und Browserverläufe mehr über uns verraten als oft vermutet. netzpolitik.org – Erläuterung, weshalb Metadaten so gefährlich für die Anwender sind https://netzpolitik.org/2017/hakuna-metadata-warum-metadaten-und-browserverlaeufe-mehr-ueber-uns-verraten-als-oft-vermutet/

48 HSTS – HTTP Strict Transport Security – eine Transportverschlüsselung https://de.wikipedia.org/wiki/HTTP_Strict_Transport_Security

49 HSTS – HTTP Strict Transport Security – eine Transportverschlüsselung https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security

50 Human Who Codes – HTTP cookies explained – eine Erklärung von HTTP-Cookies
https://humanwhocodes.com/blog/2009/05/05/http-cookies-explained/

51 Inside digital – Cookies löschen & deaktivieren: So bleiben Deine Internet-Nutzerdaten geheim – Anleitung zum Umgang mit Cookies
https://www.inside-digital.de/ratgeber/cookies-loeschen-oder-deaktivieren-so-machst-du-es-richtig

52 Intelligent Tracking Prevention – intelligente Vermeidung von Tracking
https://webkit.org/blog/7675/intelligent-tracking-prevention/

53 IONOS – Canvas Fingerprinting – Erläuterung zum Canvas Fingerprinting
https://www.ionos.de/digitalguide/online-marketing/web-analyse/canvas-fingerprinting-webtracking-ohne-cookies/

54 IONOS – Cookies deaktivieren: Wie lassen sich Cookies deaktivieren? -
https://www.ionos.de/digitalguide/websites/webseiten-erstellen/cookies-im-browser-deaktivieren/

55 Johns Hopkins University. The Price of Privacy: Re-Evaluating the NSA, A Debate – Die Podiumsdiskussion in der Michael Vincent Hayden erklärt, dass Amerika Menschen auf Grund von Metadaten tötet (ehemaliger Direktor der CIA, später NSA)
https://www.youtube.com/watch?v=kV2HDM86XgI

56 Kaspersky, How to enable Cookies – wie man Cookies aktiviert
https://support.kaspersky.com/common/windows/2843#block2

57 Kaspersky, What are Cookies – eine Erläuterung, was Cookies sind
https://www.kaspersky.com/resource-center/definitions/cookies

58 Kuksov, I. / Kaspersky. Wie flüchtige Metadaten für echte Probleme sorgen können. kaspersky.de – Erklärung wie Metadaten zu echten Problemen werden können
https://www.kaspersky.de/blog/office-documents-metadata/9915/

59 Kurz, C. & Rieger, F. / Chaos Computer Club. Stellungnahme des Chaos Computer Clubs zur Vorratsdatenspeicherung -
https://www.ccc.de/system/uploads/150/original/VDSfinal18.pdf?1403228408

60 Marketing / Open Data Security. What is Metadata and what does it reveal. opendatasecurity.io? - Was Metadaten sind
https://opendatasecurity.io/what-is-metadata-and-what-does-it-reveal/

61 Microsoft Support – Löschen und Verwalten von Cookies -
https://support.microsoft.com/de-de/windows/l%C3%B6schen-und-verwalten-von-cookies-168dab11-0753-043d-7c16-ede5947fc64d

62 mozilla Support – Cookies blockieren - https://support.mozilla.org/de/kb/Cookies-blockieren

63 Neuer Tab – Seite personalisieren -
https://chrome.google.com/webstore/category/collection/customize_your_new_tab_page

64 Netzpolitik.org. Fehler bei IP-Adressen: Viele Briten fälschlich wegen Kinderpornos verhaftet – Gefahren von Metadaten https://www.derstandard.at/story/2000070834253/fehler-bei-ip-adressen-viele-briten-faelschlich-wegen-kinderpornos-verhaftet

65 openh264.org – Website, die Video Codecs anbietet https://www.openh264.org/

66 owasp – Secure Cookie Attribute – Erläuterung, was sichere Cookies ausmacht https://owasp.org/www-community/controls/SecureCookieAttribute

67 PC-Magazin – So werden Sie mit Cookies ausspioniert - https://www.pc-magazin.de/ratgeber/so-werden-sie-mit-cookies-ausspioniert-1048816.html

68 Privacy-Preserving Ad Click Attribution for the Web – Ergänzungen von Trackern, um die Privatsphäre zu schützen https://webkit.org/blog/8943/privacy-preserving-ad-click-attribution-for-the-web/

69 Privacy-Preserving Product Analytics (P3A) – Privatsphäre schüztende Analyseverfahren https://brave.com/privacy-preserving-product-analytics-p3a/

70 Protecting against HSTS abuse – Schutz gegen den Missbrauch von HTTP Strict Transport Security https://webkit.org/blog/8146/protecting-against-hsts-abuse/

71 remind / HAW Hamburg – Informationen zu Metadaten http://www2.bui.haw-hamburg.de/pers/ulrike.spree/remind/metadaten.htm.

72 State partitioning – Verwaltung von Nutzerdaten auf Seiten des Browsers https://developer.mozilla.org/en-US/docs/Web/Privacy/State_Partitioning

73 Tales of Favicons and Caches: Persistant Tracking in modern Browsers – Erläuterungen zu dauerhaftem Tracking durch moderne Browser https://www.cs.uic.edu/~polakis/papers/solomos-ndss21.pdf

74 techopedia, Zombie Cookie - Kaspersky, What are Cookies – eine Erläuterung von Zombie Cookies https://www.kaspersky.com/resource-center/definitions/cookies

75 The most popular solution to cookie laws – rechtskonforme Einbindung von Cookies https://www.osano.com/cookieconsent

76 The Verge - Microsoft Edge is leaking the sites you visit to Bing - https://www.theverge.com/2023/4/25/23697532/microsoft-edge-browser-url-leak-bing-privacy

77 The Verge – Privacy and ads in chrome are about to become flocing complicated – Erläuterung einer neuen Trackingform durch Google. Nur für Chrome. Seit dem 14. Juli 2021 von Google eingestellt, bevor offiziell eingeführt

https://www.theverge.com/2021/3/30/22358287/privacy-ads-google-chrome-floc-cookies-cookiepocalypse-finger-printing

78 TOR Browser Bundle – Browser für weitestgehend anonymes Surfen - https://www.torproject.org/de/download/

79 Verbesserter Schutz vor Aktivitätsverfolgung in Firefox für Desktop - https://support.mozilla.org/de/kb/verbesserter-schutz-aktivitatenverfolgung-desktop

80 Verbraucherportal-bw.de – Cookies – hilfreich oder gefährlich - https://www.verbraucherportal-bw.de/,Lde/Startseite/Verbraucherschutz/Cookies+_+hilfreich+oder+gefaehrlich_

81 Verbraucherzentrale – Cookies kontrollieren und verwalten - https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/cookies-kontrollieren-und-verwalten-11996

82 VPN (Virtual Private Network) – Erklärung, was VPN sind https://de.wikipedia.org/wiki/Virtual_Private_Network

83 What is canvas fingerprinting and how the companies use it to track you online – Erklärung der Technik Canvas Fingerprinting und wie sie eingesetzt wird https://www.andreafortuna.org/2017/11/06/what-is-canvas-fingerprinting-and-how-the-companies-use-it-to-track-you-online/

84 Widevine – Software die vor Schadcode schützen soll https://www.widevine.com/

85 Wikipedia – Secure cookie – Erläuterung was sichere Cookies sind https://en.wikipedia.org/wiki/Secure_cookie