Spurenarm Surfen

Freiheitsfoo

2014

Gründe für den Firefox

- Die meisten Menschen benutzen bereits Firefox als Standard-Browser
- Weitreichende Konfigurationsmöglichkeiten
- Rege Entwicklung
- Entwickeln mit Blick auf die Nutzer

"Wir entwickeln Firefox mit einer Mission, für die Sie zuerst kommen, vor allem anderen. Wir tun dies, damit Sie die Kontrolle behalten. Wir tun dies, damit Sie sorgenfrei surfen können. Und wir tun dies, weil es sonst niemand tut." [1]

[1] https://www.mozilla.org/de/firefox/desktop/trust/

Suchmaschinen

- Suchanfragen geben ein detailliertes Bild der Nutzer
- Große Betreiber tracken Benutzer mit sehr ausgereiften Methoden
- Macht-/Wissensmonopole manipulieren mit angezeigten Ergebnissen
- Standardmäßig aktivierte Suchmaschinen verraten unnötige Informationen

Auswahl alternativer Suchmaschinen mit eigenem Index

- DuckDuckGo
- Blekko
- Open Directory

Auswahl alternativer Metasuchmaschinen

- Ixquick
- Startpage
- Metager2

Suchmaschinen via mycroftproject einbinden

Cookies

- Identifizierung wiederkehrender Nutzer
- Bei Webshops notwendig
- Bei Newsportalen oft unnötig

Cookie-Strategie mit Self-Destructing Cookies:

- Cookies werden standardmäßig nach dem schließen der Seite gelöscht
- Für vertrauenswürdige Seiten werden Ausnahmen definiert
- Nach dem schließen des Browsers werden alle Cookies gelöscht

EverCookies

- Eingeführt um gelöschte Cookies wiederherzustellen
- Setzen von Markierungen an vielen verschiedenen Stellen im Browser
- Konfiguration allein reicht nicht, um alle Arten zu blockieren
- Vollends schützt nur JonDoFox gegen alle bekannten Maßnahmen

Verteidigung:

- Verbindung zu Trackingdiensten via AdBlocker blockieren
- JavaScript kontrolliert erlauben
- IdexedDB deaktivieren

JavaScript

- Programmcode wird im Browser ausgeführt
- Sorgt für Dynamik auf Webseiten (Aufklappende Menüs, Autovervollständigung in Suchfeldern, . . .)
- Meistens nur kleine Erleichterung, aber großer Privatsphäre Verlust
  - Auslesen vieler Betriebssystem- und Computereigenschaften
  - Erkennen installierter Plugins
  - Viele EverCookies nutzen JavaScript
  - Schadcode kommt oft mit JavaScript auf den Rechner

Werbung

- Viele Webseiten finanzieren sich über Werbeeinnahmen
- Eigentliche Werbung wird von fremden Server nachgeladen
- Websiteübergreifendes Tracking möglich
- AdBlock Edge/Plus
- Ghostery

Referer und History-Sniffing

- Browser speichert besuchte Seiten in Chronik
- Die letztbesuchte Seite wird automatisch mitgeschickt (HTTP referer)
- Wie oft schaut man wirklich in diese Historie hinein?
- Um “anonyme” Datensätze der Webung zu personalisieren werden Emails o.ä. an Referer angehängt
- Plugin: Referrer Control

Cache

- Beim Aufruf von Seiten wird ETag mitgeschickt
- Beim erneuten Aufruf fragt Browser mittels ETag, ob Inhalt sich geändert hat
- Vergleich des ETags kann Cookies wieder herstellen

Schriftarten

- Vorhandene Schriftarten werden oft abgefragt
- Werden zur Berechnung eines Browser-Fingerprints genutzt
- Einschränkung auf 3 Schriftarten beste Lösung

User-Agent

- Informationen über Browser und Betriebssystem werden mitgesendet

‘Mozilla/5.0 (Macintosh; U; PPC Mac OS X; de-DE) AppleWebKit/419.3 (KHTML, like Gecko) Safari/419.3’

- Faken der Informationen schwierig

JonDoFox

- Fertiges Firefox-Profil
- Gute Javascript-, Cookie-, Zertifikatskontrolle
- Faking des HTML-Headers

`https://www.anonym-surfen.de/jondofox.html`

Links

- `https://privacy-handbuch.de` - Sehr gute Anleitung zum anonymen Umgang mit dem Internet
- `https://www.anonym-surfen.de` - JonDo
- `https://panopticlick.eff.org/` - Einfache Trackingauswertung
- `https://panopticlick.eff.org/browser-uniqueness.pdf` - Technische Erklärung verschiedener Trackingmethoden