Projekt BlindFaith - Webbasierte, Privatsphäre schützende Ansätze für Blinde und Sehschwache

Projektlaufzeit: 1. Dezember 2014 – 30. November 2015

Informationsmaterial zum barrierefreien Schutz der Privatsphäre im Internet

Austrian Institute of Technology AIT

Innovation Systems, Technology Experience

Projekt gefördert von der Internet Foundation Austria in der 9. netIdee Ausschreibung

netidee
powerful innovations

Inhaltsverzeichnis

1. Überblick

Im Rahmen des Projektes BlindFaith wurde Informationsmaterial zum Thema Privatsphäre im Internet entwickelt.

Es gibt zahlreiche Bedrohungen der Privatsphäre für Benutzer und Benutzerinnen die im Internet surfen. In diesem Dokument finden sie einen Überblick über mögliche Bedrohungen und wie man sich dagegen schützen kann.

Danach wollen wir ein Bedrohung-Szenario, nämlich Tracking und Verhaltensanalyse genauer betrachten. Als Einführung in die Thematik finden Sie Information, was man unter Tracking versteht und wie Tracking funktioniert. Anschließend wird beleuchtet wie Tracking die Privatsphäre bedrohen? Zum Abschluss finden Sie konkrete Informationen welche Möglichkeiten existieren, sich vor Tracking zu schützen.

2. Welche Bedrohungen für meine Privatsphäre gibt es im Internet?

Es gibt zahlreiche Bedrohungen der Privatsphäre, die Benutzer und Benutzerinnen die im Internet surfen, nicht immer eindeutig unterscheiden können. Im Folgenden möchten wir einen Überblick über mögliche Bedrohungen bieten und kurz beschreiben wie man sich dagegen schützen kann. Quelle ist vor allem die Web Seite WebOfTrust[1] (in Englisch).

2.1 Tracking und Verhaltensanalyse

Werbeunternehmen verwenden Cookies, Tracker, Zählpixel und andere – zum Teil in der rechtlichen Grauzone beheimateten – Techniken, um Ihr Verhalten im Web zu verfolgen, und in weiterer Folge zu analysieren. Diese Techniken sind auf den Webseiten, die Sie aufrufen eingebettet und werden automatisch gestartet. Z.B. melden Seiten mit einem Social Media Button (beispielsweise von Facebook), dass diese Seite besucht wurde, auch ohne, dass sie auf den Button klicken.

Schützen kann man sich durch “Tracking Blocker”. Siehe “2.5 Was kann ich gegen Tracker tun“.

2.2 Daten in der „Cloud“

Daten die in der Cloud, sprich auf Onlinespeicherplätzen und nicht lokal auf Ihrem Computer abgelegt werden, sind nicht mehr in Ihrer Kontrolle. Was mit den Daten geschieht, wer

[1] https://www.mywot.com/en/blog/156-the-top-10-online-privacy-threats

Zugriff hat usw. wird in den allgemeinen Geschäftsbedingungen der Anbieter festgelegt. Darüber hinaus treffen für den Anbieter je nach Firmensitz andere Datenschutzgesetze zu.

Schützen kann man sich indem man keine sensiblen Daten auf Cloud Speichern ablegt, oder durch die Verwendung von Verschlüsselungsprogrammen z.B. VeraCrypt

2.3 Suchverhalten Historie

Bekannte Suchmaschinen sammeln zu Werbezwecken zahlreiche Daten über das Suchverhalten der Nutzer und Nutzerinnen. Dies gilt besonders wenn Sie sich bei Suchmaschinen Anbietern mit einem persönlichen Benutzerkonto eingeloggt haben. Über die Suchhistorie lassen sich zahlreiche Rückschlüsse auf persönliche Präferenzen, finanzielle Möglichkeiten, politischen Einstellungen etc. ziehen. Diese Informationen werden für zielgerichtete Werbung genutzt.

Schützen kann man sich durch die Verwendung von Suchmaschinen welche keine persönlichen Daten speichern. z.B. DuckDuckGo

2.4 Spyware und Adware

Als Spyware (Spähprogramm) wird Software bezeichnet, die Daten eines Computernutzers oder einer Computernutzerin ohne dessen Wissen oder Zustimmung an den Hersteller oder an Dritte sendet. Es wird auch dazu genutzt, dem Benutzer oder der Benutzerin über Werbeeinblendungen Produkte anzubieten. Solche Spyware und Adware wird meist unabsichtlich als Zusatz bei Gratisprogrammen installiert.

Schützen kann man sich durch die Anti-Malware Software, z.B. Malwarebytes

2.5 Soziale Netzwerke

Soziale Netzwerke basieren auf der (freiwilligen) Bekanntgabe von persönlichen Daten der Nutzer und Nutzerinnen. Bei sozialen Netzwerken treten gleich zwei Probleme für die Privatsphäre auf. Zum einen können unter Umständen unbeabsichtigt private Daten von Dritten eingesehen werden. Zum anderen werten die Anbieter von sozialen Netzwerken gezielt die Daten ihrer Nutzer und Nutzerinnen aus. Insbesondere die Verknüpfungen von Daten (Suchanfragen, Aufrufe von Profilen, besuchte Orte, etc.) verraten oft mehr über persönliche Präferenzen, finanzielle Möglichkeiten etc. als die Nutzer und Nutzerinnen vermuten.

Schützen kann man sich vor allem durch überlegen, welche Informationen man im sozialen Netzwerk veröffentlicht und welche nicht.

2.6 Online Shopping

Onlineshops benötigen zu Versandzwecken, Bezahlungen usw. private und sensible Daten der Nutzer und Nutzerinnen. Was mit den Daten geschieht (z.B. Weitergabe an Dritte) wird in den allgemeinen Geschäftsbedingungen festgelegt. Darüber hinaus treffen für den Anbieter je nach Firmensitz andere Datenschutzgesetze zu.

Schützen kann man sich durch lesen der Allgemeinen Geschäftsbedingungen und der Datenschutzerklärung.

2.7 Ortsbezogene Datenanalyse

Über die IP Adresse (und bei Smartphones das GPS Signal) lässt sich der Ort an dem sich Benutzer und Benutzerinnen befinden feststellen. Durch Verknüpfung dieser Ortsdaten können detaillierte Bewegungsprofile angelegt werden. Die Daten können auch für gezielte ortsbezogene Werbung, sogenanntes Geo-Marketing genutzt werden.

Schützen kann man sich beim Smartphones durch deaktivieren der Ortungsdienste bzw. durch Kontrollieren, welche Berechtigungen Apps besitzen. Vor ortsbezogener Datenanalyse über die IP Adresse kann man sich nur über Anonymisierungsdienste wie z.B. TOR oder JonDo schützen.

3. Was kann ich gegen Verhaltensanalyse und Zielgruppenansprache tun?

Vielleicht ist Ihnen das schon einmal aufgefallen: Sie planen ihren Urlaub und recherchieren im Internet über mögliche Reiseziele. Auf einmal erscheinen auf Internetseiten die nicht mit der Urlaubsplanung zu tun haben Werbungen für diverse Reiseanbieter. Der Grund dafür, Tracking mittels sogenannter Cookies und Web Bugs.

3.1 Was ist Tracking?

Unter Tracking versteh man verschiedene Techniken um das Verhalten von Nutzerinnen und Nutzern im Internet zu verfolgen, aufzuzeichnen und anschließend zu analysieren. Das kann für statistische Zwecke (z.B. zur Analyse von Webseitenzugriffen) genutzt werden, kann aber auch dazu verwendet werden Profile von Nutzern und Nutzerinnen anzulegen, um diese Profile später für Werbezecke zu verwenden oder zu verkaufen.

3.2 Wie funktioniert Tracking?

Technisch gesehen gibt es dafür verschiedene Möglichkeiten.

Zumeist werden auf dem Computer des Nutzers oder der Nutzerin sogenannte „Cookies“ abgelegt. Cookies sind kleine Textdateien in denen ein eindeutig zuordenbarer Code

gespeichert ist. Über diesenCode können Betreiber beim Aufruf einer Seite erkennen ob der Nutzer oder die Nutzerin schon einmal auf dieser Seite war.

Eine andere Methode um Zugriffe von Nutzern und Nutzerinnen zu speichern und zu analysieren ist das Speichern von Zugriffen anhand der IP Adresse (eine Adresse in Computernetzen). Unternehmen die Daten sammeln bauen in Webseiten sogenannte Zählpixel ein. Diese kleinen unsichtbaren Bilder werden vom Server des Daten sammelnden Unternehmens geladen. So kann anhand der IP Adresse identifiziert werden welche Seiten ein Nutzer bzw. eine Nutzerin. besucht. Aufgrund der IP Adresse kann auch der ungefähre Wohnort des Nutzers oder der Nutzerin ermittelt werden.

Darüber hinaus ist es auch möglich anhand des sogenannten „Browser Fingerabdrucks“ (Browserversion, Betriebssystem, installierte Plug-Ins, etc.) den Nutzer zu identifizieren.

3.3 Wofür werden Tracker verwendet?

Es gibt verschiedene Typen von Trackern:

- Werbung: Tracker die Werbung verbreiten
- Analyse: Tracker die für statistische Zwecke, Seitenaufrufe etc. verwendet werden
- Beacon: Tracker die nur dazu da sind um NutzerInnen- und Nutzer-Verhalten zu verfolgen und zu speichern
- Widget: Tracker die außerdem eine gewisse Funktionalität erfüllen z.B. "Like" Buttons

3.4 Wie bedrohen Tracker meine Privatsphäre?

Problematisch wird es wenn Tracking von Unternehmen verwendet wird, die sich auf Datensammlung spezialisiert haben. Diese Unternehmen verwenden diese Methoden nicht nur auf einer einzelnen Webseite, sondern betten sie in verschiedenen Internetseiten ein. Bei jedem Aufruf einer Seite wird der eindeutige Code des Nutzers bzw. der Nutzerin an das Daten sammelnde Unternehmen übermittelt, zusammen mit der Information welche Seite besucht wurde.

Mit diesen Methoden, insbesondere wenn sie kombiniert und mit persönlichen Profilen von sozialen Netzwerken o.ä. verknüpft werden, lassen sich gezielte Profile erstellen, welche Webseiten von / einer NutzerIn bzw. einem Nutzer besucht wurden. Dadurch lassen sich Rückschlüsse über Kaufkraft, persönliche Interessen, Wohnort, Alter, Gesundheitszustand oder ähnliches ziehen.

So ist es auch möglich, dass sie nachdem sie eine Webseite über „die schönsten Urlaubsziele der Welt“ besucht haben anschließend auf einer anderen Webseite Werbung für einen Reise-Anbieter angezeigt bekommen.

3.5 Was kann ich gegen Tracker tun?

Es gibt verschiedene Browser Erweiterungen, mit denen es möglich ist Tacker zu blockieren. Wir haben einige davon auf Barrierefreiheit hin analysiert. Leider ist keines der analysierten Tools vollständig barrierefrei, am zugänglichsten ist mit gewissen Einstellungen das Tool Ghostery.

- Ghostery:
  - Das Plugin ist mit Tastatur bedienbar - Alt+Strg+G öffnet das Menü, welche mit dem Keyboard navigiert werden kann. Wird von Screenreader (NVDA) auch korrekt vorgelesen. Allerdings nur in der alten Version des Menüs, die neue Version ist leider nicht vollständig zugänglich.
  - https://www.ghostery.com
  - Verfügbar für Firefox, Chrome, Opera, Safari, Internet Explorer
- Privacy Badger
  - Privacy Badger ist laut Entwickler mit Tastaturen nicht bedienbar.
  - https://www.eff.org/de/node/73969
  - Verfügbar für Firefox, Chrome, Safari (geplant), Opera (geplant)
- DisconnectMe:
  - Wir haben leider keine Information zu Tastatur Bedienung gefunden. Eine Anfrage an den Support blieb unbeantwortet.
  - https://disconnect.me
  - Verfügbar für Firefox, Chrome, Internet Explorer, Safari, Opera
- Blur
  - Wir haben leider keine Information zu Tastatur Bedienung gefunden. Eine Anfrage an den Support blieb unbeantwortet.
  - https://www.abine.com/index.html
  - Verfügbar für Firefox, Chrome, Opera, Safari, Internet Explorer

3.5.1 Installation Ghostery

Die Installation von Ghostery funktioniert barrierefrei. Die Installation erfolgt durch Hinzufügen de Erweiterung zum bevorzugten Browser (unterstützt werden Firefox, Chrome, Opera, Safari und Internet Explorer). Allerdings gab es bei unserer letzten Analyse noch Probleme bei der Installation im InternetExplorer.

Wir zeigen hier exemplarisch wie die Installation unter Firefox 38.0.5 funktioniert:

1. Es wird eine alte Version von Ghostery benötigt, welche noch barrierefrei funktioniert – Ghostery Version 2.9.6
2. Nach dem Öffnen dieses Link öffnet sich ein Fenster und es wird gefragt, ob Firefox dieses Add-On installieren soll. Dies wird mit dem Button „Installieren“ bestätigt.

Nun ist die Installation abgeschlossen. Damit Ghostery Tracker auch tatsächlich blockiert, müssen noch einige Einstellungen vorgenommen werden.

1. Zuerst die Ghostery Optionen aufrufen – Extras – Ghostery - Optionen (ALT+ X + G + M)
2. Unter Blockieroptionen kann man entscheiden, welche Tracker blockiert werden sollen. Alle Tracker können man mit der Option „Alle Auswählen“ ausgewählt werden. Anschließend sollten die Einstellungen mit dem Button „Speichern“ gespeichert werden.
3. Analog dazu kann man mitentscheiden, welche Cookies blockiert werden sollen. Dazu die Schaltfläche „Cookies“ auswählen. Alle Cookies könnenmit der Option „Alle Auswählen“ ausgewählt werden. Anschließend sollten die Einstellungen mit dem Button „Speichern“ gespeichert werden.

Um eine Bedienung mit Tastatur (und Screenreader) zu ermöglichen, muss die alte Ansicht des Ghostery Menüs aktiviert werden.

1. Dazu in die Schalfläche „Erweitert“ wechseln.
2. Die Option „Noch nicht bereit für die neue Ansicht? Kehren Sie vorübergehend zum alten Menü zurück (Neustart erforderlich)“ aktivieren.
3. Anschließend wird der Browser neu gestartet, und die alte Version des Menüs ist aktiviert.
4. Mit der Tastenkombination STRG + ALT + G kann man das Menü aufrufen und überprüfen ob die Umstellung erfolgreich war. Wenn sich die Elemente mit der Tastatur navigieren lassen, dann war die Umstellung erfolgreich.

3.5.2 Bedienung von Ghostery

Ghostery zeigt auf jeder Seite an, welche Tracker in die Seite eingebunden sind, ob sie blockiert werden und bietet dazu auch weiterführende Informationen an.

Das Menü kann über die Tastenkombination STRG+ALT+G aufgerufen werden. Mit den Pfeiltasten kann durch die gefundenen Tracker navigiert werden.

Weiterführende Informationen zu jedem Tracker können durch Auswählen des Trackers und Druck auf die Pfeiltaste nach rechts aufgerufen werden. Zur Auswahl stehen als erstes Element weiterführende Informationen unter „Was ist [Name des Trackers]“.

Ob ein Tracker blockiert wurde kann ebenfalls durch Auswählen des Trackers und Druck auf die rechte Pfeiltaste aufgerufen werden. Als drittes Element der Liste steht die Info „[Name des Trackers] blocken?“. Der Tracker ist blockiert wenn diese Option ausgewählt ist, bzw. nicht blockiert wenn diese Option nicht ausgewählt wurde.

Wenn man auf einer Seite das Blockieren aller Tracker abschalten will dann kann man dies im Menü (STRG+ALT+G) unter dem Menüpunkt „Blockieren anhalten“ tun.

3.6 Weiterführende Links

- http://www.zeit.de/digital/datenschutz/2012-04/cookies-tracking-gegenwehr
- https://www.datenschutzzentrum.de/tracking/