Trackingtools auf Websites staatlicher Institutionen

1 Verständnishilfen

1.1 Kein Trackingtool ist nicht gleich kein Tracking

Ziel dieser Recherche war es, die Verwendung von Trackingtools üblicher Anbieter wie Google Analytics, Piwik oder Etracker zu messen. Wurde keine Verwendung eines Trackingtools festgestellt, bedeutet das nicht, dass Nutzer nicht verfolgt werden oder verfolgt werden können. Es bedeutet lediglich, dass keine Trackingsoftware erkannt wurde.

Eine Verfolgung der Benutzeraktivitäten ist immer noch über eigene Programme oder auch über die Auswertung der Serverlog-Datei möglich. Die Serverlog-Datei speichert in der Standardeinstellung vieler Server zahlreiche Informationen über die Aktivitäten der Nutzer, unter anderem die aufgerufene Seite, den Zeitpunkt des Aufrufs und die IP-Adresse.

1.2 Definition einer Widerspruchsmöglichkeit

Gegenstand der Recherche war auch das Vorhandensein oder Fehlen einer Widerspruchsmöglichkeit zum Tracking. Folgende Varianten des Widerspruchs wurden überprüft:

- Widerspruch durch Setzung eines Cookies, meist auf Basis eines vom Trackingprogramm zur Verfügung gestellten und vom Website-Betreiber eingebundenen Iframes
- Akzeptierung des Do Not Track-Headers[1]

In der Datenquelle wird genau angegeben, welche Methode oder welche Methoden akzeptiert werden oder nicht. Eine indirekte Widerspruchsmöglichkeit bedeutet, dass ein Widerspruch nicht direkt auf der aufgerufenen Seite möglich ist, sondern auf den Seite eines zentralen Tracking-Anbieters durch Setzung eines Cookies, der Widerspruch folglich nicht beim eigentlichen Anbieter erfolgen kann.

1.3 Unterstützung von TLS

Die Angabe, dass TLS nicht unterstützt wird, bedeutet, dass entweder keine verschlüsselte Übertragung angeboten wird oder dass nach Aufrufen einer verschlüsselten Verbindung direkt wieder zur unverschlüsselten Verbindung zurückgeleitet wird.

Die Angabe TLS unterstützt wird auch gesetzt, wenn das Zertifikat auf eine andere, aber vertrauenswürdige Stelle ausgeschrieben wurde, so zum Beispiel das Zertifikat einer Regierungswebsite auf bund.de ausgestellt ist.

1 Eine derzeit in der W3C-Standardisierung befindliche Header-Information, durch die der Benutzer eines Browser aufgerufenen Websites mitteilen kann, dass er verfolgt oder nicht verfolgt werden möchte oder keine Präferenz hat.

2 Bewertung

2.1 Allgemeines

Positiver erster Eindruck beim Studium der Rechercheergebnisse ist, dass von keiner der überprüften Websites die Analysesoftware Googles, Google Analytics, einsetzt. Diese gilt als besonders bedenklich, da Daten nicht nur erhoben werden, sondern auch an die Server Googles gesendet werden und so außerhalb der Kontrolle des Administrators liegen. Tatsächlich werden die erhobenen Nutzerdaten mit hoher Wahrscheinlichkeit außerhalb Deutschlands gespeichert und vielleicht mit den Daten anderer Websites zusammengeführt. So können ganze Profile über zahlreiche Websites hinweg erstellt werden.

Einige Bundesministerien und der Bundesfinanzhof setzen auf den hamburgischen Anbieter Etracker. Auch bei Etracker werden die Daten auf den Servern des Anbieters gespeichert. Im Gegensatz zum US-amerikanischen Google Analytics werden die gesammelten Informationen allerdings auf deutschen Servern gespeichert und nicht mit den Daten anderer Kunden zusammengeführt. Auch werden IP-Adressen grundsätzlich verkürzt gespeichert. Diese Maßnahmen wurden vom hamburgischen Datenschutzbeauftragten laut Angaben des Unternehmens im Jahre 2006 kontrolliert[2]. Es ist fraglich, wie diese Kontrolle aussah und warum es keine häufigeren Kontrollen gibt. Auch besteht bei zentralisierter Speicherung immer das Risiko, dass Daten durch das Unternehmen selbst oder auch durch einen unberechtigten Zugriff missbräuchlich verwendet werden. Im Vergleich zur Speicherung von Nutzerdaten auf dem jeweiligen Server einer Website birgt das Prinzip der zentralen Speicherung ein ungleich höheres Missbrauchspotential, weswegen davon grundsätzlich abzuraten ist. Etracker wird zum Zeitpunkt der Recherche von den Bundesministerien für Arbeit und Soziales, Ernährung und Landwirtschaft, der Finanzen, der Verkehr und digitalen Infrastruktur, Wirtschaft und Energie sowie vom Bundesfinanzhof eingesetzt.

Eine weitere zentral konzipierte Anwendung ist Econda. Sie wird vom Bundesministerium für Gesundheit eingesetzt. Econda bringt die oben beschriebenen Nachteile einer zentralen Speicherung von Benutzerdaten mit sich. Das Unternehmen bietet eine Widerspruchsfunktion per Cookie, also nicht direkt über die Website des Gesundheitsministeriums.

Aber auch zwischen den Programmen, die eine Benutzeranalyse auf dem Server des Website-Betreibers anbieten, gibt es Unterschiede. Eingesetzt werden vor allem angebotene Lösungen von Server-Betreibern wie der Init-AG und die freie Software Piwik.

Die Website bundeswehr-karriere.de hat zwar eine rechtliche Erklärung zum Einsatz von Google Analytics auf seiner Website, verwendet es jedoch nicht. Stattdessen wird Webtrends eingesetzt.

Das Bundesministerium für Ernährung und Landwirtschaft bietet als einzige untersuchte Website eine präsente Mitteilung an, dass Nutzungsdaten in anonymisierter Form erhoben werden. Andere untersuchte Websites beschränken sich auf die Verlinkung zu einer Datenschutzerklärung oder zum Impressum, was Datenschutzhinweise enthält.

2 Siehe Etracker.com abgerufen am 9.7.2015 unter https://www.etracker.com/de/datenschutz.html.

2.2 Überraschende Vielfalt und Dezentralität

Es fällt auf, dass es keine einheitliche Richtlinie zum Tracking von Websites staatlicher Institutionen zu geben scheint, nicht einmal im Rahmen der Bundesregierung. Auf Regierungswebsites finden sich die Programme Piwik, Etracker, Webtrends, Econda und die Lösung der Init-AG. Ein Sonderfall ist das Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit, dass zwar Piwik nutzt. Piwik verweist aber auf die Domain cps-projects.de.

Diese mangelnde Einheitlichkeit ist mit Verweis auf die oben beschriebenen Vorteile einer Dezentralität begrüßenswert. Es ist jedoch nicht auszuschließen, dass Log-Dateien zusammengeführt.

Weiterhin fällt auf, dass von vielen Institutionen nicht auf das BSI, sondern auf gewerbliche Anbieter gesetzt wird.

2.3 Cloudflare

Cloudflare ist ein Content Delivery Network. Es liefert Websites über die eigene Serverstruktur aus und schützt die eigentliche Website damit vor Angriffen wie DDos-Attacken. Dadurch werden aller Besucher einer Website, die beispielsweise in Deutschland gespeichert ist, zuvor an den US-amerikanischen Anbieter Cloudflare weitergeleitet. Daten von Nutzern könnten dort zentral erfasst werden über eine Vielzahl an Kundenwebsites Cloudflares.

Unter den untersuchten Websites findet sich eine, die Kunde von Cloudflare ist: Die Website des Bundestages. Angesichts diverser Angriffe auf die Infrastruktur und die Internetpräsenz des Bundestages wurde offenbar die Abwägung zwischen Datenschutz und Ausfallsicherheit zugunsten der Ausfallsicherheit entschieden. Zuständig für technischen Fragen des Bundestages ist die Kommission für Informations- und Kommunikationstechnik, eine Unterkommission des Ältestenrates[3].

2.4 Kooperation zwischen legislativen und judikativen Organ

Kritisch zu betrachten ist die gewaltenübergreifende Kooperation zwischen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Bundesverfassungsgericht. Ersteres betreibt den Server für Letzteres. Zwar ist das Verfassungsgericht materiell berechtigt an der Domain und als admin-c eingetragen, die IP verweist aber auf einen Server des BSI.

2.5 Entwicklung

Bereits 2007 wurde dem Bundesjustizministerium vom Berliner Amtsgericht untersagt,

3 Siehe Parlementarisme.de unter https://parlementarisme.de/blog/im-bundestag/angriff-auf-die-bundestag-it (abgerufen am 09.07.2015).

Daten eines Klägers, die im Zusammenhang mit der Nutzung der Ministeriums-Website stehen, über den Nutzungsvorgang hinaus zu speichern[4]. Die Aufbewahrung derartiger Verkehrsdaten verletze das Recht auf informationelle Selbstbestimmung.

2.6 Abgleich mit Vorgaben des Düsseldorfer Kreises

Der Düsseldorfer Kreis ist ein Gremium der Datenschutzbeauftragten des Bundes und der Länder. 2009 hat er Vorgaben auf Grundlage des Telemediengesetzes aufgestellt, die für eine datenschutzkonforme Ausgestaltung bei der Reichweitenmessung auf Websites zu beachten sind:

- Nutzungsprofile dürfen nur bei Verwendung von Pseudonymen erstellt werden. Die IP-Adresse ist kein Pseudonym
- Der Betroffene muss eine Möglichkeit zum Widerspruch gegen die Erstellung von Nutzungsprofilen haben
- Die pseudonymisierten Nutzungsdaten dürfen nicht mit Informationen über den Träger des Pseudonyms zusammengeführt werden und müssen gelöscht werden, wenn sie für die Erstellung der Nutzungsanalyse nicht mehr erforderlich sind oder der Nutzer dies verlangt
- Es muss deutlich auf die Erstellung pseudonymisierter Nutzungsprofile und die Möglichkeit zum Widerspruch hingewiesen werden
- Personenbezogene Daten dürfen nur gespeichert werden, wenn sie notwendig sind, um die Telemedien zu nutzen und abzurechnen. Ansonsten bedarf es der Zustimmung der Betroffenen
- Solange keine bewusste, eindeutige Einwilligung vorliegt, ist die IP-Adresse vor jeglicher Auswertung so zu kürzen, dass eine Personenbeziehbarkeit ausgeschlossen ist.

13 der 35 untersuchten Websites wiesen kein erkennbares Tracking auf, zumindest nicht per Zählpixel oder Javascript. Das ist die datensparsamste und datenschutzfreundlichste Variante und wird von folgenden Websites angewandt:

- http://bund.de
- http://bmjv.de
- http://bmi.bund.de
- https://bsi.bund.de
- https://bsi-fuer-buerger.de
- https://destatis.de
- http://auswaertiges-amt.de
- http://bundesrat.de
- https://vermittlungsausschuss.de

4 Siehe Daten-Speicherung.de unter http://www.daten-speicherung.de/index.php/urteil-vorratsspeicherung-von-kommunikationsspuren-verboten/#ag (abgerufen am 10.07.2015).

- http://bundesverfassungsgericht.de
- http://bundesgerichtshof.de
- http://www.bundesarbeitsgericht.de
- http://bsg.bund.de

Damit haben 23 Websites ein Trackingtool installiert, das sind knapp 68%. Von den 23 Websites mit Tracking akzeptieren 4 Websites den Do Not Track-Header und bieten einen Opt Out an. Weitere zwei bieten einen Opt Out an, akzeptieren allerdings nicht den Do Not Track-Header. Das wird in den Forderungen des Düsseldorfer Kreises jedoch nicht explizit verlangt.Nur diese 6 Websites entsprechen den Anforderungen des Düsseldorfer Kreises zu größten Teilen. Es ist lediglich fraglich, ob wirklich deutlich auf die Erstellung pseudonymisierter Profile hingewiesen wird. Namentlich sind das:

- http://bundesregierung.de
- http://bundeskanzlerin.de
- http://digitale-agenda.de
- http://bmub.bund.de
- http://bmz.de
- http://bmbf.de

Weitere 7 Websites bieten keine Widerspruchsmöglichkeit auf der eigenen Website an, sondern verweisen auf Funktionen des für das Tracking eingebundenen Dienstleisters, hier Etracker oder Econda:

- http://bmas.de
- http://bundesfinanzministerium.de
- http://bmel.de
- http://bmg.bund.de
- http://bmvi.de
- http://bmwi.de
- http://bundesfinanzhof.de

Von den 23 Websites mit Trackingtool bieten 9 keine Widerspruchsmöglichkeit an, was im direkten Widerspruch zu den Vorgaben des Düsseldorfer Kreises steht:

- http://bmvg.de
- http://bundeswehr.de
- https://bundeswehr-karriere.de
- http://bmfsfj.de

- http://bundestag.de
- http://mitmischen.de
- http://das-parlament.de
- https://btg-bestellservice.de
- http://bverwg.de