Technology
Arts Sciences
TH Köln

Analyse und Modellierung von Server Side Web-Tracking

Entwicklung, prototypische Implementierung und Evaluation einer serverseitigen Trackingstrategie am Anwendungsfall der Agenturwebsite der elancer-team GmbH

Praxisprojekt

ausgearbeitet von

Christian Krenn

vorgelegt an der

Technischen Hochschule Köln
Campus Gummersbach
Fakultät für Informatik und
Ingenieurwissenschaften

im Studiengang
Medieninformatik

Betreuer: Prof. Dr. Hoai Viet Nguyen
Technische Hochschule Köln

Gummersbach, im April 2025

Inhaltsverzeichnis

1 Einleitung

1.1 Problemstellung

Das Webtracking beschreibt grundlegend das Beobachten, Sammeln und Auswerten von Bewegungen eines Nutzers auf einer Webseite. Für Webagenturen im Bereich der Digital Analytics fungieren die erhobenen Daten als Instrument, um Berichte zu erstellen und somit die geleisteten Arbeitserfolge zu dokumentieren.
Ferner stellen die Trackingdaten das Fundament für verschiedene operative Prozesse wie die Anpassung des bestehenden Webseitenaufbaus oder die Optimierung für Zielvorhaben wie eine Newsletteranmeldung, den Kauf eines Produkts oder das Herunterladen einer App dar.

Der deskriptive Stand des Webtrackings besteht darin, dass Nutzerinteraktionen auf einer Webseite nachverfolgt und analysiert werden können. Das Webtracking selbst erfolgt hauptsächlich clientseitig durch den Einsatz von Technologien wie Cookies, JavaScript und Fingerprinting. Bei 77,4 Prozent aller geladenen Webseiten (engl. page loads) sind laut Ghostery, einem Anbieter von Anti-Tracking-Software, Tracker (z.B. Google Analytics) involviert. [1]

Werbetreibende und Webagenturen konnten sich hier bis jetzt auf die Tracking-Pixel der verschiedenen Unternehmen wie Facebook oder Google stützen, um zu erkennen, wie der jeweilige Interessent die angebotenen Zielvorhaben annimmt und durchführt. Die Wirksamkeit solcher Signale wird Aufgrund von Blockierung der Browser-Tracker, der Einführung von Apple's ITP und der Einstellung der Unterstützung von Drittanbieter Cookies gemindert und die erhobene Datenqualität leidet darunter. Als Unternehmen, das auf die Zusammenstellung und Nachverfolgung der erhobenen Daten aus der Benutzerebene angewiesen ist, werden Messungen und das zielgerichtete Ausspielen und Optimieren von Inhalten auf der Benutzerebene komplexer.

Anknüpfend an den deskriptiven Stand des traditionellen clientseitigen Webtrackings bietet sich serverseitiges Tracking an. Im Paradigma des Server Side Trackings ist die Datenerhebung weniger anfällig für Restriktionen und die Datenverarbeitung findet auf der Serverseite statt. Durch die serverseitige Verarbeitung können unter anderem komplexere Datenanalysen durchgeführt werden, ohne die Performance der Website für den Endnutzer zu beeinträchtigen.

1.2 Zielsetzung der Arbeit

Das Ziel des abzubildenden Praxisprojekts ist die Analyse und Konzeption einer heuristischen Server Side Tracking Strategie für die bestehende Website der Kölner Webagentur elancer-team GmbH. Die ausgearbeitete Strategie soll eine erste Grundlage für die ganzheitliche Implementierung darstellen. Darüber hinaus soll ein erster lokaler Prototyp des serverseitigen Trackings aufgebaut werden.

Das Praxisprojekt strebt an, die theoretischen und praktischen Anforderungen einer modernen Server Side Tracking Lösung zu beleuchten. Während der Ausarbeitung gilt es, den bestehenden Stand der Dinge zu beleuchten und diesen fachlich zu eruieren. Das schlussendliche Konzept soll maßgeblich auf den zuvor hergeleiteten Informationen der Analyse- und Modellierungsphase basieren. Ferner sind besondere Erfordernisse aus dem jeweiligen Kontext zu identifizieren und während der Bearbeitung zu beachten.

Des Weiteren sollen im Verlauf des Projekts Alternativen berücksichtigt und Entscheidungen nachvollziehbar begründet werden.

1.3 Methodisches Vorgehen und Aufbau der Arbeit

Damit das gesetzte Ziel erreicht werden kann, wird ein methodisches Vorgehen durchgeführt, das sich grob in vier größere Bestandteile gliedern lässt.

Im ersten Schritt wird der deskriptive Stand des Webtrackings betrachtet und Definitionen und Bedeutungen des fachlichen Kontexts untersucht. Dieser Schritt stellt die Basis der Grundprinzipien, der Wissensbasis und der technischen Aspekte des Trackings dar.

Im zweiten Schritt wird eine detaillierte Analyse der Anforderungen an das Trackingkonzept erstellt. Hier werden technologische, datenschutzrechtliche und operative Aspekte beachtet. Ferner gilt es, die bestehende Tracking-Infrastruktur der elancer-team GmbH zu untersuchen, damit spezifische Hürden und Potenziale identifiziert werden können.

Die ganzheitliche Server Side Tracking Strategie wird im dritten Schritt erstellt. Die Strategie beinhaltet die Ausarbeitung eines Modells zur Datenerhebung und -verarbeitung. Darüber hinaus soll durch sorgfältige Evaluation und Auswahl der Technologien das Konzept in die bestehenden Prozesse integriert werden. Ziel ist es, eine robuste Grundlage für eine nahtlose Integration in das bestehende System zu schaffen.

Der letzte Schritt umfasst den Aufbau eines Prototypen und die kritische Reflexion der Arbeitsergebnisse sowie die Ausarbeitung eines Ausblicks für weiterführende Fragestellungen.

2 Grundlagen des Webtrackings

2.1 Definition und Bedeutung des Trackings

Tracking im Kontext der Informationstechnik bezeichnet die Erfassung, Analyse und Auswertung von Daten. Im Kontext von „Web-Tracking“, das den Schwerpunkt dieser Arbeit bildet, steht Tracking insbesondere für das Verfolgen von Nutzeraktivitäten im Internet.

Webtracking besteht aus einer Vielzahl von Techniken, mit denen Websites über Geräte hinweg Nutzerprofile erstellen können. Es handelt sich dabei um eine weit verbreitete Internettechnik, die verschiedene Nutzerdaten für diverse Zwecke aggregiert. Tracking wird genutzt, um Online-Nutzerauthentifizierung, Inhaltspersonalisierung, zur Untersuchung für die erweiterte Website-Analyse, für die Integration sozialer Netzwerke oder zur Webentwicklung. Konkret ermöglicht Webtracking Erst- oder Drittanbieter-Websites, das Surfverhalten von Nutzern, einschließlich Browserkonfiguration und -verlauf, zu verfolgen. Das Surfverhalten der Online-Nutzer wird als eine bewährte Quelle für die Erstellung detaillierter Profile von Website-Nutzern angesehen. Diese Profile sind von hoher Signifikanz für die Verbesserung von kommerziellen Aktivitäten. [2]

Die gesammelten Daten werden oftmals für die Anpassung von kommerziellen Aktivitäten wie dem Verbessern von Gebotsstrategien für Marketingkampagnen oder die Adaption der Nutzererfahrung auf Basis der erfassten Informationen genutzt. Um die Auswirkung messbar zu machen, benutzt man sogenannte Key Performance Indicators (KPIs). Die KPIs unterscheiden sich je nach Anbieter des jeweiligen Trackingtools und können verschiedene Arten von Tracking-Daten beinhalten und veranschaulichen.

Auf Grundlage einer Studie aus dem Jahr 2016 durchgeführt vom Browser-Hersteller Clinqz wurden bei mehr als 6 von 10 Seitenaufrufen Daten an Dritte übermittelt. [3]

Dieser Trend lässt sich auch durch eine Studie aus dem Jahr 2022 belegen, wobei 79% der Webseiten Drittanbieter-Tracking einsetzen. [4]

2.2 Arten von Tracking-Daten

Webtracking kann generell unterschiedliche Arten von Daten erfassen. Die Metriken, die für die jeweilige Webpräsenz wichtig sind, unterscheiden sich je nach Fokus. Bei einem Online-Shop stehen etwa andere Kennzahlen im Vordergrund als bei einer Landingpage. Generell sind Indikatoren wie Besucherzahlen und Absprungrate wesentliche Bestandteile der zu erfassenden Daten.

Nachfolgend sind gängige Metriken aufgeführt, die häufig bei Trackingkonzepten Verwendung finden:

- Besucherzahlen und Seitenaufrufe
- Verweildauer und Absprungrate
- Klickpfade und Nutzernavigation
- Geräteinformationen und Browserdaten
- Quellen des Website-Traffics
- Conversion-Events (z.B. Käufe, Anmeldungen, Kontaktaufnahme)

Darüber hinaus werden häufig personenbezogene Daten erhoben wie Vor- und Nachname, E-Mail-Adresse, Geschlecht, Alter, Einkommen, Wohnort, Familienstand, Gesundheitszustand, Einkäufe, präferierte Unterhaltungsmedien, Filme sowie allgemeine Interessen. [5]

2.3 Technologien und Methoden

Webtracking selbst funktioniert schematisch wie in Abbildung 1 gezeigt. Wenn ein Nutzer Webseiten des Betreibers aufruft, dann empfängt die Webseite Cookies.

Cookies

Cookies sind Datenpakete, die ein Webserver an den Browser sendet. Wenn ein Browser in Zukunft ein Objekt aus derselben Domäne anfordert, sendet der Browser dieselbe Datenfolge zurück an den Ursprungsserver. [6]

Webbasierte Anwendungen verwenden häufig Cookies, um den Zustand des ansonsten zustandslosen HTTP-Protokolls zu erhalten. Als Teil seiner Antwort kann ein Server beliebige Informationen senden, wie ein Cookie. Cookies sind kleine Datenpakete, die der Server an den Browser des Nutzers sendet. Dies geschieht über den sogenannten Set-Cookie-Header im Rahmen der Serverantwort. Diese beliebige Information kann alles sein: eine Benutzerkennung, ein Datenbankschlüssel, was auch immer der Server benötigt, damit er fortfahren kann, wo er aufgehört hat.

Im Bereich des Webtrackings werden in Cookies oftmals Informationen hinterlegt, die Aufschluss über das Surfverhalten und die Identität geben. Hierzu zählen unter anderem Geräteinformationen, persönliche Daten, Daten zum Nutzerverhalten und weitere.

Diese Informationen im Cookie bleiben mit der besuchten Seite assoziiert. Das bedeutet, wenn sich die IP-Adresse des Nutzers ändert, kann der Benutzer weiterhin identifiziert werden. [7]

First Party Cookies

Wenn nur der Webserver den der Nutzer besucht die Cookies liest und schreibt, spricht man in diesem Fall von First-Party-Cookies. Sie dienen in erster Linie dazu, Nutzer während des Besuchs auf der Webseite zu identifizieren und wiederzuerkennen. Interaktionen wie das Speichern von Warenkorbinhalten oder das Nachverfolgen von Seitenaufrufen sind Beispiele hierfür.

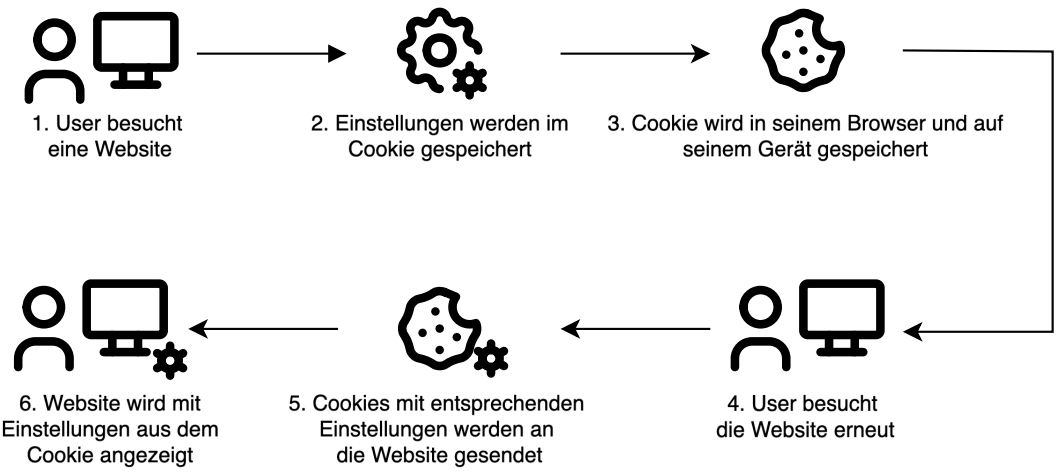

Abbildung 2.1: Entstehungsprozess von First Party Cookies

Third Party Cookies

Im Gegensatz zu First-Party-Cookies werden Third-Party-Cookies nicht vom Webserver selbst, sondern von sogenannten Dritanbietern gesetzt. Third-Party Cookies werden durch den Einsatz von Inhalten, eingebetteten Videos oder Tracking-Skripten im Browser des Nutzers hinterlegt.

Tracking-Pixel

Eine weitere Möglichkeit Daten der Nutzer zu erfassen stellt das Pixel Tracking dar. Beim Pixel Tracking wird ein meist 1x1-Pixel großes transparentes Bild auf der Webseite eingebunden.

> Zählpixel werden von Nutzern nicht wahrgenommen und haben für die Darstellung einer Webseite keine Bedeutung. Der einzige Zweck von Zählpixeln besteht darin, dass der Browser des Nutzers Kontakt mit dem Tracker aufnimmt.

[5]
Das eingebundene Pixelbild ist demnach für den Nutzer selbst nicht sichtbar und hat die Aufgabe eine Verbindung zum Trackingserver herzustellen.

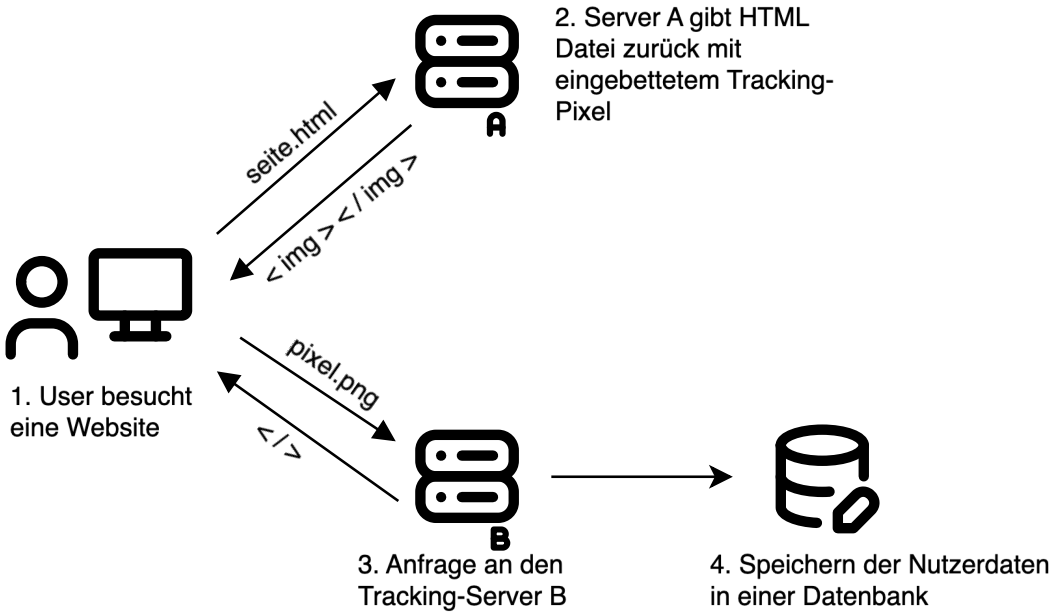

Abbildung 2.2: Ablauf von Tracking durch Tracking-Pixel

JavaScript

JavaScript wird als clientseitige Programmiersprache von 98,9% aller Websites verwendet. [8] In Anbetracht der Tracking-Domäne wird JavaScript häufig genutzt, um Tracking-Tags auf Webseiten zu implementieren und auszuführen. Hierbei handelt es sich oft um eine dynamische Implementierung, bei der Tags von Trackinganbietern wie z.B. Google direkt eingefügt oder unter Zuhilfenahme von Tag-Management-Systemen geladen werden. [9] Nachdem die Trackingfunktionalität hinterlegt worden ist, können Daten in Echtzeit erfasst und an den entsprechenden Server der Trackinganbieter gesendet werden. Auf der Webseite ist es dann möglich Ereignisse wie Klicks, Mausbewegungen und Scroll-Aktivitäten direkt zu erfassen.

Fingerprinting

Beim Fingerprinting wird seitens versucht der Tracker den Computer des Verbrauchers anhand von Systemeigenschaften und Konfigurationsaspekten von den Computern anderer Verbraucher zu unterscheiden. Als Metriken der Unterscheidung zählen unter anderem: - IP-Adressen - Browsererweiterungen - Browsereinstellungen - Browserfamilie und Browserversion - Betriebssysteme und Anwendungen - Hardware Eine Übersicht der verschiedenen Metriken und Aspekte ist auf der Website http://amiunique.org/ zu finden. Hier kann man ebenfalls den Selbsttest durchführen und betrachten, ob man unter den von amiunique vorhandenen Datensätzen einzigartig ist.

HTTP headers attributes	**Similarity ratio**	**Value**
1 - User agent	0.02 %	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
2 - Accept	21.12 %	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
3 - Content encoding	17.84 %	gzip, deflate, br, zstd
4 - Content language	1.13 %	de-DE,de;q=0.9, en-US;q=0.8, en;q=0.7
5 - Upgrade Insecure Requests	89.21 %	1
6 - Referer	10.31 %	https://www.google.com/

Tabelle 2.1: Test amiunique.org 15.02.2025

Die Tabelle zeigt Testdaten der HTTP-Header Attribute, welche von der Website amiunique.org erkannt werden. Darüber hinaus werden weitere 57 JavaScript Spezifikationen erhoben die ebenfalls darüber Aufschluss geben inwiefern das geprüfte Gerät anderen Datensätzen der Seite ähnelt. Der Test hat ergeben, dass das geprüfte Endgerät einzigartig unter 3409452 anderen Datensätzen ist und mittels Fingerprinting eindeutig identifizierbar is.

Anonymisierung und Pseudonymisierung
Die Anonymisierung und Pseudonymisierung sind zentrale Methoden im Datenschutz, insbesondere bei der Verarbeitung personenbezogener Daten. Beide Methoden beabsichtigen den Personenbezug von Daten zu verringern oder zu entfernen. Die Methoden unterscheiden sich maßgeblich in ihrer Umsetzung und in ihrer Bedeutung.

Anonymisierung
Die Anonymisierung verändert personenbezogene Daten so, dass sie nicht mehr oder nur mit unverhältnismäßig großem Aufwand einer bestimmten Person zugeordnet werden können. Hierbei werden alle Merkmale entfernt oder verfälscht, sodass kein Rückschluss mehr auf die Identität möglich ist. Ein vollständig anonymisierter Datensatz gilt nicht mehr als personenbezogen und unterliegt dadurch nicht unter die Datenschutz-Grundverordnung (DSGVO).

Beispiele für Anonymisierung:

- Entfernung von Namen, Adressen oder Geburtsdaten.
- Aggregation von Informationen, durch die Bildung von Altersklassen statt konkreter Geburtsdaten.
- Verzerrung von Daten, etwa durch Reduktion räumlicher oder zeitlicher Bezüge

Pseudonymisierung
Die Pseudonymisierung ersetzt direkte Identifikationsmerkmale (z. B. Name oder Adresse) durch ein Pseudonym, wie eine ID-Nummer oder einen Code. Die Zuordnung zwischen Pseudonym und Originaldaten wird durch zusätzliche Informationen (z. B. eine Schlüsseldatei) ermöglicht, die getrennt aufbewahrt werden müssen. Dadurch bleibt eine Re-Identifikation theoretisch möglich, weshalb pseudonymisierte Daten weiterhin unter die DSGVO fallen.

Beispiele für Pseudonymisierung:

- Ersetzung des Namens durch eine ID-Nummer oder einen erzeugten Hash-Wert.
- Speicherung der Zuordnungsmöglichkeit getrennt vom erhobenen Datensatz

2.4 Definition von Conversions

Conversions oder auch Zielvorhaben genannt, sind ein zentrales Konzept im Bereich der Web Analytics und sind ein wichtiges Werkzeug bei der Bewertung der Effektivität von digitalen Marketingmaßnahmen. Eine Conversion bezeichnet im Kontext des Web-Trackings die erfolgreiche Durchführung einer Aktion durch einen Website-Besucher. Diese Aktionen können je nach Zielsetzung variieren und sind z.B.:

- Ein Kauf im Onlineshop
- Das Ausfüllen und Absenden eines Kontaktformulars
- Die Anmeldung für einen Newsletter
- Der Download einer Datei oder eines Whitepaper
- Die Registrierung auf der Website

Conversion-Rate

Die Conversion-Rate ist eine wesentliche Kennzahl im Bereich der Web-Analytics und wird wie folgt berechnet:

$$Conversionrate = \left(\frac{AnzahlderConversions}{GesamtanzahlderBesucher} \right) * 100$$

Diese Kennzahl ermöglicht die Messung der Effektivität von Marketingmaßnahmen und Website-Optimierungen. Er hilft bei der Identifizierung von Schwachstellen und dient als datengetriebene Grundlage zur Verbesserung der Nutzererfahrung.

2.5 Tracking Prevention

Ad-Blocker

Adblocker sind Softwaretools oder Browsererweiterungen, die Online-Werbung identifizieren und blockieren, um Nutzern ein werbefreies Surferlebnis zu ermöglichen. Ihre Funktionsweise basiert auf drei Kernprinzipien:

1. **Filterlisten**
   Bei einem Seitenaufruf prüft der Adblocker die Inhalte unter Zuhilfenahme einer Zugriffsliste in Form einer Blacklist. Diese Liste enthält Informationen wie typische Bildgrößen von Werbeanzeigen, deren Positionen, relevante Schlagwörter, Dateinamen, Dateiformate und vieles mehr. Die genannten Merkmale werden seitens des Adblockers abgeglichen und potenzielle Werbeinhalte werden somit blockiert und dem Nutzer nicht weiter angezeigt. [10]

2. **Heuristische Analyse**
   Wenn ein Ad-Blocker kein spezifisches Muster durch die Filterliste feststellt, können heuristische Algorithmen eingesetzt werden, welche auf spezifische Merkmale wie JavaScript-Aufrufe oder Cookies mit auffälligen Namen reagieren.

3. **DNS- und Netzwerkfilterung**
   Einige Adblocker-Tools blockieren Werbung bereits auf Netzwerkebene, indem sie DNS-Anfragen an Werbedomains unterbinden oder HTTPS-Filter einsetzen

Laut BSI verhindern Ad-Blocker das Tracking von Nutzern, indem u.a. das Speichern von Cookies bestimmter Vermarkter blockiert wird. [11] Dies funktioniert durch das Erkennen und Unterbinden der Kommunikation zu den Tracking-Domains oder das Blockieren der dazugehörigen Trackingfunktionen der verschiedenen Adblocker. **Do-not-Track Header**

Der HTTP DNT (Do Not Track) Request-Header zeigt die Tracking-Präferenz des Nutzers an. Er ermöglicht es den Nutzern anzugeben, ob sie Datenschutz gegenüber personalisierten Inhalten bevorzugen. DNT ist zugunsten von Global Privacy Control veraltet. Diese wird den Servern über den Sec-GPC Header mitgeteilt und ist über navigator.globalPrivacyControl für Clients zugänglich. [12]

Global Privacy Control

Global Privacy Control (GPC) ist eine vorgeschlagene Spezifikation, die es Internetnutzern ermöglichen soll, Unternehmen ihre Datenschutzpräferenzen mitzuteilen, z. B. ob sie möchten, dass ihre persönlichen Daten verkauft oder weitergegeben werden oder nicht. Diese Spezifikation löst die Do Not Track Methodik ab und soll als weiterführender Mechanismus dienen. Bei der Funktionsweise von GPC sendet der Browser des Nutzer eine Flag in der HTML-Kopfzeile, das seitens der Webseiten erkannt werden kann. Obwohl große Medien wie die New York Times und Tech-Firmen wie Mozilla GPC unterstützen, ist die Verbreitung noch begrenzt. Kritiker bemängeln, dass viele Websites das Signal ignorieren, solange keine gesetzliche Verpflichtung besteht.

Browserseitige Trackingprevention

Browserbasierte Trackingprävention umfasst verschiedene technische Ansätze, um Nutzerdaten vor Cross-Site-Tracking zu schützen. Drei zentrale Systeme – Apples ITP, Mozillas ETP und Googles Tracking Prevention – zeigen unterschiedliche Strategien und Wirksamkeitsgrade. Nachfolgend wird auf die verschiedenen Ansätze der Anbieter eingegangen: **WebKit - Apples ITP**

Abbildung 2.3: Beispiel Apple ITP

Die intelligente Tracking-Verhinderung (ITP) von Safari, die von WebKit entwickelt wurde, ist ein Mechanismus zum Schutz der Privatsphäre, der das seitenübergreifende Tracking einschränken und gleichzeitig die Funktionalität der Website beibehalten soll. Die 2017 eingeführte ITP nutzt maschinelles Lernen und strenge Cookie-Richtlinien, um die Privatsphäre der Nutzer zu schützen, ohne den legitime Speicheranforderungen unnötig einzuschränken.

Hauptmerkmale von ITP:

1. Blockierung von Drittanbieter-Cookies:
   ITP blockiert standardmäßig alle Cookies von Drittanbietern und verhindert so, dass Werbetreibende Nutzer über verschiedene Websites hinweg verfolgen

können. Ausnahmen erfordern eine explizite Benutzerinteraktion über die Storage Access API, die einen begrenzten Cookie-Zugriff für Szenarien wie eingebettete Anmeldeformulare erlaubt.

2. Klassifizierung durch maschinelles Lernen:
   ITP analysiert das Surfverhalten (z. B. das Laden von Subressourcen, Weiterleitungen), um Domänen mit seitenübergreifendem Tracking-Potenzial zu identifizieren. Bei klassifizierten Trackern werden die Cookies sofort gelöscht, wenn der Nutzer innerhalb von 30 Tagen nicht mit ihnen interagiert hat.

3. Richtlinien zum Ablauf von Cookies:
   Cookies von Erstanbietern laufen nach 7 Tagen ab, wenn der Nutzer nicht aktiv mit der Website interagiert (z. B. sich anmeldet), was die Verfügbarkeit auf 24 Stunden nach der Interaktion verlängert. Cookies von URLs mit Tracking-Parametern (z. B. utm_source) verfallen nach 24 Stunden.

[13] **Gecko - Mozilla ETP**

Mozillas Enhanced Tracking Protection (ETP) ist ein datenschutzorientiertes Framework, das in die Gecko-Browser-Engine integriert ist und die Anti-Tracking-Funktionen von Firefox unterstützt. ETP wurde 2018 eingeführt und kontinuierlich weiterentwickelt. Es kombiniert eine geräteinterne Klassifizierung mit strengen Richtlinien zum Blockieren von Inhalten, um das seitenübergreifende Tracking zu begrenzen und gleichzeitig die Webkompatibilität zu erhalten.

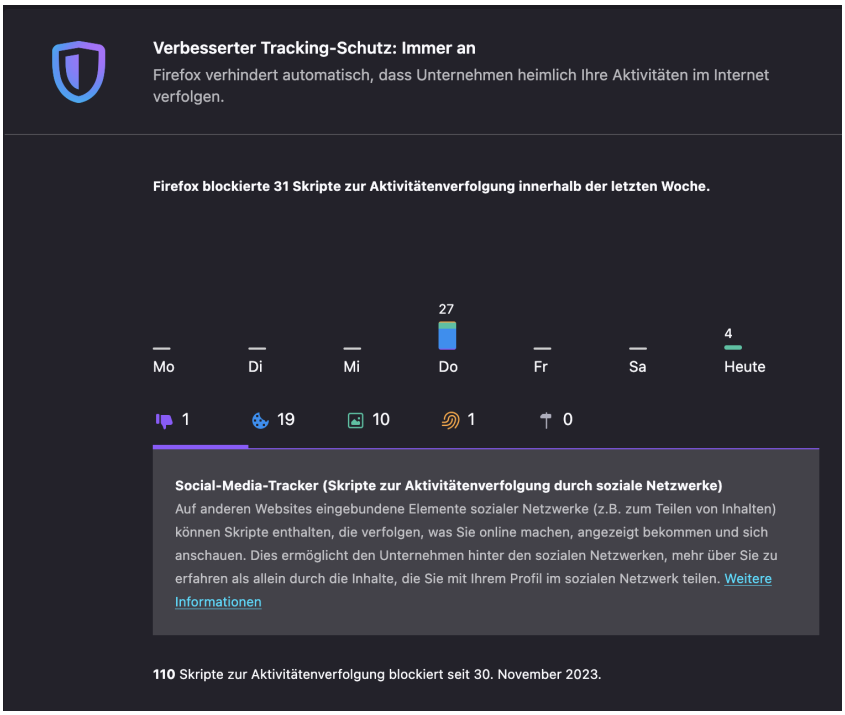

Abbildung 2.4: Beispiel Mozilla Enhanced Tracking Prevention

Hauptmerkmale von ETP:

1. Tracker-Klassifizierung:
   Verwendet Disconnect.me-Listen, um Domains zu identifizieren, die Social Media Tracking, Fingerprinting, Cryptomining und Cross-Site-Cookie-Nutzung betreiben. Blockiert standardmäßig Cookies von Drittanbietern und isoliert die verbleibenden Cookies über Total Cookie Protection, so dass sie auf ihre Ursprungswebsites beschränkt bleiben.

2. Blockierung von Inhalten:
   Blockiert Anfragen an Tracker-Domains in eingebetteten Inhalten (Werbung, Videos) mithilfe der integrierten Filterung von Gecko.

3. Automatische Löschung:
   Automatische Löschung von Cookies und Speicherplatz von klassifizierten Trackern nach 30 Tagen Inaktivität.

[14]

Chromium - Tracking Protection

Der Tracking-Schutz von Google Chrome ist eine Datenschutzfunktion, die das seitenübergreifende Tracking einschränken soll, indem der Zugriff auf Cookies von Drittanbietern standardmäßig eingeschränkt wird.

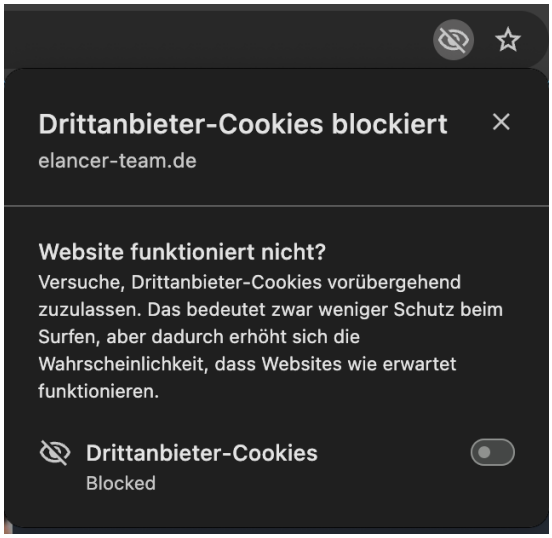

Abbildung 2.5: Beispiel Chromium Tracking Prevention

Hauptmerkmale der Tracking Protection:

1. Blockierung von Drittanbieter-Cookies:
   Schränkt den Zugriff auf Cookies von Drittanbietern ein und begrenzt so die Möglichkeit von Websites, Nutzer über verschiedene Websites hinweg zu verfolgen.

2. Schrittweise Einführung:
   Zunächst ab dem 4. Januar 2024 für 1 % der Chrome-Nutzer weltweit.

3. Umsetzung und Zeitplan:
   Q1 2024: Testphase beginnt mit 1 % der Chrome-Nutzer.
   Q3 2024: Geplante vollständige Abschaffung der Cookies von Drittanbietern, vorbehaltlich der Berücksichtigung von Wettbewerbsbedenken9.
   Anfang 2025: Beginn des Ausstiegs aus der Verwendung von Cookies von Drittanbietern für alle Nutzer.

Googles Ansatz beim Tracking-Schutz zielt darauf ab, ein Gleichgewicht zwischen der Verbesserung der Privatsphäre der Nutzer und der Aufrechterhaltung der Funktionalität des Internets zu finden, einschließlich der Werbe-Ökosysteme, die kostenlose Inhalte unterstützen. [15]

2.6 Tools und Frameworks

Es existieren verschiedene Tools und Frameworks, die unterschiedliche Ansätze zum Web-Tracking verfolgen. Nachfolgend werden gängige Softwarelösungen kurz vorgestellt.

Google Analytics

Google Analytics ist ein kostenloser Webanalysedienst von Google, der den Website-Verkehr verfolgt. Er ermöglicht es Websitebesitzern Einblicke in das Verhalten ihrer Besucher zu gewinnen einschließlich Metriken wie Seitenaufrufe, Sitzungsdauer, Absprungraten und weiteren. Google Analytics verwendet in Webseiten einen eingebetteten JavaScript-Code, um Daten zu sammeln, die dann verarbeitet werden und in verschiedenen Berichten und Dashboards angezeigt werden. Die Hauptmerkmale von Google Analytics sind:

- Datenverfolgung in Echtzeit
- Segmentierung von Zielgruppen
- Verfolgung von Konversionen
- Integration mit anderen Google-Diensten

Google Analytics unterstützt Unternehmen, datengestützte Entscheidungen zu treffen, um die Online-Präsenz und Marketingstrategien zu verbessern.

Matomo

Matomo, früher bekannt als Piwik, ist eine Open-Source-Webanalyseplattform, die eine Alternative zu Google Analytics darstellt. Die Tracking-Alternative bietet ähnliche Funktionen, setzt aber den Fokus auf Datenschutz und Nutzerkontrolle. Matomo kann im Einsatz selbst gehostet werden oder als Cloud-Service Verwendung finden. Die Hauptmerkmale von Matomo sind:

- Vollständige Datenhoheit und Datenkontrolle
- Anpassbare Dashboards und Berichte
- E-Commerce Verfolgung
- Tools zur Einhaltung der GDPR

Matomo wurde entwickelt um die Privatsphäre der Nutzer zu schützen und trotzdem einen detaillierten Einblick in den Website-Verkehr zu bieten.

Google Ads

Google Ads stellt eine Online-Werbeplattform für Websitebetreiber zur Verfügung. Es ermöglicht Unternehmen Anzeigen im Google Netzwerk zu schalten. Hierzu gehören die Suchergebnisse, Partner-Websites und YouTube. Die Hauptmerkmale von Google Ads sind:

- Pay-per-Click Werbemodell
- Keyword-basiertes Targeting
- Remarketing-Funktion
- Leistungsverfolgung und -optimierung

Google Ads bietet somit ein mächtiges Werkzeug, um potenzielle Kunden im Google Netzwerk zu erreichen und gezielt die Förderung von Conversions zu ermöglichen.

Meta-Pixel

Meta bietet für das Tracking im Kosmos des Unternehmens (Facebook, Instagram) den Meta Pixel an. Dies ist ein JavaScript-Code, der auf der Webseite platziert wird, um Nutzerinteraktionen und Konversionen von Meta Anzeigen zu verfolgen. Die Hauptmerkmale des Conversion Trackings von Meta zählen:

- Nachverfolgung bestimmter Ereignisse (z. B. Käufe, Anmeldungen)
- Erstellung benutzerdefinierter Zielgruppen für Retargeting
- Optimierung der Konversion
- Geräteübergreifende Verfolgung
- Integration mit Facebook Ads Manager

Das Meta Pixel unterstützt dabei die Customer Journey vom Anzeigenklick bis zur Konversion zu verstehen.

Google Tag Manager

Der Google Tag Manager ist ein kostenloses Tag-Management-System, mit dem verschiedene Tracking- und Marketing-Tags auf einer Webseite hinzugefügt werden können. Unter Zuhilfenahme des Google Tag Managers muss der bestehende Website-Code nicht angepasst werden, sondern die Anpassungen werden direkt durch die Tags injiziert. Die Hauptmerkmale des Google Tag Managers sind:

- Zentralisierte Verwaltung mehrerer Tags
- Einfache Implementierung von Tracking-Codes (z. B. Google Analytics, Facebook Pixel)
- Benutzerdefinierte Ereignisverfolgung
- Versionskontrolle und Debugging-Tools

Der Tag Manager von Google vereinfacht den Prozess der Implementierung und Verwaltung der verschiedenen Tracking- und Marketing Technologien auf einer Website.

2.7 Datenschutz

Datenschutz ist ein Grundrecht. Der Datenschutz ist in Anbetracht der Grundlagen des Webtrackings ein wichtiges und komplexes Thema, welches mit den in Kapitel 2 behandelten Technologien und Frameworks einhergeht. Generell gilt es klarzustellen, dass Datenschutz darauf abzielt, die Privatsphäre und persönliche Informationen von Nutzern im Web zu schützen. Im Trackingkontext hat dies zur Folge, dass die Thematik bestimmten Regeln und Einschränkungen unterliegt.

Datenschutzrechtliche Herausforderungen

Das Tracking von Nutzerdaten muss immer den jeweiligen Gesetzesgrundlagen entsprechen, was im deutschsprachigen Raum von der DSGVO geregelt wird. Die DSGVO stellt klare Anforderungen an die Verarbeitung von personenbezogenen Daten damit die Rechte von Nutzern bestmöglich geschützt sind. Nachfolgend sollen die Punkte die zentralen Aspekte und Problemstellungen verdeutlichen:

- **Einwilligung der Nutzer**
  Eine der größten Herausforderungen seitens des Webseitenbetreibers ist es die Einwilligung der Nutzer einzuholen. Das Einholen geschieht standardmäßig unter Zuhilfenahme eines Cookie-Banners. Das Cookie-Banner stellt hier ein zentrales Werkzeug dar, welches dafür zuständig ist den Nutzer über die Datenerhebung zu informieren und dem Nutzer eine Wahlmöglichkeit zu bieten.
- **Prinzip der Datensparsamkeit**
  Der Grundsatz der Datensparsamkeit bedeutet, dass nur unbedingt erforderliche Nutzerdaten seitens der Unternehmen erhoben werden sollen.
- **Einhaltung der Zweckbindung**
  Die Einhaltung der Zweckbindung beschreibt, dass die gesammelten Daten ausschließlich für den angegebenen Zweck gesammelt und verwendet werden dürfen.

Somit wird Tracking zu einer Disziplin Daten zu erfassen und eine Balance zu schaffen zwischen den wirtschaftlichen Interessen und den gesetzlichen Anforderungen. Im weiteren Verlauf der Arbeit werden stetig die geltenden EU Vorgaben beachtet und Prozesse so transparent wie möglich dargestellt.

2.8 Anwendungsgebiete von Trackingdaten

Erfolgsmessung von Marketingkampagnen

Um den Erfolg von Marketingkampagnen messen zu können ist Tracking eine unverzichtbare Quelle und liefert wichtige Einblicke über KPI-Metriken. Ferner ermöglicht die systematische Erfassung der Marketingkampagnen-Daten eine qualitative und quantitative Bewertungsgrundlage.

Optimierung von Webseiten und Zielvorhaben

Das Webtracking bietet eine fundierte Basis für Entscheidungen für die Weiterentwicklung und einer dynamischen Verbesserung von Inhalten. Darüber hinaus können Probleme identifiziert werden und Handlungsbedarf wird anhand der erhobenen Daten aufgezeigt.

Nutzerakquise und Geschäftsentscheidungen

Für den Bereich der Nutzerakquise sowie der übergeordneten Unternehmenssteuerung lassen sich die Trackingdaten als datengetriebene Grundlage verwenden. Trackingverfahren unterstützen hier bei der Nutzerakquise die wichtigsten Vertriebskanäle zu identifizieren durch das Erkennen der Nutzergruppen mit erhöhten Konversionsraten.

Somit bieten Trackingdaten eine evidenzbasierte Entscheidungsgrundlage und sind im Bereich des Digital Marketings in der heutigen Zeit nicht mehr wegzudenken.

3 Herausforderungen des clientseitigen Webtrackings

Das clientseitige Webtracking steht vor diversen Herausforderungen, die im folgenden Kapitel erläutert werden.

3.1 Auswirkungen auf die Performance

Der Einsatz von clientseitigem Tracking geht stets mit Auswirkungen auf die Performance einher. Da JavaScript-Skripte bei dem clientseitigen Tracking auf der Seite eingebunden werden, kann die Ladezeit verlangsamt werden und das Nutzererlebnis wird entsprechend beeinträchtigt.

Bei einem für diese Arbeit erstellten in-vitro-Testing wurden folgende Testparameter verwendet:

Browser-Engine	Chromium
Cache	Deaktiviert
Netzwerkeinstellung	Langsame 4G Verbindung 1.6 Mbt/s Download 0.75 Mbt/s Upload 150ms Latenz
Content-Encoding	deflate, gzip, br

Tabelle 3.1: In-Vitro Test Payload clientseitges Tracking

Auf der Seite der elancer-team GmbH wird der Tag Manager als Tag Management System verwendet, um die hinterlegten Tags von verschiedenen Anbietern zu steuern. Instanziiert durch den Google Tag Manager, werden maßgeblich die Tracking-Codes von Google Analytics, Google Ads und Microsoft Clarity bei dem Seitenaufruf geladen.

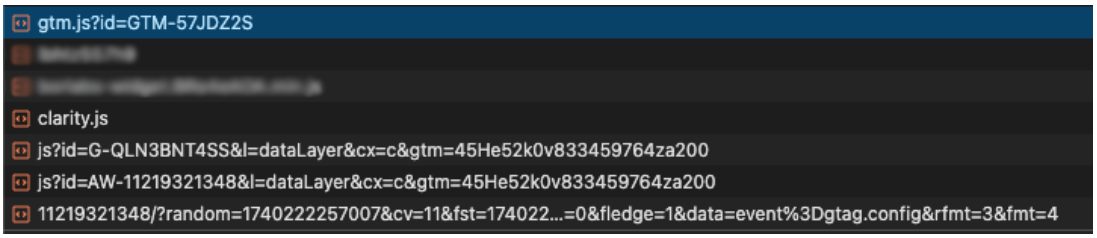

Abbildung 3.1: Relevante Tracking Skripte

Die in Abbildung 3.1 gezeigten Skripte weisen eine Gesamtreaktionszeit auf, die wie folgt berechnet werden kann:

$$\text{Gesamtreaktionszeit} = \begin{matrix} 1,18s_{(gtm.js)} + 0,73s_{(clarity.js)} + 1,95s_{(js?ID=G)} \\ +1,78s_{(js?ID=AW)} + 1,78s_{(googleads)} \end{matrix}$$

Wie aus den obigen Bildern zu entnehmen ist, erhöht sich die Gesamtreaktionszeit des Seitenaufrufs im simulierten 4G Netzwerk durch die Verwendung des Google Tag Managers und den verwendeten Tags insgesamt um 6.24 Sekunden erhöht.

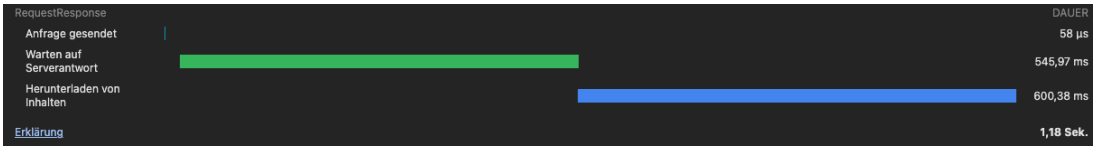

Abbildung 3.2: Payload gtm.js

Bei der Anfrage und der Serverantwort ist das Warten auf die Serverantwort jeweils ein nicht zu unterschätzender zeitlicher Anteil. Wie in Abbildung 3.2 zu sehen beträgt dieser Anteil 53,81 % des eigentlichen Payloads.

3.2 Auswirkungen von Tracking Preventions

Die unterschiedlichen Tracking-Preventions der verschiedenen Anbieter welche in Kapitel 2.5 erläutert wurden, haben einen Einfluss auf die Datenqualität und die Menge der erhobenen Daten. Durch die Begrenzung der Lebensdauer von First-Party-Cookies, die Reduzierung von Click-IDs oder der gesamten Blockierung von Tracking-Domains, erschwert dies die Erkennung wiederkehrender Nutzer und von Conversions. Darüber hinaus können unvollständige oder verzerrte Datensätze die Folge sein und Nutzer-Attributionen sind kaum noch möglich.

3.3 Herausforderungen für Unternehmen und Webagenturen

Für Webagenturen im Bereich der Digital Analytics stellt clientseitiges Tracking vor diverse Hürden und Herausforderungen dar. Misalignment und die eingeschränkte Personalisierung der Customer Journeys sowie die verminderte Genauigkeit von Marketing-Attributionen sind schwerwiegende Barrieren. Die Trackingdaten dienen dazu den Erfolg der Marketingstrategien und -kampagnen zu messen und bieten eine objektive Grundlage. Generell bestehen somit technische, rechtliche und praktische Probleme bei dem Einsatz von clientseitigem Tracking.

4 Server Side Tracking als Alternative

4.1 Konzept und Funktionsweise von Server Side Tracking

Serverseitiges Tracking ist eine Praktik der Datenerhebung im Online Marketing. Bei dieser Art der Datengewinnung findet die Verarbeitung der Nutzerdaten auf einem vom Website-Betreiber gehosteten Server statt. Grundlegend wird ein einzelner JavaScript-Code auf der Website hinterlegt, der für die Datenerhebung verantwortlich ist. Im Gegensatz zum clientseitigen Tracking werden die erhobenen Nutzerdaten nicht direkt an die Anbieter Google, Facebook und Co gesendet, sondern in erster Instanz gebündelt an den eigenen Webserver übertragen. Von dort aus lass sich diese dann kontrolliert an die jeweiligen Drittanbieter-Tools, wie zum Beispiel Google Analytics, weiterleiten.

Abbildung 4.1 veranschaulicht den Unterschied zum clientseitigen Tracking:

4.2 Vorteile des Server Side Trackings

Serverseitiges Tracking bringt einige Vorteile mit sich, die hier kurz aufgezeigt und erläutert werden:

1. **Keine Beeinflussung von Ad-Blockern und Tracking Preventions**
   Die Daten werden wie in Abbildung 4.1 gezeigt direkt an den Trackingserver gesendet und von dort aus zu den Analysetools. Somit haben Adblocker und browserbasierte Tracking-Preventions keinen Einfluss auf die Datenerfassung was zu einer zuverlässigen Erhebung führt.

2. **First-Party-Datenstrategie**
   Die Cookies werden innerhalb der Hauptdomain gesetzt und ermöglichen ein stabiles Fundament für eine First-Party-Datenstrategie. First-Party-Cookies sind im Grundsatz wesentlich robuster und werden im Zweifel nicht von Content-Blockern behindert.

3. **Cookieless Tracking**
   Durch den Einsatz von Datenstrategien und der Voraussetzung von eindeutigen Nutzermerkmalen kann eine eindeutige Nutzer-ID erzeugt werden und dem Nutzer entsprechend zugeordnet werden. Das Cookieless Tracking kann ebenfalls durch die Verwendung von kohortenbasierten Modellen oder über Login-Daten realisiert werden.

4. **Volle Datenkontrolle der Rohdaten**
   Serverseitiges Tracking macht es möglich genau festzulegen, welche Nutzerdaten erfasst und weiterverarbeitet werden. Dieser Umstand ermöglicht eine bessere

Einhaltung der DSGVO Datenschutzbestimmungen und lässt eine transparentere Kommunikation gegenüber der Websitenutzern zu.

5. **Performanceoptimierung**
   Wie in Abschnitt 3 beschrieben stellt clientseitiges Tracking einen zusätzlichen Verwaltungsaufwand für den Webserver dar, weil Tracking-Pixel und -Skripte jeweils Anfragen an die Drittanbieter-Server stellen. Dieser Umstand wird durch den Einsatz des serverseitigen Trackings unterbunden und die Website-Leistung wird erhöht.

6. **Datenanreicherung**
   Externe Datenquellen können genutzt werden um die Messdaten im serverseitigen Tracking anzureichern. Dies ist maßgeblich für E-Commerce-Unternehmen sinnvoll, bei denen Trackingdaten aus verschiedenen Quellen eingebunden werden. Mögliche externe Datenquellen können beispielsweise CRM oder ERP Systeme sein.

7. **Pseudonymisierung**
   Nutzerdaten können charakteristisch pseudonymisiert werden. Hier können zum Beispiel eine E-Mail-Adresse im Klartext in eine für außenstehende nicht nutzbaren Hash-Wert konvertiert werden. Diese umgewandelten Werte sind für Analysen weiterhin nutzbar und unterliegen seitens des Datenschutzes weniger strengen Regulierungen.

4.3 Nachteile des Server Side Trackings

1. **Komplexität der Implementierung**
   Die Implementierung von Server Side Tracking ist in der Regel komplexer als die des Client Side Trackings. Dies erfordert ein höheres Maß an technischem Fachwissen und Ressourcen. Das Einrichten und die Konfiguration des Servers, die Verbindung zur Website sowie die Evaluierung der Funktionalität muss bewältigt werden.

2. **Kosten**
   Für den Einsatz des serverseitigen Trackings wird ein Trackingserver benötigt, der für die Verarbeitung der Anfragen stetig Kosten verursacht. Darüber hinaus ist durch die komplexere Einrichtung der Methode mit höheren Entwicklungskosten zu rechnen.

3. **Verlust detaillierter Clientseitiger Daten**
   Ein wesentlicher Nachteil des Server Side Tracking ist, dass die clientseitiger Daten verloren gehen. Mit Clientseitigen Daten sind Verhaltensdaten wie Mausbewegungen, Scrollverhalten oder die Verweildauer gemeint. Diese Metriken sind nicht direkt Verfügbar, da diese im Browser des Nutzers entstehen und der Server an dieser Stelle keinen Zugriff darauf hat.

4. **Skalierbarkeitsherausforderungen**
   Die Hürden bei der Skalierbarkeit ergeben sich primär aus der Verarbeitung

und der Weiterleitung von größeren Datenmengen. Bei einer erhöhten Anzahl an Nutzeranfragen müssen Techniken wie die Lastenverteilung eingesetzt werden, um das Tracking und die Verfügbarkeit effizient zu gewährleisten.

5. **Datenschutzkonformität** Entgegen der häufigen Annahme führt Server Side Tracking nicht automatisch zu einer datenschutzkonformen Datenerhebung.

   Die DSGVO-Anforderungen bleiben bestehen, einschließlich der Einwilligungspflicht für bestimmte Datenverarbeitungen.

   Die Konfiguration muss sorgfältig vorgenommen werden, um personenbezogene Daten korrekt zu anonymisieren oder zu filtern.

   Bei der Nutzung von Cloud-Umgebungen US-amerikanischer Anbieter können Datenschutzprobleme auftreten.

4.4 Herausforderungen und Grenzen

Viele der zuvor genannten Nachteile des Server Side Trackings bergen Herausforderungen für die Implementierung. Darunter zählen Faktoren wie die technische Komplexität, die erhöhten Kosten, die Datenschutzkonformität und die Skalierbarkeitsherausforderungen. Somit ist eine sorgfältige Planung und Implementierung unerlässlich, um die Vorteile zu maximieren und die Herausforderungen effektiv zu bewältigen. Herausforderungen und Grenzen können unter anderem die nachfolgend gelisteten sein:

- Kein direktes Tracking von clientseitigen Technologien
- Serverseitiges Tracking kann nicht direkt auf Cookies im Browser zugreifen
- Daten wie die Client-ID und Session-ID müssen über Header, URL-Parameter oder POST-Daten aktiv vom Client mitgesendet werden
- Conversionereignisse müssen clientseitig getriggert und dezidiert an den Server geschickt werden.

5 Ansätze zur Modellierung von Server Side Tracking

5.1 Anforderungen an eine moderne Trackingstrategie

Eine aktuelle Trackingstrategie muss flexibel, skalierbar und robust sein, um den Anforderungen der heutigen digitalen Landschaft gerecht zu werden. Hier gilt es diverse Aspekte zu betrachten, um eine holistische Strategie anzuwenden, die in diesem Kapitel erläutert werden.

5.1.1 Technische Anforderungen

Die wichtigsten technischen Anforderungen, welche sich durch den Einsatz des serverseitigen Trackings abbilden lassen, sind:

Datenqualität und Genauigkeit
Wie in Kapitel 4 aufgezeigt bietet Server-Side Tracking eine höhere Datenqualität, da es nicht durch Adblocker oder Browser-Einschränkungen beeinträchtigt wird. Daten werden direkt auf dem Server verarbeitet, was die Konsistenz und Präzision erhöht.

Skalierbarkeit
Die gewählte Architektur sollte in der Lage sein auch größere Datenmengen effizient zu verarbeiten. Dies umfasst die Nutzung von Clustering, um auch höhere Lasten zu verteilen und zu bewältigen. Hosting-Optionen wie Google Cloud Platform, Microsoft Azure oder europäische Anbieter wie IONOS sind gängige Lösungen für die Server-Infrastruktur.

Flexibilität und Integration
Die verwendete Lösung sollte sich nahtlos in die bestehenden Systeme und genutzten Ökosysteme der Webseite einbinden lassen. Analyse-Frameworks, CRM-Plattformen und Marketingtools müssen sich gut integrieren lassen, was eine zentrale Datenverwaltung ermöglicht.

Performance
Durch das Auslagern des Trackings auf die Serverseite verbessert sich die Performance und somit die Ladezeit, was eine positive Auswirkung auf die Nutzererfahrung und das Suchmaschinenranking der Seite hat.

Fehlerresistenz
Generell gilt es die Trackingstrategie robust und ganzheitlich zu planen und aus-

zuführen. Darunter fällt auch ein etwaiger Schutz vor Angreifern und der Einsatz von Schutzmaßnahmen, um Ausfälle zu vermeiden.

5.1.2 Datenschutz und Compliance

Datenschutz ist ein zentraler Bestandteil moderner Trackingstrategien, insbesondere im Hinblick auf die Einhaltung von Vorschriften wie der DSGVO:

Datenminimierung und Anonymisierung: Server-Side Tracking ermöglicht es, sensible Daten vor der Weitergabe an Dritte zu anonymisieren und nur relevante Informationen zu speichern.

Zentrale Datenkontrolle: Durch die Verarbeitung auf dem eigenen Server behalten Unternehmen die volle Kontrolle über die Datenerhebung und -nutzung, was die Einhaltung von Datenschutzrichtlinien erleichtert.

Einwilligungsmanagement: Nutzer müssen transparent über die Datenerhebung informiert werden, und ihre Zustimmung muss eingeholt werden. Dies kann durch Consent-Management-Plattformen unterstützt werden.

Auswahl der Technologien: Bei der Wahl der geeigneten Technologien und Frameworks sollte ebenfalls den Datenschutz berücksichtigen:

5.2 Architektur und Datenfluss im Server Side Tracking

Ein typisches serverseitiges Tracking-System umfasst:

1. **Webserver:** Empfängt Benutzeranfragen und löst serverseitige Ereignisse auf der Grundlage von Aktionen aus.
2. **Ereignis-Sammelschicht:** Erfasst serverseitige Ereignisse, die vom Webserver generiert werden, unter Verwendung benutzerdefinierter Skripte oder spezieller Tools.
3. **Datenverarbeitungseinheit (optional):** Bereinigt, transformiert und bereichert die vom Server erzeugten Ereignisrohdaten vor der weiteren Verarbeitung. Dies kann das Herausfiltern irrelevanter Daten oder das Hinzufügen von Kontext wie Zeitstempel und Benutzer-IDs beinhalten.
4. **Worker-Prozess (optional):** Prozess im Hintergrund, der die Verarbeitung und das Senden von Server gesendeten Ereignissen an Analyseplattformen übernimmt und eine effiziente Datenverarbeitung ohne Beeinträchtigung der Leistung des Haupt-Webservers gewährleistet.
5. **Analyseplattform:** Der endgültige Bestimmungsort für verarbeitete, vom Server gesendete Ereignisse, z.B. wie Google Analytics oder Segment, die Einblicke in das Nutzerverhalten, die Marketingeffektivität und die Leistung der Website bieten.

5.3 Auswahl geeigneter Technologien und Frameworks

Frameworks und Tools

Framework/ Tool	Beschreibung	Vorteile	Nachteile
Server-Side Google Tag Manager (sGTM)	Ermöglicht die serverseitige Verarbeitung von Tags und Tracking-Events. Besonders geeignet für Unternehmen, die bereits im Google-Ökosystem arbeiten.	Einfache Integration mit Google Analytics und Ads, kosteneffizient.	Datenschutzbedenken bei der Nutzung von Google-Diensten.
JENTIS	Eine unabhängige Lösung aus Österreich mit Fokus auf Datenschutz. Unterstützt über 100 Tool-Integrationen und bietet Hosting innerhalb der EU.	Hohe Flexibilität, robuste Datenanreicherung, datenschutzfreundlich.	Höhere Kosten und komplexe Einrichtung.
Stape.io	Benutzerfreundliche Lösung für SST, basierend auf Google-Technologie.	Einfache Implementierung, kostengünstig.	Eingeschränkte Auswahl des Serverstandorts.
Piwik PRO	Datenschutzorientierte Plattform mit hybriden Tracking-Optionen.	Integrierte Module wie Consent Manager und Customer Data Platform.	Komplexe Konfiguration bei spezifischen Anforderungen.

Tabelle 5.1: Server-Side-Tracking-Frameworks und Tools im Überblick

Für Unternehmen mit bestehenden Google-Integrationen ist Google Server Side Tracking eine schnelle und kosteneffiziente Option. Datenschutzorientierte Organisationen sollten datenschutzkonforme Lösungen wie JENTIS oder Piwik PRO in Betracht ziehen. Für kleinere Teams mit begrenzten Ressourcen kann Stape.io eine geeignete Option sein.

Zusammengefasst hängt die Auswahl des richtigen Frameworks von den individuellen Anforderungen an Datenschutz, Skalierbarkeit und der technischen Expertise ab.

Die Entscheidung für serverseitiges Tracking mit Google Technologien als zentrale Lösung für die elancer team GmbH resultiert aus einer sorgfältigen Abwägung der bestehenden Systemlandschaft und der strategischen Ausrichtung des Unternehmens. Da die Agentur bereits umfassend in das Google-Ökosystem integriert ist und Tools wie Google Analytics, Google Ads sowie den Google Tag Manager produktiv nutzt, bietet sich die Nutzung der serverseitigen Tracking-Lösung von Google aus Gründen der technischen Kompatibilität und Effizienz.

Insbesondere der geringe Implementierungsaufwand und die Möglichkeit, bestehende Workflows ohne größere Umstellungen weiterzuführen, sprechen für diese Wahl. Die Lösung ermöglicht eine konsistente Datenverarbeitung und -weiterleitung innerhalb der bereits etablierten Infrastruktur und trägt somit zu einer hohen Systemstabilität und Performance bei. Darüber hinaus ist die datenschutzkonforme Umsetzung im gegebenen Anwendungsfall, beschränkt auf standardisierte Kontaktformulare und ohne Verarbeitung besonders schutzbedürftiger personenbezogener Daten, problemlos realisierbar.

Vor diesem Hintergrund stellt Google Server Side Tracking für die elancer team GmbH nicht nur die technisch und wirtschaftlich sinnvollste, sondern auch die strategisch sinnvolle Wahl dar. Die Lösung unterstützt die bestehende Digitalstrategie optimal und ermöglicht es dem Unternehmen, die Vorteile des serverseitigen Trackings effizient zu nutzen, ohne in komplexe oder kostenintensive Alternativsysteme investieren zu müssen.

6 Implementierung: Server Side Tracking Prototype

6.1 Technischer Aufbau des Tracking-Prototyps

Für die Implementierung des Tracking-Prototyps wurde auf die serverseitige Tracking-Lösung von Google zurückgegriffen. Grundlage hierfür war zum einen, dass die bestehende Firmenwebsite der elancer-team GmbH bereits auf Google-Dienste wie Google Analytics und den Google Tag Manager (GTM) nutzt. Zum anderen kann dadurch eine möglichst genaue Vergleichbarkeit zwischen dem client- und serverseitigen Ansatz gewährleistet werden. Auch persönliche Präferenzen im Umgang mit den Google-Technologien spielten bei der Wahl des Tracking-Stacks eine Rolle.

6.1.1 Containerbasierte Architektur

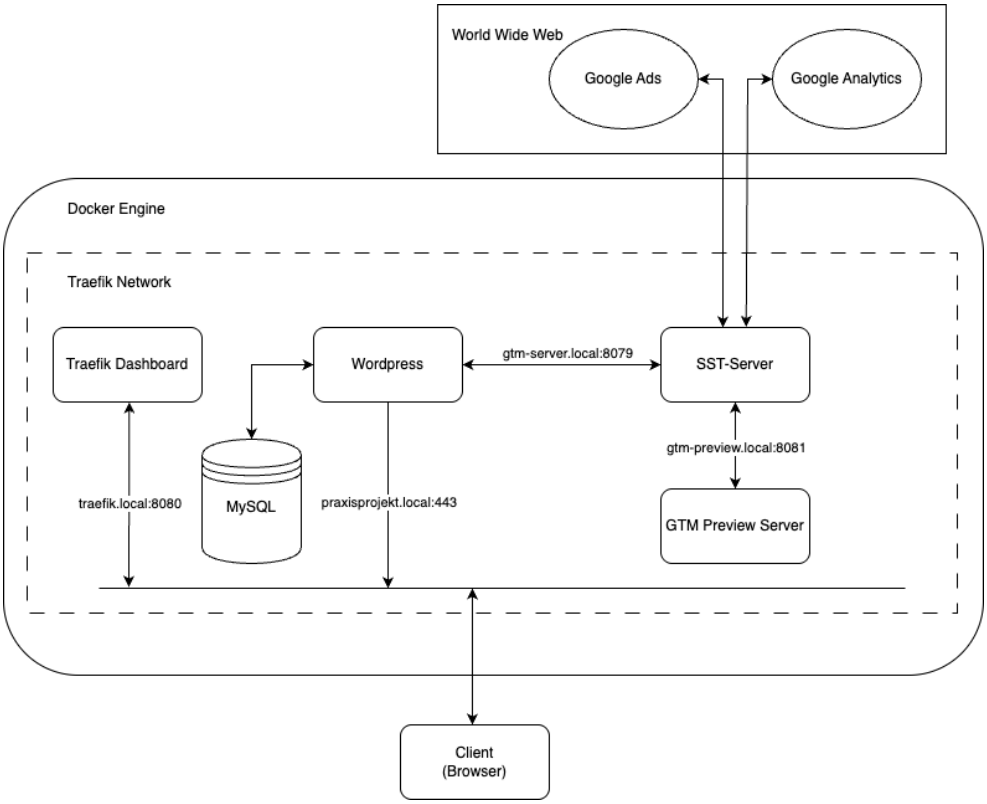

Abbildung 6.1: Architekturdiagramm Prototyp

Die technische Umsetzung des Prototyps erfolgte mittels einer containerbasierten Infrastruktur mit dem Einsatz von Docker. Durch die Nutzung von Docker kann eine reproduzierbare und lokale Umgebung aufgebaut werden, ohne dass hier die Verwendung eines externen Servers notwendig ist.
Das Setup umfasst fünf zentralen Containern, die für das serverseitige Tracking erforderliche Funktionalitäten bereitstellen:

- **Traefik:** Als Reverse Proxy übernimmt Traefik das Routing von HTTP-Anfragen an die jeweils zuständigen Container. Ferner wird der automatisierte Umgang mit SSL-Zertifikaten sowie das dynamische Service-Discovery ermöglicht.
- **GTM-Preview:** Dieser Container basiert auf dem offiziellen Google Tag Manager Preview Image (`gcr.io/cloud-tagging-10302018/gtm-cloud-image:stable`) und erlaubt das Testen und Debuggen von serverseitigen Tag-Konfigurationen in einer lokalen Umgebung.
- **SST-Server:** Der Server Side Tagging-Container fungiert als zentraler Endpunkt für Tracking-Anfragen. Eingehende Datenströme werden hier empfangen, verarbeitet und an Zielsysteme wie Google Analytics oder andere Drittanbieter weitergeleitet. Auch dieser Container basiert auf dem GTM-Image von Google.
- **WordPress:** Als zu analysierende Webpräsenz dient ein Container mit dem offiziellen WordPress-Image (`wordpress:latest`). In diesem wurde ein Klon der Firmenwebsite der elancer team GmbH integriert, um realitätsnahe Testszenarien zu ermöglichen.
- **MYSQL:** Die WordPress-Instanz greift auf eine MySQL-Datenbank (`mysql:5.7`) zurück, die in einem separaten Container betrieben wird und für die Speicherung der Website-Inhalte und Wordpress-Einstellungen sorgt.

Der Tracking-Prototyp wurde mittels einer `docker-compose.yml`-Datei definiert. Diese Datei beschreibt alle beteiligten Dienste, deren Konfigurationen sowie die zugrundeliegenden Netzwerke und Volumes. Im Folgenden ist die vollständige Konfigurationsdatei dargestellt:

```yaml
version: '3.8'

services:
  traefik:
    image: traefik:v2.9
    platform: linux/amd64
    container_name: traefik
    restart: always
    command:
      - --api.insecure=true
      - --api.dashboard=true
      - --providers.docker=true
      - --entrypoints.web.address=:80
      - --entrypoints.websecure.address=:443
      - --entrypoints.websecure.http.tls=true
      - --providers.file.filename=/config/dynamic.yml
```

```
    ports:
      - 8082:8080
      - 80:80
      - 443:443
    volumes:
      - /var/run/docker.sock:/var/run/docker.sock
      - ./certs:/certs
      - ./config:/config
    networks:
      - traefik_network
    labels:
      - traefik.enable=true
      - traefik.http.routers.traefik.rule=Host(`traefik.local`)
      - traefik.http.routers.traefik.entrypoints=websecure
      - traefik.http.routers.traefik.service=api@internal
      - traefik.http.routers.traefik.tls=true

  gtm-preview:
    image: gcr.io/cloud-tagging-10302018/gtm-cloud-image:stable
    platform: linux/amd64
    container_name: gtm-preview
    restart: always
    ports:
      - 8081:8081
    networks:
      - traefik_network
    environment:
      - CONTAINER_CONFIG=${CONTAINER_CONFIG}
      - RUN_AS_PREVIEW_SERVER=true
      - PORT=8081
      - HOST=0.0.0.0
    labels:
      - traefik.enable=true
      - traefik.http.routers.gtm-preview.rule=Host(`gtm-preview.local`)

      - traefik.http.routers.gtm-preview.entrypoints=websecure
      - traefik.http.services.gtm-preview.loadbalancer.server.port
    =8081
      - traefik.http.routers.gtm-preview.tls=true
      - traefik.http.routers.gtm-preview.service=gtm-preview

  sst-server:
    image: gcr.io/cloud-tagging-10302018/gtm-cloud-image:stable
    platform: linux/amd64
    container_name: sst-server
    ports:
      - 8079:8079
    networks:
      - traefik_network
    labels:
      - traefik.enable=true
      - traefik.http.routers.sst-server.rule=Host(`gtm-server.local`)
      - traefik.http.routers.sst-server.entrypoints=websecure
      - traefik.http.services.sst-server.loadbalancer.server.port=8079
      - traefik.http.routers.sst-server.tls=true
    environment:
```

```
      - CONTAINER_CONFIG=${CONTAINER_CONFIG}
      - PREVIEW_SERVER_URL=https://gtm-preview.local
      - PORT=8079
      - HOST=0.0.0.0

  wordpress:
    image: wordpress:latest
    container_name: wordpress
    platform: linux/amd64
    restart: always
    depends_on:
      - mysql
    networks:
      - traefik_network
    environment:
      - WORDPRESS_DB_HOST=mysql
      - WORDPRESS_DB_USER=wpuser
      - WORDPRESS_DB_PASSWORD=wppass
      - WORDPRESS_DB_NAME=wordpress
    volumes:
      - /Users/christiankrenn/Local Sites/praxisprojekt/app/public:/var
    /www/html
    labels:
      - traefik.enable=true
      - traefik.http.routers.wordpress.rule=Host(`praxisprojekt.local`)

      - traefik.http.routers.wordpress.entrypoints=websecure
      - traefik.http.routers.wordpress.tls=true

  mysql:
    image: mysql:5.7
    container_name: mysql
    platform: linux/amd64
    restart: always
    networks:
      - traefik_network
    environment:
      - MYSQL_ROOT_PASSWORD=rootpass
      - MYSQL_DATABASE=wordpress
      - MYSQL_USER=wpuser
      - MYSQL_PASSWORD=wppass
    volumes:
      - mysql_data:/var/lib/mysql

networks:
  traefik_network:
    driver: bridge

volumes:
  mysql_data:

```

Listing 6.1: docker$_c$*ompose.yml*

6.1.2 Zielsysteme und Datenspeicherung

Zur persistenten Datenhaltung der WordPress-Inhalte wird eine MySQL-Datenbankinstanz eingesetzt. Die statischen Websiteinhalte befinden sich in einem lokalen Verzeichnispfad auf dem Host-System und werden mittels eines Volume-Mounts in das Dateisystem des WordPress-Containers unter dem Pfad `/var/www/html` eingebunden. Dies ermöglicht dem Container den Zugriff auf die Webinhalte.

Der implementierte Prototyp übermittelt definierte Ereignisdaten an die Google Analytics-Plattform, nachdem diese zuvor durch den Tracking-Server empfangen und verarbeitet wurden. Als zentrale Plattform für die Analyse der serverseitig erfassten Tracking-Daten fungiert Google Analytics. Dieser Prozess beschreibt den Datenfluss des serverseitigen Trackingsystems.

6.1.3 Client-seitige Event-Erfassung

Für die clientseitige Ereigniserfassung wird ein Google Tag Manager (GTM) Web-Container verwendet. Dieser Container wird direkt in die Website implementiert und läuft im Browser des Nutzers. Wird beispielsweise eine Seite aufgerufen, löst ein entsprechend konfigurierter Trigger ein Tag aus, das ein Pageview-Ereignis erfasst und diese Information direkt aus dem Browser des Nutzers an den Tracking-Server im Traefik-Netzwerk.

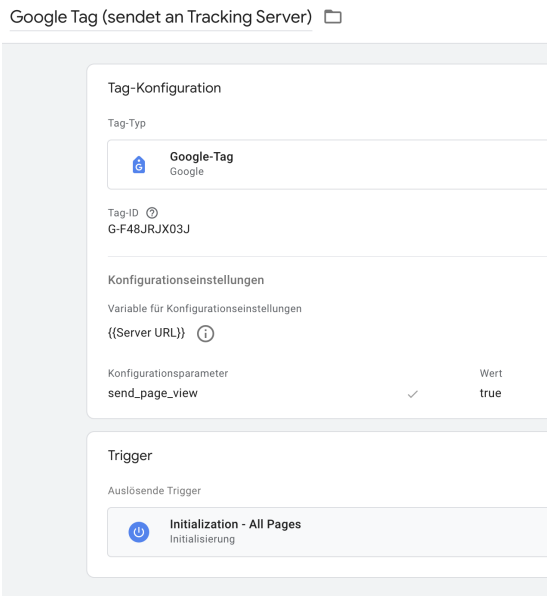

Abbildung 6.2: Konfiguration Google Tag

Wie in Abbildung 6.2 zu erkennen wurde ein Google-Tag definiert, welcher die Tag-ID der Analytics-Property beinhaltet und als Konfigurationseinstellung die Tracking-Server URL gesetzt ist. Als Konfigurationsparameter wird zur Veranschaulichung der page_view übergeben.

6.1.4 Server-seitige Verarbeitung der Events

Der im Docker-Container bereitgestellte Server empfängt die vom Webcontainer des Tag Managers übermittelten Tracking-Daten und leitet diese nach einer einfachen Verarbeitung an die Zielplattform, in diesem Fall Google Analytics, weiter.

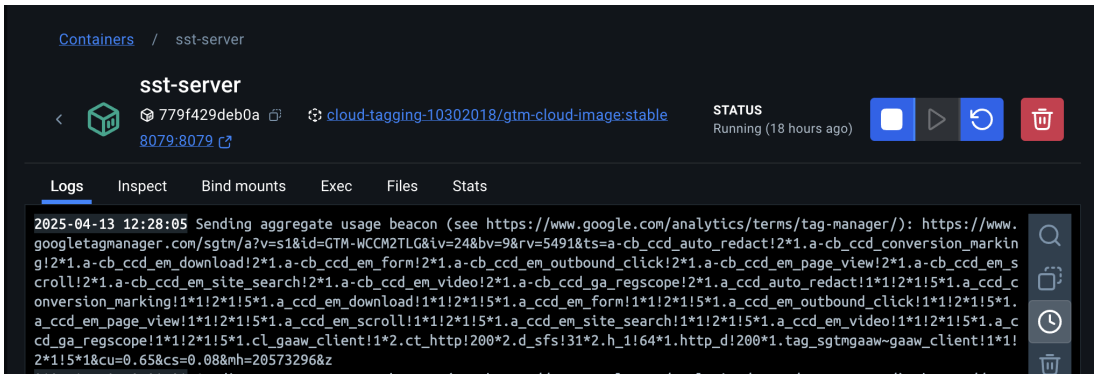

Abbildung 6.3: Logfile Server Side Tracking Server

Im Rahmen des Rapid Prototypings wurde auf eine weiterführende Transformation oder Anreicherung der Daten verzichtet. Die eingehenden Informationen werden in ihrer ursprünglichen Form an den Analyse-Dienst übermittelt.

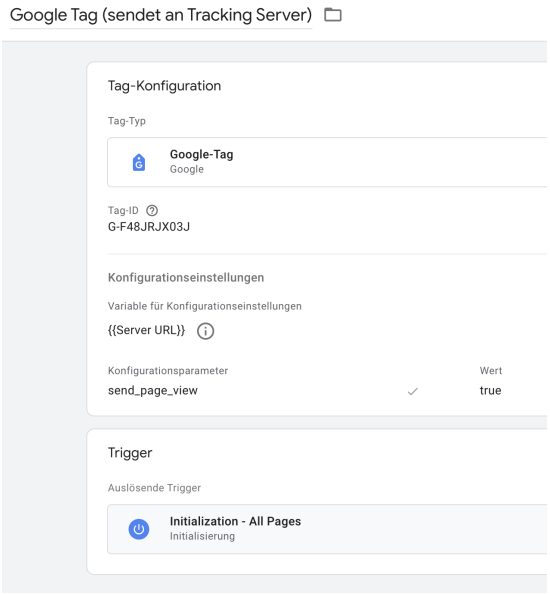

Abbildung 6.4: Konfiguration Google Tag

Im Debug-View von Google Analytics ist zu erkennen, dass das im serverseitigen Tag Manager definierte Event sst_ga4_triggered bei Analytics ankommt. Eine Ansicht des Debug-Views ist in Abbildung 6.5 veranschaulicht.

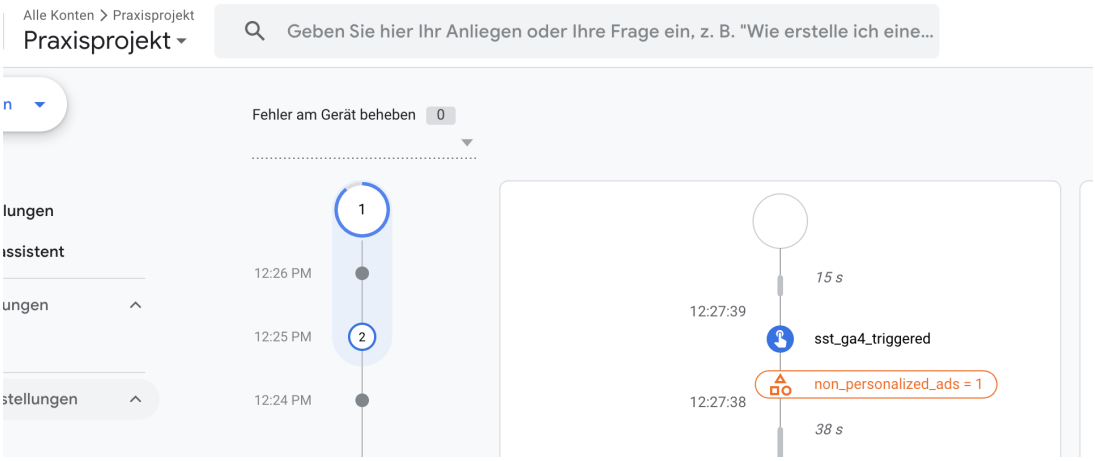

Abbildung 6.5: Debug View Google Analytics

7 Evaluation der Tracking Prevention

In diesem Kapitel dieser Arbeit wird die Effektivität der Tracking-Prevention-Maßnahmen verschiedener Webbrowser und Ad-Blocker im Hinblick auf die Umgehung durch serverseitige Tracking-Methoden untersucht. Ziel ist es, zu evaluieren, inwieweit aktuelle Tracking-Schutzmechanismen in der Lage sind, serverseitige Tracking-Ansätze zu detektieren oder zu blockieren.

7.0.1 Testaufbau und Methodik

Für die Durchführung der Tests wurde eine Kopie der Unternehmenswebsite der elancerteam GmbH erstellt, um eine praxisnahe und kontrollierte Testumgebung zu gewährleisten. In dieser Umgebung werden verschiedene Konfigurationen von Tracking-Schutzmaßnahmen getestet, wobei die gängigen Webbrowser Google Chrome, Mozilla Firefox und Apple Safari zum Einsatz kommen. Zusätzlich wird der Ad-Blocker uBlock Origin in das Testing einbezogen, um den Einfluss auf das serverseitige Tracking zu analysieren. Als zu messendes Tracking-Ereignis wird ausschließlich das Laden einer Seite `page_view)` erfasst. Dabei werden die Informationen des Browser-Navigators sowie weitere clientseitige Informationen, wie sie typischerweise im Rahmen serverseitigen Trackings übermittelt werden, aufgezeichnet.

7.0.2 Nutzereinwilligung und Vorgehen

Zur Einholung und Verwaltung der Nutzereinwilligung wird das Consent Management Tool Borlabs eingesetzt. Borlabs ist so konfiguriert, dass es den Google Consent Mode unterstützt und das Consent-Signal `analytics storage` für den Dienst Google Analytics übergibt. Nach Erteilung der Zustimmung durch den Nutzer wird das definierte Ereignis vom Webserver an den serverseitigen Tagging-Server (SST) weitergeleitet, wodurch eine datenschutzkonforme Signalübertragung
gewährleistet wird. Der Übertrag des Ereignisses findet durch den Einsatz eines Google Server Side Web-Container statt sowie einem JavaScript fetch Skript. Das verwendete JavaScript ist wie folgt aufgebaut:

```
fetch('https://gtm-server.local/collect', {
    method: 'POST',
    body: new URLSearchParams({
        v: '2',
        tid: 'G-F48JRJX03J',
        cid: 'debug.1',
        en: 'page_view'
    }),
    keepalive: true
});
```

Bei dem Testing selbst wird geprüft, ob die jeweiligen Browser die Verbindung nach Einwilligung des Consents zulassen oder Unterbinden. Der erste Test findet immer mit einer Kommunikation zum serverseitigen Tracking mittels Google Tag Manager Webcontainers statt. Sollte hier kein Ereignis beim Tracking Server ankommen, wird das Ereignis direkt per fetch Anfrage an den Server gesendet.
Zusammengefasst ist das Testing wie folgt aufgebaut:

Testumgebung	**Beschreibung**
Website	Klon der Firmenwebsite der elancer-team GmbH
Browser	Google Chrome, Mozilla Firefox, Apple Safari
Ad-Blocker	uBlock Origin; kein weiterer Ad-Blocker aktiv
Tracking-Ereignis	`page_view`; Übermittlung von `navigator`- und Client-Informationen
Consent Management	Borlabs CMP mit Google Consent Mode (`analytics_storage`)
Signalübertragung	Direkt an den Tracking-Server bzw. über GTM Webcontainer; Mit fetch Anfrage

Tabelle 7.1: Übersicht der Testumgebung zur Tracking Prevention

7.0.3 Testings

Google Chrome

Die Signalübertragung durch den GTM Webcontainer funktionierte im Chrome Browser ohne Einschränkungen, auch bei aktivierter Blockierung von Drittanbieter-Cookies. Chrome blockierte die Netzwerkverbindung zu den Endpunkten des webbasierten Google Tag Managers nicht, somit wurde auch die fetch-Anfrage ohne Probleme übermittelt.

Mozilla Firefox

Analog zu Chrome wurden im Firefox Browser die Signale erfolgreich an den Webcontainer unter Zuhilfenahme des webbasierten GTM und der fetch-Anfrage übermittelt.

Apple Safari

Im Gegensatz zu Chrome und Firefox blockierte Safari im Inkognito-Modus die Kommunikation zum Tag Manager vollständig. Dies verhinderte die Übermittlung von Signalen an Analytics. Mit dem Einsatz der fetch-Anfrage konnte jedoch das Signal an Analytics ohne Probleme übermittelt werden.

uBlock Origin

Bei aktiviertem uBlock Origin wurde die Domain des Tag Managers durch die integrierten Filterlisten erkannt und blockiert, wodurch sämtliche Signalübertragungen unterbunden wurden. Der Ad-Blocker hat ebenfalls das Senden mittels fetch-Anfrage unterbunden, da der Domainpfad /collect ebenfalls erkannt wurde.

Zusammenfassung der Testergebnisse

Die Ergebnisse zeigen deutliche Unterschiede im Blockierungsverhalten zwischen den Browsern und dem getesteten Ad-Blocker. Bemerkenswert ist, dass nur Apples ITP in Safari die webbasierte GTM-Kommunikation blockierte, während Chrome und Firefox dies nicht taten. Dies könnte darauf zurückzuführen sein, dass Browser den GTM differenziert behandeln, da er nicht ausschließlich für Tracking-Zwecke verwendet wird, sondern auch für andere Funktionalitäten wie Schema-Markup-Implementierung oder Chat-Integrationen.

Die Untersuchung zeigt, dass zur Umgehung von Ad-Blockern mit Filterlisten ein Proxy-Server implementiert werden könnte, der Anfragen von alternativen Domainpfaden z.B. /api an die eigentlichen Tracking-Endpunkte wie /collect weiterleitet. Diese Methode würde die heuristischen Mechanismen moderner Blockierungstechnologien umgehen.

Zusammenfassend verdeutlicht dieses Testing die Komplexität des Tracking-Ökosystems und die Variabilität der Blockierungsmechanismen. Entwickler und Analysten sollten diese Faktoren berücksichtigen und eine Balance zwischen legitimen Analysebedürfnissen und dem Respekt für Nutzerentscheidungen anstreben.

8 Ausblick

8.1 Ausblick auf zukünftige Entwicklungen und offene Fragestellungen

Die Welt des Online-Trackings und datengetriebenen Marketings steht vor einem grundlegenden Wandel. Mit dem schrittweisen Verschwinden von Third-Party-Cookies und strengeren Datenschutzanforderungen müssen Unternehmen ihre Strategien neu ausrichten und gleichzeitig das Vertrauen der Nutzer gewinnen.

Wegfall der Third-Party-Cookies
Mit dem Wegfall von Third-Party-Cookies verlagert sich der Fokus eindeutig auf First-Party-Daten. Ein vielversprechender Ansatz besteht darin, auf direkt erhobene Nutzerdaten zurückzugreifen, etwa solche, die durch freiwillige Angaben oder durch Interaktionen innerhalb eigener Systeme gewonnen werden. Diese Daten sind direkt kontrollierbar und eher konform mit Datenschutzbestimmungen. Unternehmen müssen daher robuste Mechanismen zur Sammlung von First-Party-Daten implementieren und diese für personalisierte Empfehlungen nutzen.

Transparenz und Vertrauen als Erfolgsfaktoren
Das Vertrauen der Nutzer wird zu einem kritischen Erfolgsfaktor. Aktuell glauben gerade einmal 19% aller Deutschen, ihre Daten im Internet seien im Allgemeinen sicher. [16] Dieses tiefgreifende digitale Misstrauen muss durch eine neue, transparente Herangehensweise überwunden werden. Die transparente Erhebung und Verarbeitung von Kundendaten ist von zentraler Bedeutung. In Bezug auf die Analyse des Nutzerverhaltens und den Umgang mit personenbezogenen Informationen ist höchste Sorgfalt geboten.

Regulatorische Entwicklungen
Die ePrivacy-Verordnung soll als Ergänzung zur DSGVO den Schutz der Vertraulichkeit der elektronischen Kommunikation gewährleisten und den Datenschutz im digitalen Raum verbessern. Sie soll die Privatsphäre der Nutzer im Rahmen elektronischer Kommunikation schützen und die veraltete ePrivacy-Richtlinie ablösen. Die lang erwartete ePrivacy-Verordnung soll 2025 in Kraft treten, allerdings gibt es immer noch Uneinigkeiten zwischen den EU-Mitgliedstaaten und Interessenvertretern. Bis zur endgültigen Verabschiedung gilt in Deutschland das TDDDSG, das die bisherige ePrivacy-Richtlinie in nationales Recht umsetzt.

Neue Tracking-Ansätze
In der cookielosen Zukunft entwickeln sich verschiedene alternative Tracking-Methoden:

Google plant für 2025 ein neues Tracking-Opt-In-System basierend auf digitaler Fingerabdrucktechnologie (Device Finger Printing). Ob diese Umsetzung mit der DSGVO konform ist, bleibt abzuwarten. Weitere Methoden umfassen Contextual Advertising, serverseitiges Tracking und kontextbezogene Werbung.

Ethische Fragen
Datengetriebenes Marketing in einer cookielosen Welt wirft fundamentale ethische Fragen auf. Unternehmen müssen Datenschutz als Grundprinzip in ihre Tracking-Strategien integrieren und gleichzeitig sicherstellen, dass ihre Tracking-Praktiken mit Datenschutzgesetzen übereinstimmen.

Ausblick
Die kommenden Jahre werden eine Phase intensiven Wandels im digitalen Marketing darstellen. Erfolgreiche Unternehmen werden diejenigen sein, die nicht nur technisch innovative Lösungen implementieren, sondern auch ethisch verantwortungsvoll agieren und das Vertrauen ihrer Nutzer gewinnen. Eine cookie-freie Zukunft wird den Ansatz des digitalen Marketings weitreichend verändern. Die Herausforderung besteht darin, ein Gleichgewicht zwischen effektivem Marketing und dem Schutz der Privatsphäre zu finden. Eine Aufgabe, die sowohl technologisches Know-how als auch ethisches Bewusstsein erfordert.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

[1] M. Brandt. (2017) Sie wissen, was du letzten sommer geklickt hast. Statista. [Online]. Available: https://de.statista.com/infografik/12252/tracking-reichweite-von-internet-unternehmen/

[2] M. Falahrastegar, H. Haddadi, S. Uhlig, and R. Mortier. (2016) Tracking personal identifiers across the web. Queen Mary University of London, University of Cambridge, Cambridge, UK. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-30505-9_3?fromPaywallRec=false

[3] M. Brandt. (2016) Google trackt mehr als 6 von 10 seitenaufrufen. Statista. [Online]. Available: https://de.statista.com/infografik/12252/tracking-reichweite-von-internet-unternehmen/

[4] U. B. Lehrstuhl für Privatsphäre und Sicherheit in Informationssystemen, "Untersuchung der wirksamkeit von cookie-bannern und tracking-diensten auf deutschsprachigen webseiten," 2022, die Studie wurde als Projekt des Lehrstuhls durchgeführt, ohne einzelne Autoren hervorzuheben. [Online]. Available: https://web.psi.uni-bamberg.de/tracker-scan-2022/

[5] S. Markus, E. Matthias, and S. Martin, "Web-tracking-report 2014," 2014. [Online]. Available: https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Web_Tracking_Report_2014.pdf

[6] S. Fiebrandt. (2016) What are cookies? what are the differences between them (session vs. persistent)? cisco. Abgerufen: 2017-07-01. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117925-technote-csc-00.pdf

[7] D. M. Kristol, "Http cookies: Standards, privacy, and politics," 2001. [Online]. Available: https://arxiv.org/pdf/cs/0105018

[8] W3Tech, "Usage statistics of javascript as client-side programming language on websites," 2025. [Online]. Available: https://w3techs.com/technologies/details/cp-javascript

[9] Google, "Google-tag mit gtag.js einrichten," 2024. [Online]. Available: https://developers.google.com/tag-platform/gtagjs?hl=de

[10] M. Angerstein, "Google-tag mit gtag.js einrichten," 2021. [Online]. Available: https://www.medienkompass.de/was-ist-ein-adblocker/

[11] B. für Sicherheit in der Informationstechnik, "Ad-blocker tracking," 2025-02-05. [Online]. Available: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Updates-Browser-Open-Source-Software/Der-Browser/Adblocker-Tracking/adblocker-tracking_node.html#:~:text=Ad%2DBlocker%20sollen%20au%C3%9Ferdem%20das,Werbebannern%20und%20Trackern%20verwaltet%20werden.

[12] M. Foundation, "Dnt," 2025. [Online]. Available: https://developer.mozilla.org/de/docs/Web/HTTP/Headers/DNT

[13] W. A. Inc., "Tracking prevention in webkit," 2023-04-27. [Online]. Available: https://webkit.org/tracking-prevention/#intelligent-tracking-prevention-itp

[14] M. Foundation, "Enhanced tracking protection in firefox for desktop," 2024-11-26. [Online]. Available: https://support.mozilla.org/en-US/kb/enhanced-tracking-protection-firefox-desktop

[15] Google, "New safety features in chrome for more protection," 2024-09-12. [Online]. Available: https://blog.google/products/chrome/google-chrome-safety-update-september-2024/

[16] G. Kaiser, "Was glauben sie, wie sicher sind ihre persönlichen daten im internet im allgemeinen?" 2024-01-01. [Online]. Available: https://de.statista.com/statistik/daten/studie/217842/umfrage/sicherheit-von-persoenlichen-daten-im-internet/