INF FAKULTÄT FÜR INFORMATIK

Der Webauftritt durchleuchtet:

das privatere, datensparsamere, nachhaltigere und IT-sicherere Web

SITSEC: DR3
05.07.2023

Jonas Morawietz
Bernhard Birnbaum
Meryem Lasri

Inhalt

1. Ergebnisse
   a. Evaluation der EDPS-Erweiterungen
   b. Evaluation der Blockiermaßnahmen
   c. Zusammenfassung der Website-Analysen
   d. Dynamische Analyse
2. Tabellarische Zusammenfassung
   a. Tools
   b. Referenzen
3. Aussicht

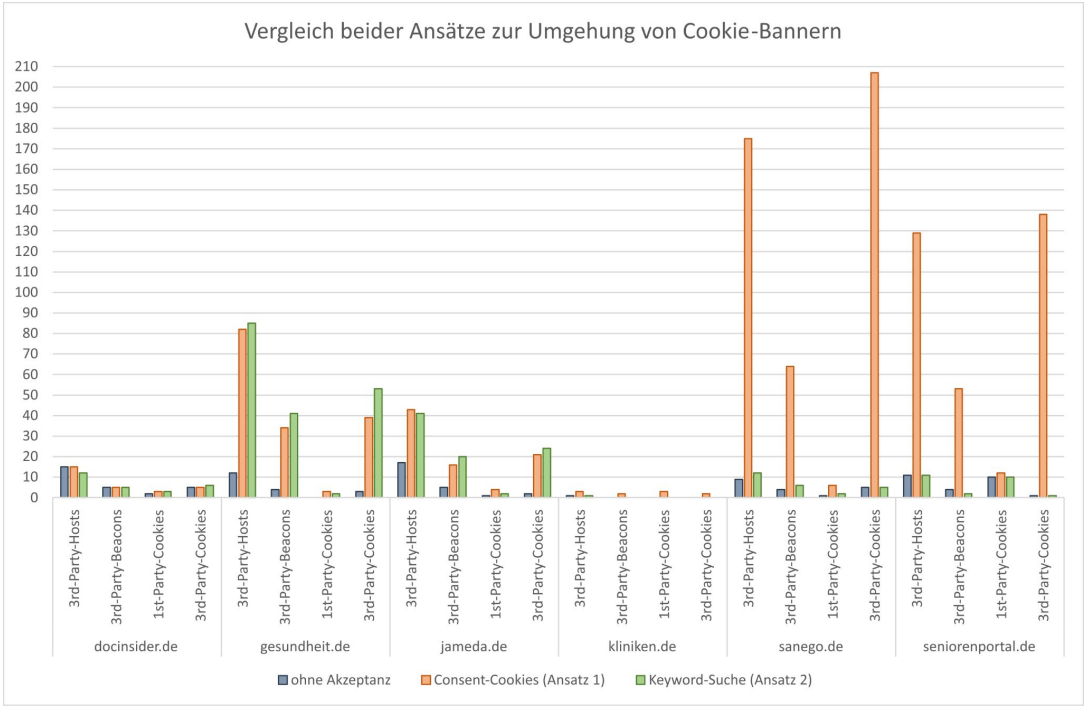
1. Ergebnisse: Evaluation d. EDPS-Erweiterungen

Ansatz 1: Consent-Cookies

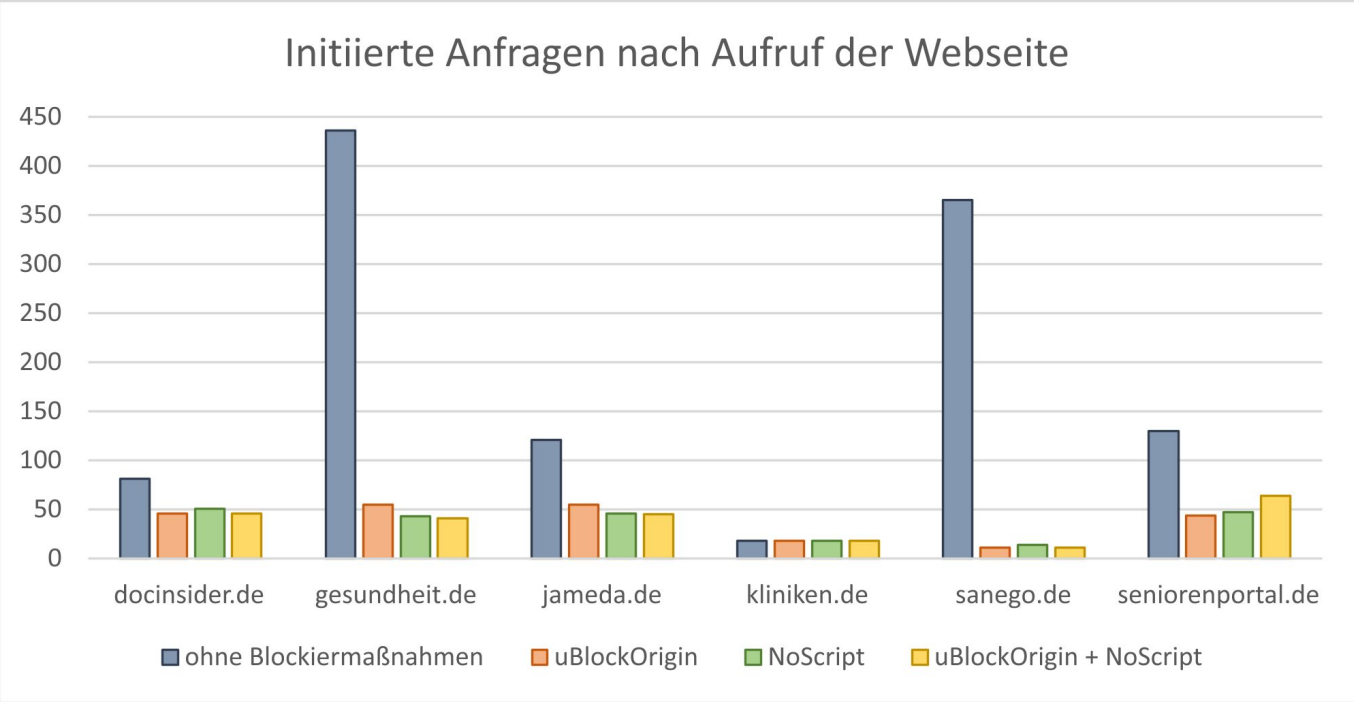
- manuelles Extrahieren der Consent-Cookies über Entwickler-tools von Firefox
- Übergabe der Consent-Cookies an den EDPS

Ansatz 2: Keyword-Suche

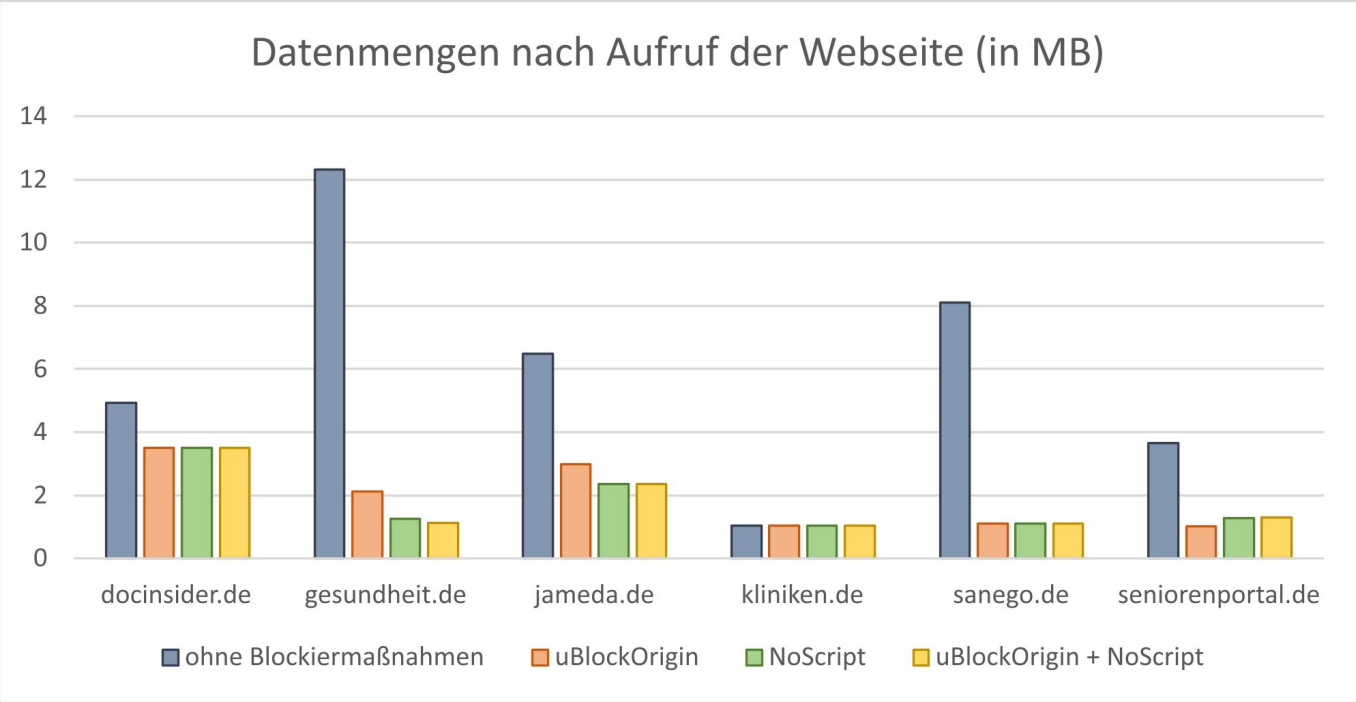
- EDPS wird manuell in Docker-Container mit Patch der “browser-session.js”-Datei gebaut
- implementierte Keyword-Suche versucht, den Accept-Button zu identifizieren und zu klicken



1. Ergebnisse: Evaluation d. Blockiermaßnahmen



1. Ergebnisse: Evaluation d. Blockiermaßnahmen



1. Ergebnisse: Zusammenf. der Website-Analysen

Webseite	Kurze Zusammenfassung der Ergebnisse
docinsider.de	*Drittanbieterbeteiligung*: 5 Tracker, lange Cookie-Dauer bis 790 Tage *IT-Sicherheit*: SWEET32-Angriff möglich, XFO und CSP-Header nicht gesetzt *Blockiermaßnahmen*: 7,45 MB mit 81 Anfragen → 5,44 MB mit 46 Anfragen
gesundheit.de	*Drittanbieterbeteiligung*: 34 Tracker, lange Cookie-Dauer bis 730 Tage *IT-Sicherheit*: HSTS nicht implementiert, CSP-Header und Referrer-Policy nicht gesetzt *Blockiermaßnahmen*: 2.98 MB mit 436 Anfragen → 221.34 KB mit 41 Anfragen
jameda.de	*Drittanbieterbeteiligung*: 20 Tracker, Tracking-Pixel, lange Cookie-Dauer bis zu 730 Tage *IT-Sicherheit*: kein HTTP Public Key Pinning → **MITM-Angriffsvektor**, unzureichende XSS-Protection, SRI verletzt *Blockiermaßnahmen*: 2.10 MB mit 121 Anfragen → 806.79 KB mit 45 Anfragen
kliniken.de	*Drittanbieterbeteiligung*: 2 Tracker, lange Cookie-Dauer bis 790 Tage *IT-Sicherheit*: HSTS-preloading möglich, CSP-Header und Referrer-Policy fehlen *Blockiermaßnahmen*: 1,44 MB mit 18 Anfragen → 1,44 MB mit 18 Anfragen
sanego.de	*Drittanbieterbeteiligung*: 64 Tracker, Tracking-Pixel, sehr lange Cookie-Dauer bis zu 1838 Tage (*Amazon Adsystem*) *IT-Sicherheit*: kein HTTP Public Key Pinning → **MITM-Angriffsvektor**, unzureichende XSS-Protection, **Click-Jacking** möglich durch unzureichende CSP, SRI verletzt *Blockiermaßnahmen*: 2.82 MB mit 365 Anfragen → 468.51 KB mit 11 Anfragen
seniorenportal.de	*Drittanbieterbeteiligung*: 53 Tracker, lange Cookie-Dauer bis 1866 Tage *IT-Sicherheit*: HSTS nicht implementiert, XFO-Header,CSP-Header,X-Content-Type-Header und Referrer-Policy nicht gesetzt *Blockiermaßnahmen*: 1.21 MB mit 130 Anfragen → 452.12 KB mit 64 Anfragen

1. Dynamische Analyse

- DisconnectMe List einfügen:

```
#!/bin/bash

#Download DuckDuckGo tracker Radar list :
# wget https://github.com/duckduckgo/tracker-radar/archive/refs/tags/2022.12.zip

#Unzip the file and move it to /home/tester/AppDynamics/duckduckgo
# unzip /home/tester/Downloads/tracker-radar-2022.09.zip -d /home/tester/AppDynamics/-duckduckgo
curl -o /home/tester/AppDynamics/duckduckgo/DisconnectMe.txt --noproxy '*' https://raw.githubusercontent.com/disconnectme/disconnect-tracking-protection/master/entities.json

jq '.entities | to_entries[] | .value.properties[]' /home/tester/AppDynamics/duckduckgo/DisconnectMe1.json > /home/tester/AppDynamics/duckduckgo/DisconnectMe.txt
Get DuckDuckGo list
cd "/home/tester/AppDynamics/duckduckgo/tracker-radar-2022.09/domains/DE"

for file in *.json ; do
echo "$file" | sed "s/\.json//g"
done > "/home/tester/AppDynamics/Tracker/DDGList_domain.txt
echo "File containing JSON filenames successfully created"
```

2. Tabellarische Zusammenfassung: Tools

finale Werkzeugauswahl:

Titel	Link	Beschreibung
Testerstick	intern	rauscharme Untersuchungsumgebung
Website-Evidence-Collector (EDPS)	https://github.com/EU-EDPS/website-evidence-collector	automatisierte Analyse von Speicherung und Transfer von persönlichen Daten
ungoogled Chromium	https://github.com/ungoogled-software/ungoogled-chromium	Google Chrome without Google
PrivacyScore	https://privacyscore.org/	bewertet Websites hinsichtlich einer Reihe von Sicherheits- und Datenschutzfunktionen
webbkoll	https://webbkoll.dataskydd.net/	prüft, welche Datenschutzmaßnahmen eine Website ergriffen hat
Firefox ESR	https://www.mozilla.org/de/firefox/all/#product-desktop-esr	Webbrowser mit Netzwerkanalyse
NoScript	https://noscript.net/	Blockierung bzw. kontrollierte Freigabe von JavaScript
uBlockOrigin	https://ublockorigin.com/de	Open-Source-Werbeblocker mit Zusatzfunktionen
Wireshark	https://www.wireshark.org/	Netzwerkprotokoll-Analyse und Entschlüsselung von Traffic (SSLKEYLOGFILE)
EDPS-Erweiterung von Tim Reiprich	https://gitlab.informatik.uni-halle.de/ajpqa/ovgu/	vollautomatischer Ansatz zur Umgehung von Cookie-Bannern

2. Tabellarische Zusammenfassung: Referenzen

Wissensbasis:

Titel	Quelle
[AKL+20] Introduction to Being a Privacy Detective: Investigating and Comparing Potential Privacy Violations in Mobile Apps Using Forensic Methods	ISBN 978-1-61208-821-1, pp 60-68, 2020
[Rie23] GitHub - EU-EDPS/website-evidence-collector: The tool Website Evidence Collector (WEC) automates the website evidence collection of storage and transfer of personal data.	https://edps.europa.eu/edps-inspection-software_en
tshark(1) Manual Page	https://www.wireshark.org/docs/man-pages/tshark.html
How to convert .img to usable VirtualBox format	https://superuser.com/questions/554862/how-to-convert-img-to-usable-virtualbox-format
Tim Reiprich: Automatisierter Ansatz zur Cookie-Banner-Akzeptanz basierend auf Keyword-Suche	https://gitlab.informatik.uni-halle.de/ajpqa/ovgu/

3. Aussicht

- Draft finalisieren
- Ausblick für zukünftige Arbeiten:
  - EDPS: vollautomatischer Ansatz: Schlüsselwortsuche weiter ausbauen
  - Untersuchungsergebnisse könnten auf Windows abweichen

Danke für Ihre Aufmerksamkeit!

Ergebnistabelle ‘docinsider.de’

Werkzeug	Metrik	Ergebnisse
PrivacyScore 07.06.2023, 10:12	Drittanbieteranfragen	13 einzigartige Hosts
	Tracker	9 bekannte Tracker
	1st-Party Cookies	2 Kurzzeit-Cookies, 4 Langzeit-Cookies
	3rd-Party Cookies	1 Kurzzeit-Cookie, 1 Langezeit-Cookie von Tracker
	Verschlüsselung/HSTS	HSTS preloading Angriff möglich, TLS 1.2
	Mail-Verschlüsselung	SWEET32-Angriff möglich, Secure Client Re-Negotiation-Angriff möglich
	potentielle Schwachstellen	XFO-Header nicht gesetzt, CSP-Header nicht gesetzt, Referrer-Policy nicht gesetzt
webbkoll 07.06.2023, 10:13:37	Drittanbieteranfragen	62 Anfragen an 17 einzigartige Hosts
	Tracker	0 bekannte Tracker
	1st-Party Cookies	1 Cookie
	3rd-Party Cookies	1 Cookie
	Verschlüsselung/HSTS	TLS 1.2, HSTS implementiert, aber nicht für Subdomains
	Policies (Content-Security, Referrer)	CSP mit Fehlern implementiert
	Subresource Integrity	29 Objekte werden von Quellen ohne integrity- oder crossorigin-Attribut geladen
EDPS Website Evidence Collector 20.06.2023, 12:56:34	Drittanbieteranfragen	15 einzigartige Hosts
	Tracker	5 third-Party Web Beacons
	1st-Party Cookies	3 Cookies
	3rd-Party Cookies	5 Cookies
	Verschlüsselung/HSTS	Redirect zu HTTPS
	Social-Media-Einbindungen	Facebook
NoScript	nicht blockierbar ohne Funktionseinschränkungen	docinsider.de
	Datenmengen mit Blockierung	51 Anfragen mit 3,50 MB / 1,96 MB
uBlockOrigin	CNAME-Tracking	-
	Datenmengen mit Blockierung	46 Anfragen mit 3,50 MB / 1,96 MB
Firefox ESR	Datenmengen mit beiden/ ohne Blockierungen	ohne Blockierungen: 81 Anfragen mit 4,93 MB / 2,52 MB, mit beiden Addons: 46 Anfragen mit 3,50 MB / 1,96 MB
Wireshark	DNS-Anfragen	25 einzigartige Anfragen, 15 mit Blockiermaßnahmen
	Pakete $S \rightarrow C$	ohne Blockierungen: 1322 (2918 KB); mit Blockierungen: 661 (2155 KB)
	Pakete $C \rightarrow S$	ohne Blockierungen: 922 (129 KB); mit Blockierungen: 574 (53 KB)

Ergebnistabelle ‘gesundheit.de’

Werkzeug	Metrik	Ergebnisse
PrivacyScore 13.06.2023, 11:48	Drittanbieteranfragen	9 einzigartige Hosts
	Tracker	2 bekannte Tracker
	1st-Party Cookies	1 Kurzzeit-Cookie, 1 Langzeit-Cookie
	3rd-Party Cookies	0 Cookie
	Verschlüsselung/HSTS	HSTS nicht implementiert
	Mail-Verschlüsselung	SWEET32-Angriff möglich
	potentielle Schwachstellen	CSP-Header nicht gesetzt, Referrer-Policy nicht gesetzt
webbkoll 13.06.2023, 11:49	Drittanbieteranfragen	60 Anfrage an 9 einzigartige Hosts
	Tracker	0 Tracker
	1st-Party Cookies	2 Cookie
	3rd-Party Cookies	1 Cookie
	Verschlüsselung/HSTS	HSTS nicht implementiert
	Policies (Content-Security, Referrer)	CSP nicht implementiert, Referrers werden übermittelt
	Subresource Integrity	49 Objekte werden von Quellen ohne integrity- oder crossover-Attribut geladen
EDPS Website Evidence Collector 20.06.2023, 13:26:58	Drittanbieteranfragen	82 einzigartige Hosts
	Tracker	34 third-Party Web Beacons
	1st-Party Cookies	3 Cookies
	3rd-Party Cookies	39 Cookies
	Verschlüsselung/HSTS	Redirect zu HTTPS
	Social-Media-Einbindungen	Facebook, Twitter, Pinterest, Instagram
NoScript	nicht blockierbar ohne Funktionseinschränkungen	gesundheit.de
	Datenmengen mit Blockierung	43 Anfragen mit 1,25MB / 392,15KB
uBlockOrigin	CNAME-Tracking	-
	Datenmengen mit Blockierung	55 Anfragen mit 2,12MB / 492,80KB
Firefox ESR	Datenmengen mit beiden/ ohne Blockierungen	ohne Blockierungen: 436 Anfragen mit 12,31MB / 2,98MB, mit beiden Addons: 41 Anfragen mit 1,12MB / 221,34KB
Wireshark	DNS-Anfragen	162 einzigartige Anfragen, 22 mit Blockiermaßnahmen
	Pakete $S \rightarrow C$	ohne Blockierungen: 3144 (3502 KB); mit Blockierungen: 1574 (2345 KB)
	Pakete $C \rightarrow S$	ohne Blockierungen: 2910 (747 KB); mit Blockierungen: 1388 (162 KB)

Ergebnistabelle ‘jameda.de’

Werkzeug	Metrik	Ergebnisse
PrivacyScore 20.06.2023, 18:01	Drittanbieteranfragen	17 einzigartige Hosts
	Tracker	6 bekannte Tracker
	1st-Party Cookies	2 Langzeit-Cookies
	3rd-Party Cookies	1 Kurzzeit-Cookie von Tracker
	Verschlüsselung/HSTS	alle Objekte werden über HTTPS übertragen, TLS 1.2
	Mail-Verschlüsselung	SWEET32-Angriff möglich
	potentielle Schwachstellen	XFO-Header nicht gesetzt, X-XSS-Protection-Header nicht gesetzt, X-Content-Type-Header nicht gesetzt, Referrer-Policy nicht gesetzt
webbkoll 20.06.2023, 18:02:37	Drittanbieteranfragen	72 Anfragen an 17 einzigartige Hosts
	Tracker	4 bekannte Tracker (Analytics)
	1st-Party Cookies	2 Cookies
	3rd-Party Cookies	1 Cookie
	Verschlüsselung/HSTS	TLS 1.3, HSTS implementiert aber nicht für Subdomains
	Policies (Content-Security, Referrer)	CSP mit Fehlern implementiert, Referrers werden übermittelt
	Subresource Integrity	29 Objekte werden von Quellen ohne integrity- oder crossorigin-Attribut geladen
EDPS Website Evidence Collector 20.06.2023, 11:45:42	Drittanbieteranfragen	41 einzigartige Hosts
	Tracker	20 third-Party Web Beacons
	1st-Party Cookies	14 Cookies
	3rd-Party Cookies	12 Cookies
	Verschlüsselung/HSTS	Redirect zu HTTPS
	Social-Media-Einbindungen	keine
NoScript	nicht blockierbar ohne Funktionseinschränkungen	jameda.de, docplanner.com, sentry.io, maps.googleapis.com
	Datenmengen mit Blockierung	46 Anfragen mit 2.36 MB / 807.38 KB
uBlockOrigin	CNAME-Tracking	-
	Datenmengen mit Blockierung	55 Anfragen mit 2.98 MB / 994.57 KB
Firefox ESR	Datenmengen mit beiden/ ohne Blockierungen	ohne Blockierungen: 121 Anfragen mit 6.49 MB / 2.10 MB, mit beiden Addons: 45 Anfragen mit 2.36 MB / 806.79 KB
Wireshark	DNS-Anfragen	54 einzigartige Anfragen; 11 mit Blockiermaßnahmen
	Pakete $S \rightarrow C$	ohne Blockierungen: 2288 (2.923 MB); mit Blockierungen: 575 (995.813 KB)
	Pakete $C \rightarrow S$	ohne Blockierungen: 1519 (302.457 KB); mit Blockierungen: 298 (37.534 KB)

Ergebnistabelle ‘kliniken.de’

Werkzeug	Metrik	Ergebnisse
PrivacyScore 15.05.2023, 13:22	Drittanbieteranfragen	0 einzigartige Hosts
	Tracker	0 bekannte Tracker
	1st-Party Cookies	0 Cookies
	3rd-Party Cookies	0 Cookies
	Verschlüsselung/HSTS	HSTS preloading Angriff möglich
	Mail-Verschlüsselung	keine Schwachstellen
	potentielle Schwachstellen	CSP-Header nicht gesetzt, Referrer-Policy nicht gesetzt
webbkoll 15.05.2023, 13:38:17	Drittanbieteranfragen	0 Anfragen
	Tracker	0 bekannte Tracker (Analytics)
	1st-Party Cookies	0 Cookies
	3rd-Party Cookies	0 Cookies
	Verschlüsselung/HSTS	HSTS implementiert aber nicht für Subdomains
	Policies (Content-Security, Referrer)	CSP nicht implementiert, Referrers werden nicht übermittelt
	Subresource Integrity	nicht eingebunden, aber alle Ressourcen laden vom gleichen Ort
EDPS Website Evidence Collector 20.06.2023, 13:30:17	Drittanbieteranfragen	3 einzigartige Hosts
	Tracker	2 third-Party Web Beacons
	1st-Party Cookies	3 Cookies
	3rd-Party Cookies	2 Cookies
	Verschlüsselung/HSTS	Redirect zu HTTPS
	Social-Media-Einbindungen	Twitter, Facebook, LinkedIn
NoScript	nicht blockierbar ohne Funktionseinschränkungen	kliniken.de
	Datenmengen mit Blockierung	18 Anfragen mit 1,04MB / 404,79KB
uBlockOrigin	CNAME-Tracking	-
	Datenmengen mit Blockierung	18 Anfragen mit 1,04MB / 404,79KB
Firefox ESR	Datenmengen mit beiden/ ohne Blockierungen	ohne Blockierungen: 18 Anfragen mit 1,04 MB / 404,79 KB, mit beiden Addons: 18 Anfragen mit 1,04 MB / 404,79 KB
Wireshark	DNS-Anfragen	15
	Pakete $S \rightarrow C$	ohne Blockierungen: 354 (645 KB); mit Blockierungen: 354 (645 KB)
	Pakete $C \rightarrow S$	ohne Blockierungen: 322 (35 KB); mit Blockierungen: 322 (35 KB)

Ergebnistabelle ‘sanego.de’

Werkzeug	Metrik	Ergebnisse
PrivacyScore 22.06.2023, 14:14	Drittanbieteranfragen	6 einzigartige Hosts
	Tracker	3 bekannte Tracker
	1st-Party Cookies	3 Kurzzeit-Cookies, 4 Langzeit-Cookies
	3rd-Party Cookies	1 Kurzzeit-Cookie
	Verschlüsselung/HSTS	alle Objekte werden über HTTPS übertragen
	Mail-Verschlüsselung	Secure Client Re-Negotiation-Angriff möglich
	potentielle Schwachstellen	XFO-Header nicht gesetzt, X-XSS-Protection-Header nicht gesetzt, X-Content-Type-Header nicht gesetzt, Referrer-Policy nicht gesetzt
webbkoll 22.06.2023, 14:15:16	Drittanbieteranfragen	14 Anfragen an 10 einzigartige Hosts
	Tracker	3 bekannte Tracker (Analytics)
	1st-Party Cookies	7 Cookies
	3rd-Party Cookies	0 Cookies
	Verschlüsselung/HSTS	HSTS implementiert aber nicht für Subdomains
	Policies (Content-Security, Referrer)	CSP mit Fehlern implementiert, Referrers werden immer übermittelt
	Subresource Integrity	8 Objekte werden von Quellen ohne integrity- oder crossorigin-Attribut geladen
EDPS Website Evidence Collector 20.06.2023, 13:31:19	Drittanbieteranfragen	175 einzigartige Hosts
	Tracker	64 third-Party Web Beacons
	1st-Party Cookies	6 Cookies
	3rd-Party Cookies	207 Cookies
	Verschlüsselung/HSTS	Redirect zu HTTPS
	Social-Media-Einbindungen	Instagram, Facebook, YouTube, LinkedIn
NoScript	nicht blockierbar ohne Funktionseinschränkungen	sanego.de
	Datenmengen mit Blockierung	14 Anfragen mit 1.11 MB / 468.57 KB
uBlockOrigin	CNAME-Tracking	-
	Datenmengen mit Blockierung	11 Anfragen mit 1.11 MB / 468.49 KB
Firefox ESR	Datenmengen mit beiden/ ohne Blockierungen	ohne Blockierungen: 365 Anfragen mit 8.10 MB / 2.82 MB, mit beiden Addons: 11 Anfragen mit 1.11 MB / 468.51 KB
Wireshark	DNS-Anfragen	134 einzigartige Anfragen; 9 mit Blockiermaßnahmen
	Pakete $S \rightarrow C$	ohne Blockierungen: 4143 (3.78 MB); mit Blockierungen: 151 (486.586 KB)
	Pakete $C \rightarrow S$	ohne Blockierungen: 3380 (700.706 KB); mit Blockierungen: 140 (15.578 KB)

Ergebnistabelle ‘seniorenportal.de’

Werkzeug	Metrik	Ergebnisse
PrivacyScore 13.06.2023, 19:39	Drittanbieteranfragen	10 einzigartige Hosts
	Tracker	3 bekannte Tracker
	1st-Party Cookies	4 Kurzzeit-Cookies, 7 Langzeit-Cookies
	3rd-Party Cookies	0 Cookie
	Verschlüsselung/HSTS	HSTS nicht implementiert
	Mail-Verschlüsselung	SWEET32-Angriff möglich
	potentielle Schwachstellen	XFO-Header nicht gesetzt, CSP-Header nicht gesetzt, X-Content-Type-Header nicht gesetzt, Referrer-Policy nicht gesetzt
webbkoll 13.06.2023, 19:42	Drittanbieteranfragen	21 Anfrage an 10 einzigartige Hosts
	Tracker	2 bekannte Tracker (Analytics)
	1st-Party Cookies	11 Cookies
	3rd-Party Cookies	0 Cookie
	Verschlüsselung/HSTS	HSTS nicht implementiert
	Policies (Content-Security, Referrer)	CSP nicht implementiert, Referrers werden übermittelt
	Subresource Integrity	5 Objekte werden ohne integrity- oder crossorigin-Attribut geladen
EDPS Website Evidence Collector 20.06.2023, 13:33:42	Drittanbieteranfragen	129 einzigartige Hosts
	Tracker	53 third-Party Web Beacons
	1st-Party Cookies	12 Cookies
	3rd-Party Cookies	138 Cookies
	Verschlüsselung/HSTS	Redirect zu HTTPS
	Social-Media-Einbindungen	Facebook, Twitter
NoScript	nicht blockierbar ohne Funktionseinschränkungen	seniorenportal.de
	Datenmengen mit Blockierung	47 Anfragen mit 1,28 MB / 247,72 KB
uBlockOrigin	CNAME-Tracking	-
	Datenmengen mit Blockierung	44 Anfragen mit 1,02 MB / 274,26 KB
Firefox ESR	Datenmengen mit beiden/ ohne Blockierungen	ohne Blockierungen: 130 Anfragen mit 3,65 MB / 1,21 MB, mit beiden Addons: 64 Anfragen mit 1,30 MB / 452,12 KB
Wireshark	DNS-Anfragen	116 einzigartige Anfragen, 42 mit Blockiermaßnahmen
	Pakete $S \rightarrow C$	ohne Blockierungen: 3647 (2153 KB); mit Blockierungen: 1880 (1999 KB)
	Pakete $C \rightarrow S$	ohne Blockierungen: 2273 (1978 KB); mit Blockierungen: 745 (203 KB)