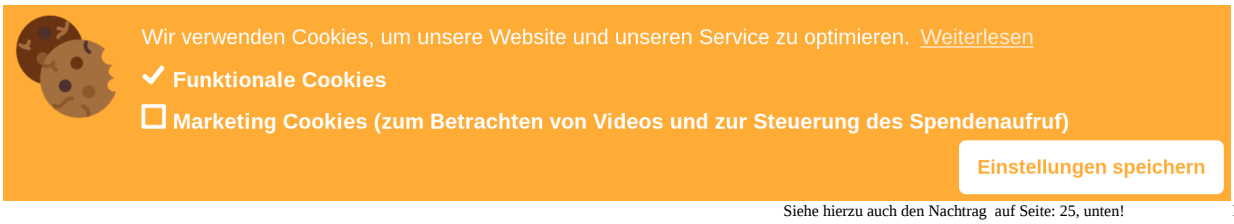
Cookies bei den newslichtern

Bettina Sahling , 2. Oktober 2019 — Keine Kommentare ↓

Auch bei den newslichtern braucht es nach einem bindenden Gerichtsurteil ab dem 1.10.2019 ein paar Clicks mehr, damit wir rechtlich bei den Cookies auf der sicheren Seite sind. Gerade das schauen von Videos ist nur noch möglich, wenn Du die Cookies-Einstellungen akzeptiert hast. Danke.



Siehe hierzu auch den Nachtrag auf Seite: 25, unten! Bild: 1

Sieht so ein Cookie-Banner aus „… *mit wirklicher Entscheidungsfreiheit* …“? Nicht wirklich!

Einstellungen speichern ? Niemals, aber was würde das bedeuten:

Zitat: […] **Wir sind frei zugänglich und verzichten bewusst auf klassische Werbung.** [...]

„Marketing Cookies (zum Betrachten von Videos und Steuerung des Spendenaufrufs)“?

Der Host: Paypal sieht nicht nach […] Betrachten von Videos und … Spendenaufruf [...] aus:

1.) Cookies von Dritten (2)

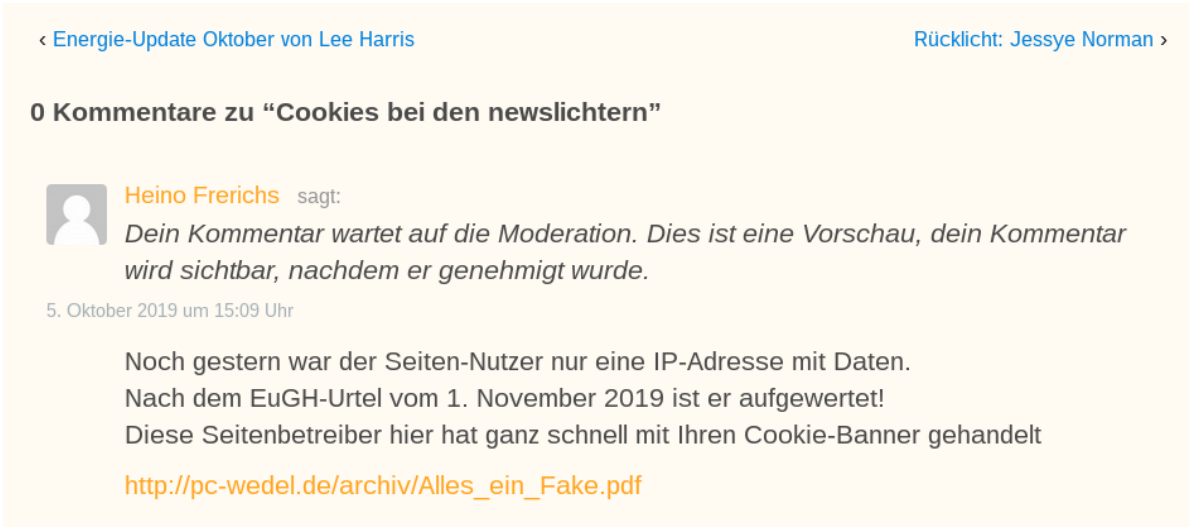
Domain	Name	Wert	Verfällt am
.abmr.net	01AI	2-2-B685BE374FEF0E1F...	2020-10-04 09:07:03Z
.paypalobjects.com	PYPF	CT-USR	2019-11-02 09:07:03Z

2.) Drittanfragen (Third Party)

5 Anfragen (5 sichere, 0 unsichere) bis **2** einmalige Hosts.

Ein "Third-party-request" ist ein Abruf von Ressourcen, die nicht von der Ursprungsdomain **`newslichter.de`** oder einer ihrere Subdomains kommen.

Host	IP	Land
ak1s.abmr.net • https://ak1s.abmr.net/is/www.paypalobjects.com?U=/de_DE/DE/i/btn/btn_d...	23.206.8.149	NL
www.paypalobjects.com • https://www.paypalobjects.com/de_DE/DE/i/btn/btn_donateCC_LG.gif?01AD=... • https://www.paypalobjects.com/de_DE/i/scr/pixel.gif • https://www.paypalobjects.com/de_DE/DE/i/btn/btn_donateCC_LG.gif • https://www.paypalobjects.com/de_DE/DE/i/btn/btn_donateCC_LG.gif	104.80.21.224	US



6.10.2019 12:32 / [….]Hallo lieber Webseitenbesucher der **newslichter.de,**

dein Kommentar auf der **newslichter-Webseite** und die Timeline bei pc-wedel.delässt schlimmes vermuten, aber zunächst mal danke für den Hinweis zu dem Paypal-Cookie. Als sorgsamer Wächter der eigenen Daten ist das beim Cookie-Scan durchgerutscht, da der Browser natürlich das no-track Flag gesetzt hat.
Die Trackingbilder von Paypal werden jetzt nicht mehr von Paypal und Akamai nachgeladen, insofern ist das schreierische PDF überflüssig. […].

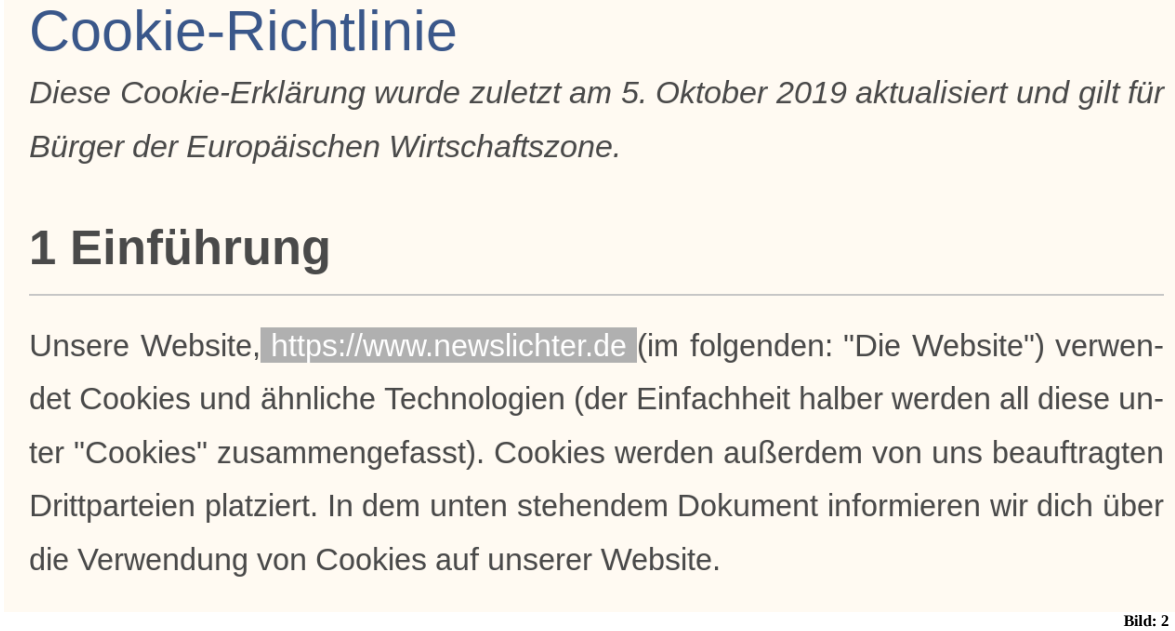


Bild: 2

Wer steht hinter newslichter.de?

Die Idee zu dem Magazin der guten Nachrichten hatte Bettina Sahling. Nach intensiver Planung und Vorbereitung ging newslichter.de im Oktober 2009 online. Ein Netzwerk an freien Mitarbeitern, Autoren und Befürwortern unterstützt seitdem die Herausgeberin tatkräftig. Die helfenden Hände, die klugen Köpfe und offenen Herzen machen den guten Geist des Projekts aus. Namentlich sei dafür Rolf Ahlborn, der Mann für alle Fälle der Webtechnik, genannt.

Bild: 3

Beispiel einer umfassenden Information

Über Cookies
Notwendige (3)
Präferenzen (0)
Statistiken (4)
Marketing (0)
Nicht klassifiziert (0)

(https://www.khh-legal.de/)

I.) **Notwendige Cookies** (3) helfen dabei, eine Webseite korrekt nutzbar zu machen, indem sie gundlegende Funktionalitäten wie Navigation oder Zugriffe auf sichere Bereiche der Webseite ermöglichen. Der Webseite ist nicht möglich ohne diese Cookies richtig zu funktionieren.

II.) **Statistik-Cookies** (4) helfen Webseiten-Inhabern zu verstehen, wie Sie als Besucher mit der Webseite interagieren und wie Sie sie benutzen, indem Informationen anonym gesammelt und beispielsweise an Analysetools gemeldet werden.

Zu I.) Notwendige Cookies: (https://www.khh-legal.de/)

Name	Anbieter	Zweck	Gespeicherte Daten	Ablauf	Typ
cookie_banner_14v	www.khh-legal.de	Speichert den Zustand über die getroffenen Auswahl im Cookie Banner.	ID der Cookiearten die man nicht akzeptiert hat, oder all falls alle akzeptiert wurde	1 Jahr	http
PHPSESSID	www.khh-legal.de	Behält die Zustände des Benutzers bei allen Seitenanfragen bei.	Zufällig generierte ID	Session	http
fe_typo_user	www.khh-legal.de	Behält die Zustände des Benutzers bei Seitenanfragen bei.	Zufällig generierte ID	Session	http

Zu II.) Statistik-Cookies: (https://www.khh-legal.de/)

Name	Anbieter	Zweck	Gespeicherte Daten	Ablauf	Typ
_ga	www.khh-legal.de	Registriert eine eindeutige ID, die verwendet wird, um statistische Daten dazu, wie der Besucher die Website nutzt, zu generieren.	Zufällig generierte ID	2 Jahre	http
_pk_id	www.khh-legal.de	Erfasst anonyme Statistiken über Besuche des Benutzers auf der Website, wie z. B. die Anzahl der Besuche, durchschnittliche Verweildauer auf der Website und welche Seiten besucht wurden.	Anzahl der Besuche, Verweildauer, Besuchte Seiten	1 Jahr	http
_pk_ref	www.khh-legal.de	Wird von Matomo Analytics Platform genutzt, um die Referring-Webseite zu identifizieren, über die der Besucher gekommen ist.	Webseitenadresse von der aus man gekommen ist	6 Monate	http
_pk_ses	www.khh-legal.de	Wird von Matomo Analytics Platform genutzt, um Seitenabrufe des Besuchers während der Sitzung nachzuverfolgen.	Zufällig generierte ID	Session	http

Drittanfragen (Third Party)

6 Anfragen (6 sichere, 0 unsichere) bis **3** einmalige Hosts.

Ein "Third-party-request" ist ein Abruf von Ressourcen, die nicht von der Ursprungsdomain **`khh-legal.de`** oder einer ihrere Subdomains kommen.

Host	IP	Land	Einordnung
code.jquery.com • https://code.jquery.com/jquery-migrate-1.2.1.min.js • https://code.jquery.com/ui/1.11.4/jquery-ui.js	209.197.3.24	US	
fonts.googleapis.com • https://fonts.googleapis.com/css?family=Source+Sans+Pro:400,300,600,20...	216.58.198.202	US	Content (Google)
fonts.gstatic.com • https://fonts.gstatic.com/s/sourcesanspro/v13/6xKydSBYKcSV-LCoeQqfX1RY... • https://fonts.gstatic.com/s/sourcesanspro/v13/6xK3dSBYKcSV-LCoeQqfX1RY... • https://fonts.gstatic.com/s/sourcesanspro/v13/6xKydSBYKcSV-LCoeQqfX1RY...	216.58.204.99	US	Content (Google)

Bild: 3

Nach Betätigen des Button

„ICH BIN EINVERSTANDEN“

wird unverändert wie Bild: 3 angezeigt:

Keine Cookies gefunden.

Kein Kommentar!

Kategorien der verwendeten Cookies (kraftknotenadapter.de)

Je nach Verwendungszweck und Funktion unterteilen wir die von der Website verwendeten Cookies in die folgenden Kategorien:

- Unbedingt erforderliche Cookies;
- Funktionale-Cookies;
- Performance-Cookies;
- Marketing- / Third Party- / Zustimmungspflichtige-Cookies

Marketing- / Third Party-Cookies

Marketing- / Third Party- / Zustimmungspflichtige-Cookies stammen unter anderem von externen Werbeunternehmen und werden verwendet, um Informationen über die vom Nutzer besuchten Websites zu sammeln, um z. B. zielgruppenorientierte Werbung für den Benutzer zu erstellen.

Auf unserer Webseite kommen folgende
Marketing- / **Third Party**- / Zustimmungspflichtige-Cookies zum Einsatz:

Name	Zweck	Laufzeit
__utma	Jimdo Statistikfunktion (Google Analytics)	2 Jahre
__utmb	Jimdo Statistikfunktion (Google Analytics)	1 Tag
__utmc	Jimdo Statistikfunktion (Google Analytics)	Session
__utmz	Jimdo Statistikfunktion (Google Analytics)	6 Monate
__utmt_b	Jimdo Statistikfunktion (Google Analytics)	1 Tag

Der Nutzer kann der Verwendung von Marketing-Cookies jederzeit widersprechen, indem er seine Cookie-Einstellungen entsprechend anpasst.

Drittanfragen (Third Party)

15 Anfragen (15 sichere, 0 unsichere) bis **6** einmalige Hosts.

Ein "Third-party-request" ist ein Abruf von Ressourcen, die nicht von der Ursprungsdomain **kraftknotenadapter.de** oder einer ihrere Subdomains kommen.

Host	IP	Land	Einordnung
a.jimdo.com			
• https://a.jimdo.com/app/web/loginstate?callback=jQuery1120043154838187...	54.171.136.184	IE	
assets.jimstatic.com			
• https://assets.jimstatic.com/bfa0b4b8941d94d9d6d8bc6fe31ef9f9.woff • https://assets.jimstatic.com/web.js.687c2004b33e517e5a54.js • https://assets.jimstatic.com/ckies.js.d8b51412786171ff7488.js • https://assets.jimstatic.com/web.css.935c0e9d85a10f52b2786792578fd18c....	151.101.122.2	FR	
fonts.jimstatic.com			
• https://fonts.jimstatic.com/s/roboto/v20/KFOmCnqEu92Fr1Mu4mxK.woff2 • https://fonts.jimstatic.com/s/roboto/v20/KFOlCnqEu92Fr1MmWUlfBBc4.woff... • https://fonts.jimstatic.com/s/roboto/v20/KFOlCnqEu92Fr1MmSU5fBBc4.woff... • https://fonts.jimstatic.com/css?family=Roboto%3Aregular%7CRoboto%3Areg... • https://fonts.jimstatic.com/css?family=Roboto:300,400,700|Roboto+Slab:...	151.101.122.2	FR	
image.jimcdn.com			
• https://image.jimcdn.com/app/cms/image/transf/dimension=140x10000:form...	151.101.122.2	FR	
u.jimcdn.com			
• https://u.jimcdn.com/cms/o/s50c59aa927d3ef39/userlayout/img/titel-rech... • https://u.jimcdn.com/cms/o/s0f3a2c4713008cb6/layout/dm_6d544d1f504d249... • https://u.jimcdn.com/cms/o/s50c59aa927d3ef39/userlayout/js/jquery-2-2-...	151.101.122.2	FR	
www.google-analytics.com			
• https://www.google-analytics.com/ga.js	216.58.201.238	US	Disconnect (Google)

Kein Kommentar!

01
OKT 2019

EuGH-Urteil: Cookie-Banner ohne Opt-In rechtswidrig

Viele Cookie-Banner erfüllen aktuelle Anforderungen nicht

Paukenschlag des Europäischen Gerichtshofs (EuGH): Mit Urteil vom 1. 10. 2019 (Az. C-673/17) hat das Gericht eine weit verbreitete Praxis zu Cookie-Hinweisen auf Webseiten für unzulässig erklärt. Ein Großteil der Webseiten auch von deutschen Anbietern dürfte aufgrund dieser Entscheidung datenschutzrechtlich zu beanstanden sein. Diese Webseiten müssen nun kurzfristig umgestaltet werden.

Welche Cookie-Hinweise der EuGH beurteilt hat

Dem EuGH war vom Bundesgerichtshof (BGH) u.a. die Frage vorgelegt worden, ob es ausreicht, wenn eine Webseite zwar auf die Verwendung von Cookies hinweist, nicht aber das Einverständnis des Besuchers der Webseite ausdrücklich erfragt.

Vielfach sind Webseiten nämlich so aufgebaut, dass

- der Besucher, also die „betroffene Person“, nur auf die Verwendung von Cookies hingewiesen wird („Unsere Webseite verwendet Cookies. Wir gehen von Ihrem Einverständnis aus, wenn Sie unsere Webseite nutzen.“)
- oder ein Cookie-Hinweis mit einem vorausgefüllten Kästchen (Checkboxen) angezeigt wird, das der Besucher abwählen muss, wenn er mit Cookies nicht einverstanden ist („Opt-Out“).

Der EuGH hat nun entschieden, dass diese beiden Varianten nicht den Anforderungen der EU-Datenschutzrichtlinie für elektronische Kommunikation entsprechen.

Besucher muss Cookies aktiv zustimmen

Gemäß EU-Recht (Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation [Datenschutzrichtlinie für elektronische Kommunikation]) muss der Betreiber einer Webseite – dazu gehören auch Onlineshops – vor dem Einsatz von Cookies, die auf dem Gerät des Besuchers installiert werden, die „Einwilligung der betroffenen Person“ einholen.

Dazu sei es erforderlich, dass ein Besucher seine Einwilligung aktiv erklärt, z.B. durch Klicken auf einen entsprechenden Button („Ja, ich bin mit dem Einsatz von Cookies einverstanden“), auch als „Opt-In“ bezeichnet.

Die bloße Nutzung einer Webseite oder die Möglichkeit zum Widerspruch genügen nicht als Einwilligung.

Zusätzlich: Information über Einsatzzweck nötig

Als weitere Voraussetzung für den Einsatz von Cookies sieht der EuGH vor, dass der Betreiber einer Webseite „gegenüber dem Nutzer hinsichtlich der Cookies u.a. Angaben zur Funktionsdauer und zur Zugriffsmöglichkeit Dritter machen muss“.

Ohne eine solche Information ist auch die aktiv erklärte Einwilligung unwirksam.

Anforderungen an die Gestaltung von Webseiten – handeln Sie jetzt!

Wie also müssen Webseiten gestaltet werden, die künftig rechtskonform Cookies einsetzen wollen? Sie müssen folgende Grundregeln beachten:

- Informieren Sie in Ihrem Cookie-Banner mindestens darüber,
    - welche Informationen mit Ihren Cookies gespeichert werden,
    - zu welchem Zweck Sie diese Informationen speichern,
    - ob Sie Dritten Zugriff auf die Cookies gewähren, es sich also um einen Third-Party-Cookie handelt,
    - wo der Besucher Ihre Datenschutzerklärung findet, um sich über Details zu informieren.
- **Lassen Sie dem Besucher Ihrer Webseite eine echte Wahl, sich für oder gegen die Speicherung von Cookies zu entscheiden**. Wenn Sie eine Checkbox für die Einwilligung verwenden, darf diese nicht vorausgefüllt sein. Die Voreinstellung muss immer ein Widerspruch gegen Cookies sein („Privacy by Default“).

Gericht stellt sich auch gegen „Hidden Identifiers“

Der EuGH stellt in seinem Urteil auch klar, dass die oben genannten Anforderungen nicht nur für solche Cookies gelten, die unmittelbar personenbezogene Daten speichern (Namen, Anschriften, E-Mail-Adressen etc.). **Vielmehr gelten die Anforderungen auf für Cookies, die „nur“ gerätebezogene Merkmale („Unique Hardware IDs“) oder zufällige, aber eindeutige Kennzeichen (z.B. eine Seriennummer) enthalten.**

Der EuGH begründet dies wie folgt: *„**Es macht keinen Unterschied, ob es sich bei den im Gerät des Nutzers gespeicherten oder abgerufenen Informationen um personenbezogene Daten handelt oder nicht.** Das Unionsrecht soll den Nutzer nämlich vor jedem Eingriff in seine Privatsphäre schützen, insbesondere gegen die Gefahr, dass „Hidden Identifiers“ oder ähnliche Instrumente in sein Gerät eindringen.“*

Autor

Franz Wegener / Rechtsanwalt /

Studium in Berlin, Warschau und Norwich (GB).

Weitere Auslandsaufenthalte in Polen und den USA. Zweites Staatsexamen 2005 in Hannover.

Tätigkeitsschwerpunkte:

Internetrecht/Onlinerecht, Urheber-, Marken- und Wettbewerbsrecht,
Datenschutz- und Softwarerecht, Gesellschaftsrecht.

Analyse einer Beschwerde:

06.10.2019 […] Beim irritierten durchstöbern der Senioren-Internetseite pc-wedel,
scheinen ja IT-Dienste angeboten zu werden, wenn man das rudimentäre Design versteht,
stellt man nach langem scrollen an polemischen Meinungsüberschriften fest,
dass das **Impressum** fehlt. Das findet man nur mit Hilfe einer Suchmaschine,
kommerziell oder nicht.
Spätestens hier kommt die Frage auf:
warum wird hier die newslichter-Webseite mit "Fake News" angekreidet,
nicht aber z. B. der Betreiber des Internet Cafes?

.

https://www.vhw-hamburg.de/seniorenresidenz-graf-luckner-haus.html

setzt ohne zu fragen Cookies, und hat einen nicht mehr passenden Cookie Banner.
Was will Heino, der freie IT Experte uns damit sagen? [...]

Ist das so:

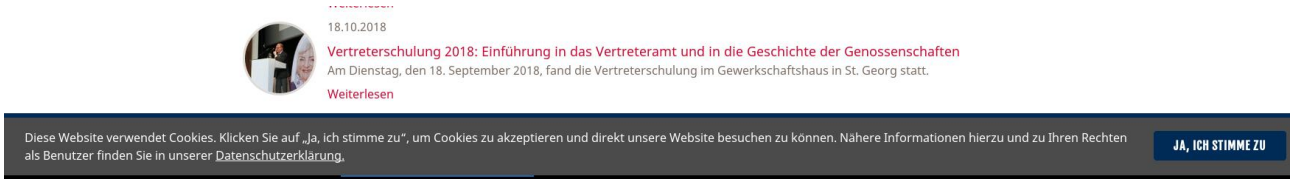


Bild: 1

Die angegebene WebSite bis auf die letzte Zeile gescrollt, der gezeigte Cookie-Banner (nicht verschiebbar) bleibt unveränderbar an der unteren Bildschirmdarstellung stehen. Bevor der Button: „**Ja ich stimme zu**“ angeklickt wird, braucht man die erforderlichen Informationen:

Bild: 2

Google Analytics kann man sich nicht „ins Boot holen“ ohne sich so gut wie möglich zu schützen! Es wird stark vermutet, dass hinter dem Cookies-Banner
noch mehr sichtbar(!) ist, also was nun?

Darum wird der Webbrowser entsprechen konfiguriert:

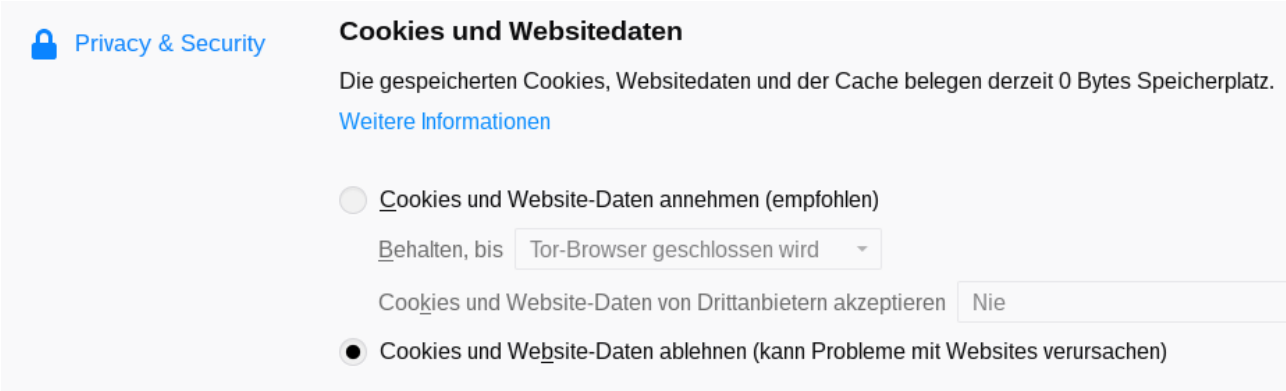


Bild: 3

Nach Neustart der WebSite bleibt Bild: 1 unverändert! Insofern erfolgt ein Neustart mit einem Life-System (Tails, Betriebssystem auf Linux basierend, siehe Anhang) und auf „**JA, ICH STIMME ZU**“ nach Bild: 1 ein Click:

Bild: 4

Mit einigen Internetkenntnissen hätten Sie, lieber Beschwerdeführer, wissen müssen, wo ich in Deutschland auf einer kommerziellen WebSite immer das **Impressum** finde (Bild: 4)!

vhw ... mehr als Wohnen!

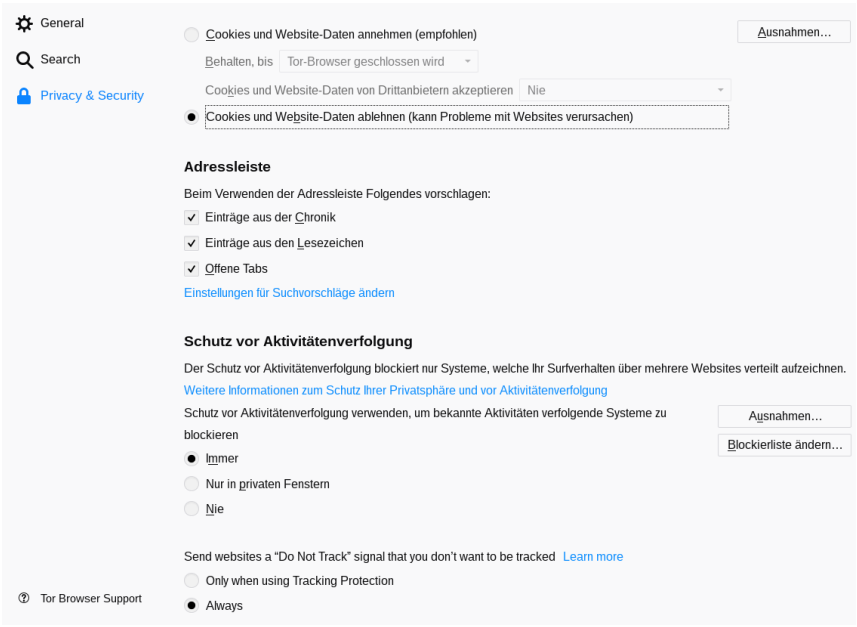
Überprüfe Deine Webseite!

`https://www.vhw-hamburg.de/seniorenresic`

Webbkoll hilft Dir festzustellen, welche datenschutzrechtlichen Maßnahmen eine Website ergriffen hat, um Dir die Kontrolle über Deine Privatsphäre zu geben.
Bitte beachte:

1. Dieses Tool simuliert einen normalen Browser mit ausgeschalteter "Do Not Track" Funktion (ist bei den meisten die Standardeinstellung) und ohne Erweiterungen.
2. Auch wenn Du https:// eingibst, prüfen wir http:// und ob es automatisch auf eine https:// Seite weiter leitet (Weiterleitungen wird gefolgt).
3. Im Allgemeinen sollte alles funktionieren, manchmal kann es jedoch vorkommen, dass einzelne Seiten aus den verschiedensten Gründen nicht funktionieren.
4. Das Back-End läuft derzeit auf einem einzelnen Server mit begrenzten Ressourcen. In Spitzenzeiten kann ein Durchlauf daher etwas dauern. (Wenn Du willst, kannst Du Webbkoll in einer eigenen Instanz betreiben!)

Ein weiteres Beispiel mit folgender Browser Einstellung:



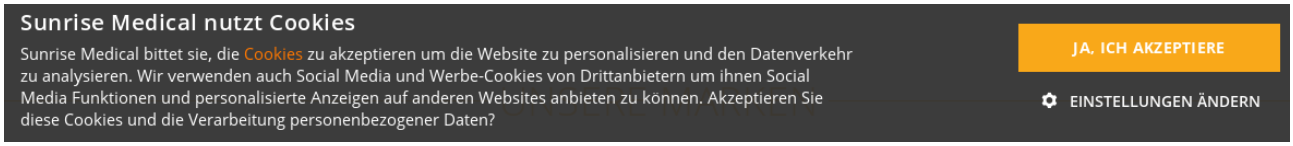


Bild: 1

Ob tatsächlich durch „Drittanfragen (Third Party)“ nach Bild: 3 schon beim Aufruf der Webseite, also vor(!) einem Click auf **„JA, ICH AKZEPTIERE“** oder **„EINSTELLUNGEN ÄNDERN“**, Daten auf US amerikanische Server gespeichert werden, wer weiß! Weiter mit Tails (s. Anhang: I).

Abfrage durch scannen, gefunden: Cookies

First-Party-Cookies (9)

Domain	Name	Wert	Verfällt am
.sunrisemedical.de	_gat	1	2019-10-16 09:40:41Z
.sunrisemedical.de	_gid	GA1.2.1303781956.157...	2019-10-17 09:39:41Z
.sunrisemedical.de	_ga	GA1.2.731964314.1571...	session
www.sunrisemedical.de	CMSCookieLevel	200	2020-10-16 09:39:40Z
www.sunrisemedical.de	CMSCurrentTheme	Responsive-framework	2019-10-17 09:39:40Z
www.sunrisemedical.de	CurrentContact	41687222-9df7-4d4d-a...	2069-10-03 09:39:40Z
www.sunrisemedical.de	ASP.NET_SessionId	1nzgtg3qgvgps52uyeut...	session
www.sunrisemedical.de	CMSCsrfCookie	HVxQCFCAhkFRpxY9QUDl...	session
www.sunrisemedical.de	CMSPreferredCulture	de-DE	2020-10-16 09:39:40Z

Bild: 2

Abfrage durch scannen, gefunden: Drittanfragen (Third Party)

7 Anfragen (7 sichere, 0 unsichere) bis **3** einmalige Hosts.

Ein "Third-party-request" ist ein Abruf von Ressourcen, die nicht von der Ursprungsdomain **`sunrisemedical.de`** oder einer ihrere Subdomains kommen.

Host	IP	Land	Einordnung
fonts.googleapis.com • https://fonts.googleapis.com/css?family=Open+Sans:300,400,600,700;subs...	216.58.215.42	US	Content (Google)
fonts.gstatic.com • https://fonts.gstatic.com/s/opensans/v17/mem5YaGs126MiZpBA-UNirkOUuhp.... • https://fonts.gstatic.com/s/opensans/v17/mem5YaGs126MiZpBA-UN_r8OUuhp.... • https://fonts.gstatic.com/s/opensans/v17/mem5YaGs126MiZpBA-UN7rgOUuhp.... • https://fonts.gstatic.com/s/opensans/v17/mem8YaGs126MiZpBA-UFVZ0b.woff...	216.58.204.131	US	Content (Google)
www.google-analytics.com • https://www.google-analytics.com/r/collect?v=1&_v=j79&aip=1&a=14723500... • https://www.google-analytics.com/analytics.js	172.217.22.142	US	Disconnect (Google)

Bild: 3

Nutzung von Cookies auf SunriseMedical.de

Was sind Cookies?

Cookies sind kleine Dateien, die von einer Website gesendet und während des Zugriffs auf die Seite auf dem Gerät des Nutzers gespeichert werden. Cookies werden zu verschiedenen Zwecken genutzt, zum Beispiel um auf der Website Informationen über Aktivitäten bei vorherigen Besuchen zu speichern, damit Sie die Seite bequemer und effizienter nutzen können, um Ihre Präferenzen zu speichern, die Navigation auf der Seite zu ermöglichen, sowie um zu prüfen, ob Sie sich bereits auf der Seite registriert haben oder ob Sie einen Einkauf tätigen möchten.

Welche Cookies nutzt unsere Website SunriseMedical.de?

Es gibt drei Gruppen von Cookies die wir auf unserer Website nutzen:

Wichtig

Die Cookies sind aktiviert und für grundlegende Funktionen der Website verantwortlich.
Das beinhaltet Cookies, die sich Ihre Sitzungs-ID bei Nutzung unserer Website merken und unterstützen auch die Sicherheit und Login-Authentifizierung.

CMSCookieLevel	Dieses Cookie wird verwendet, um das Cookie Präferenz des Benutzers zu registrieren.
ASP.NET_SessionId	Dieses Cookie wird benutzt, um Besucher zu zählen und zu identifizieren, damit diese Informationen mit bereits vorliegenden abgeglichen werden können.
CMSPreferredCulture	Dieses Cookie verfolgt, welche Teile der Seite besucht wurden und welche Sprachenauswahl getroffen wurde.
CurrentTheme	Speichert den Namen des aktuellen visuellen Themas zur onungsgemässen Gestaltung der Dialogfenster.
CMSCsrfCookie	Speichert ein Sicherheites-Token, welches das System verwendet um alle ausgefüllten Daten zu validieren, die via POST-Anfragen genutzt werden. Schützt gegen seitenübergreifende Falsch-Anfragen.
.ASPXFORMSAUTH	Speichert das verschlüsselte Nutzer-Authentifizierungs-Ticket bei der Authentifizierung durch den Login.
CMSCookieSocialAdvertising	Definiert ob Social Media- und Werbe-Cookies akzeptiert wurden.
CMSCookieLevel	Definiert welche Cookies durch den Nutzer erlaubt sind.

Leistung

Leistungs-Cookies helfen uns die Seitenfunktionalität, durch Nachverfolgung der Nutzung der Website, zu verbessern und ermöglicht es uns Ihre Website Einstellungen zu merken. Wenn Sie diese Cookies nicht akzeptieren, können Sie trotzdem auf den Großteil der Website zugreifen, folglich kann jedoch die Nutzung bestimmter Services eingeschränkt sein.

CMSBodyClass	Body-Element-Klasse für die Bereitstellung von Standards von Zugangsmöglichkeiten.
VisitorStatus	Gesamtstatus des Besuchers zur Verfolgung der Webseiten-Besucher innerhalb der Webanalyse.
Campaign	Speichert die dem Besucher zugeordnete Kampagne zur Webanalyse.
UrlReferrer	Speichert den URL Referrer, aus denen der Benutzer auf die Website gelangt.
CurrentContact	Speichert den GUID des Kontakts im Zusammenhang mit dem aktuellen Besucher der Webseite. Wird verwendet, um die Aktivitäten auf der Webseite zu verfolgen.
Source	Speichert den Kanal, von welchem der Nutzer zugreift, als Teil einer Kampagne (z. B. email, Facebook, Twitter etc.). Basiert auf den UTM-Parametern.
Content	Speichert den spezifischen Inhalt, über welchen der Nutzer auf die Webseite zugreift, als Teil einer Kampagne. Basiert auf den UTM-Parametern.
TrackedCampaigns	. **Speichert alle Kampagnen, welche durch ein JavaScript nachverfolgt werden sollen!**

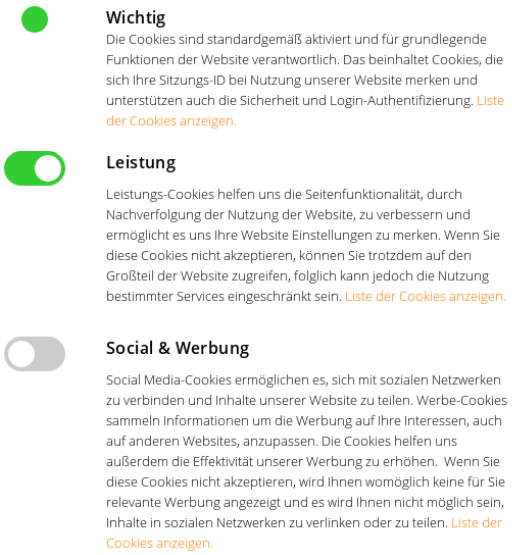
CMSUserPage	Speichert die IDs (DokumentID, NodeID) der zuletzt besuchten Seite. Wird zur Datenerhebung hinsichtlich Ein- und Ausstiegsseiten-Web-Analyse verwendet werden.
CMSLandingPage Loaded	Gibt an dass die Seite bereits besucht wurde und die dortige Aktivität nicht noch einmal für den Nutzer erhoben wird. Verfällt nach 20 Minuten, die Gültigkeits-Periode des Schlüssels wird bei jedem Webseitenbesuch erneuert.
Google Analytics: **_ga** **_gid** **_gat**	**Diese Cookies werden verwendet, Informationen darüber zu sammeln, wie Besucher unsere Website nutzen. Aus diesen Informationen werden Berichte zusammengestellt, die der Verbesserung der Webseite dienen. Diese Informationen sind anonym und indentifizieren die Besucher nicht. Die Daten zählen die Anzahl der Besucher, woher die Besucher gekommen sind und die Seiten die besucht wurden.**

Social & Werbung

Social Media-Cookies ermöglichen es, sich mit sozialen Netzwerken zu verbinden und Inhalte unserer Website zu teilen. Werbe-Cookies sammeln Informationen um die Werbung auf Ihre Interessen, auch auf anderen Websites, anzupassen. Die Cookies helfen uns außerdem die Effektivität unserer Werbung zu erhöhen. Wenn Sie diese Cookies nicht akzeptieren, wird Ihnen womöglich keine für Sie relevante Werbung angezeigt und es wird Ihnen nicht möglich sein, Inhalte in sozialen Netzwerken zu verlinken oder zu teilen. Ändern Sie die Cookie-Einstellungen

YouTube	Wir binden Videos von unserem offiziellen YouTube-Kanal ein und nutzen hierfür den "privacy-enhanced" Modus von YouTube. Dieser Modus setzt Cookies auf Ihrem Computer, sobald Sie auf den YouTube-Player geklickt haben. YouTube speichert bei diesem Modus keine persönlich identifizierbaren Informationen für Wiedergaben von eingebundenen Videos.	Google Privacy policy

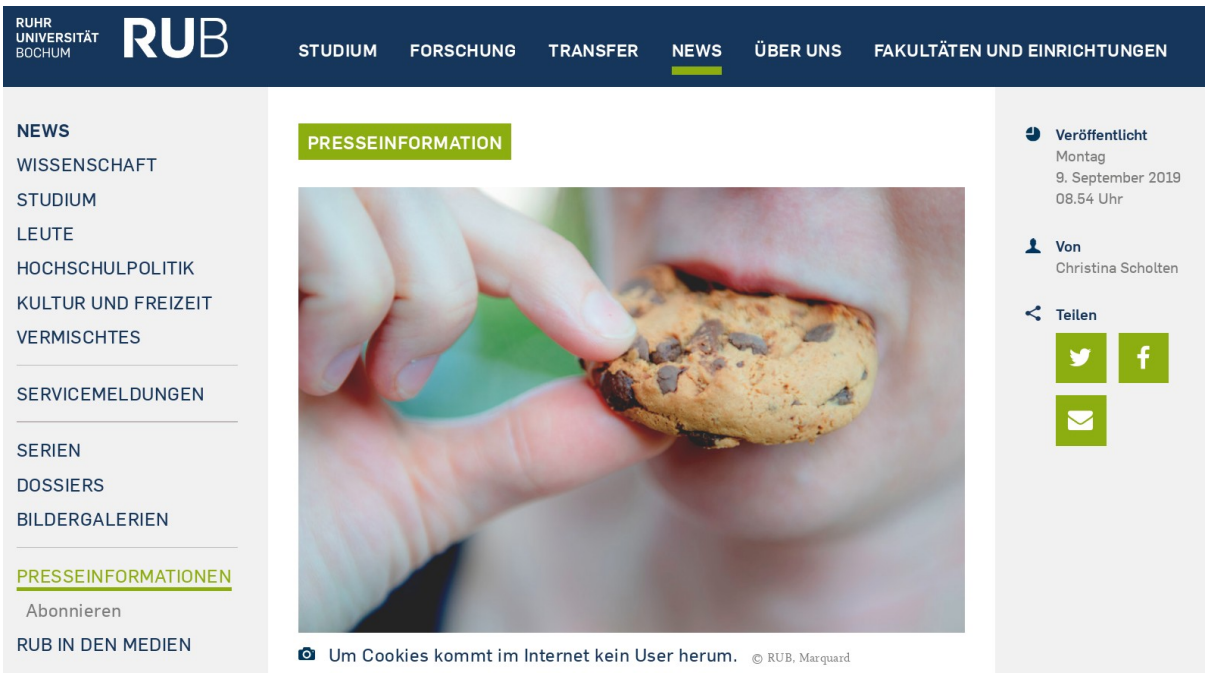
Bei „Ändern Sie die Cookie-Einstellungen“ oder bei Betätigung: **„EINSTELLUNGEN ÄNDERN“** nach Bild: 1 auf Seite: 11 wird die neben stehende **Voreinstellung** gezeigt**:**



„Social & Werbung“ darf nach dem EuGH-Urteil vom 01.10.2019 **NICHT** voreingestellt sein!

Bild: 4

Nach dem EuGH Urteil sollten die Rechte des Webseiten-Benutzers erheblich gestärkt werden! Die Dokumentation mit der provokativem Arbeitsbezeichnung: **„Alles_ein_Fake.pdf“** lässt vermuten, dass der Besucher einer Webseite gut aufgeklärt wird, aber bestimmt nicht auch noch **ungezwungen** „Drittanfragen (Third Party)“ ins „Boot holt“.



IT-Sicherheit

Viele Cookie-Banner erschweren den Schutz der eigenen Daten

Cookie-Hinweise entsprechen nicht nur oft nicht den Regeln des Datenschutzes. Sie nutzen auch teils psychologische Tricks, um User zu manipulieren.

Wer im Netz surft, kommt nicht um sie herum: Cookie-Hinweise zum Schutz der persönlichen Daten, auch bekannt als Cookie-Banner. Forscherinnen und Forscher des Horst-Görtz-Instituts für IT-Sicherheit der Ruhr-Universität Bochum (RUB) haben untersucht, wie Cookie-Banner nach der Einführung der Europäischen Datenschutzgrundverordnung (DSGVO) im Mai 2018 auf Websites umgesetzt werden und wie Userinnen und User mit ihnen interagieren. Dabei haben sie herausgefunden, dass viele Banner nicht den Vorschriften der DSGVO entsprechen – und zum Teil psychologische Tricks angewendet werden, um User zu manipulieren. Christine Utz, Dr. Martin Degeling, Prof. Dr. Sascha Fahl und Prof. Dr. Thorsten Holz veröffentlichten nun in Zusammenarbeit mit Florian Schaub von der University of Michigan dazu ihr Paper „(Un)informed consent: Studying GDPR consent notices in the field“.

Login-Daten oder Infos fürs Marketing

Cookies werden von den Website-Anbietern genutzt, um Informationen über ihre Besucherinnen und Besucher zu speichern. Das können beispielsweise Login-Daten sein, die nicht jedes Mal aufs Neue eingegeben werden müssen. Doch auch Verhaltensweisen und Präferenzen werden – meist zu Marketingzwecken – gespeichert und zudem oftmals an Dritte weitergeben. Die DSGVO sieht jedoch vor, dass diese Daten nicht ohne die Zustimmung der User genutzt werden dürfen.

Tatsächlich zeigen über 60 Prozent beliebter europäischer Websites Cookie-Hinweise an. Doch die Umsetzung variiert laut den Forschern stark. Sie analysierten innerhalb eines Samples von 1.000 Cookie-Hinweisen die möglichen Positionen, ... und Links der Banner.

Sie wollten herausfinden, wie das Design der Banner dazu beitragen kann, es den Usern zu erleichtern, eine informierte Auswahl zu treffen und so ihre Daten zu schützen.

Kleine Manipulationen sollen die Auswahl lenken

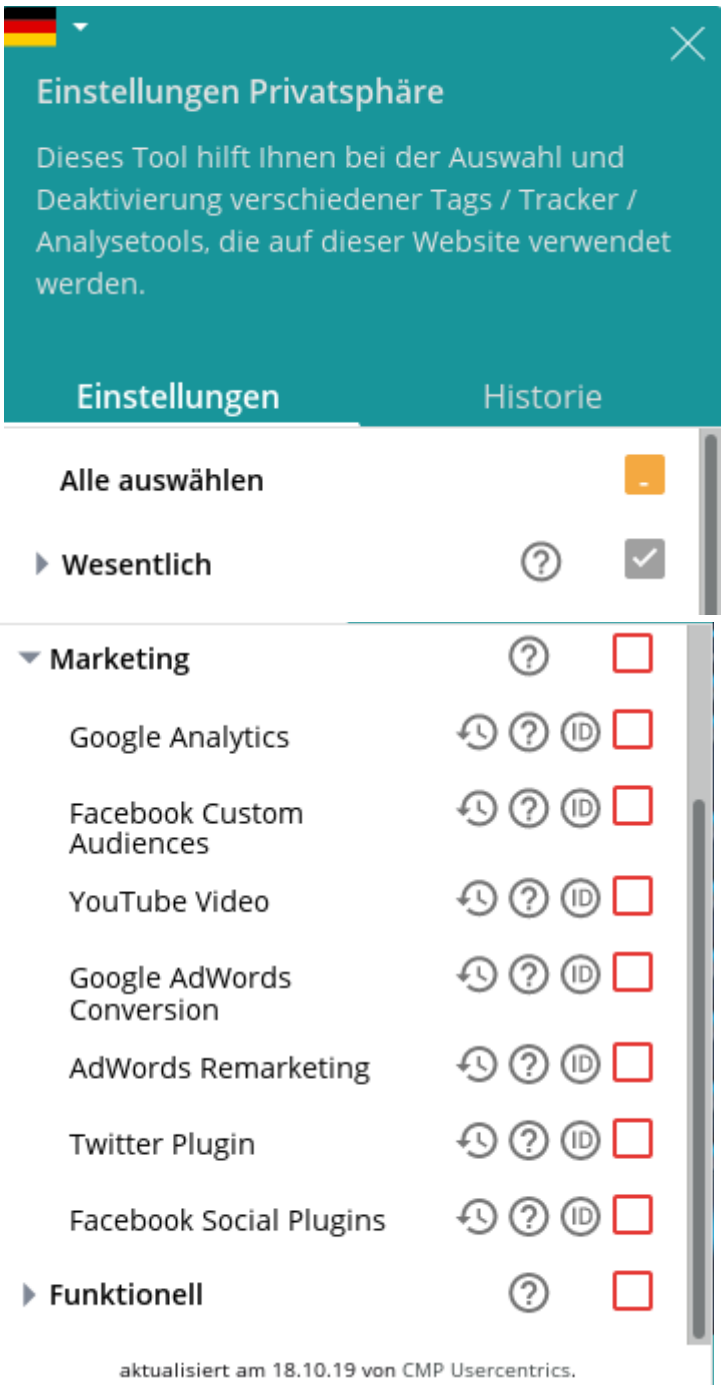
„Es hat sich dabei gezeigt, dass die Mehrheit der Cookie-Hinweise nicht den Vorgaben der europäischen Datenschutzbehörden entspricht, die klar vorgeben, dass die Hinweise transparent sein **und wirkliche Entscheidungsfreiheit bieten müssen**“, erklärt Christine Utz. Doch nicht nur das: 57 Prozent der untersuchten Websites wenden außerdem sogenannte Nudging-Verfahren (siehe den den Nachtrag auf Seite: 25) an, mit dem das Verhalten von Menschen gezielt mit Änderungen der Rahmenbedingungen oder kleinen Manipulationen gelenkt werden soll. Innerhalb der Cookie-Banner waren das beispielsweise farbliche Akzentuierungen des „Zustimmen“-Buttons als Hervorhebung oder unübersichtliche Darstellungen der „Opt-Out“-Möglichkeit. Das Ziel dieser Methode: Die User zum Einverständnis zu bewegen, dass ihre Daten genutzt werden können.

Diese Erkenntnisse haben die Wissenschaftlerinnen und Wissenschaftler genutzt, um sie in einer anschließenden Feldstudie an über 80.000 Nutzerinnen und Nutzern einer deutschen E-Commerce-Website zu erproben. Über vier Monate hinweg haben sie dort unterschiedliche Cookie-Banner ausgespielt, um die Userinteraktion zu beobachten. Zudem fragten sie in einer anschließenden Umfrage die Nutzer nach ihren Präferenzen und Wissen zu Cookie-Bannern. Dabei kam heraus, dass diese am stärksten mit einem Banner interagieren, das in der linken unteren Hälfte des Bildschirms erscheint. „Eine wichtige Erkenntnis war für uns außerdem, dass die Nutzer und Nutzerinnen bei einer Wahl zwischen zwei Optionen eher gewillt sind, das Datentracking zuzulassen, als wenn sie eine größere Anzahl an Optionen haben“, so die Wissenschaftlerin. Antworten aus dem Fragebogen deuten darauf hin, dass Nutzer häufig befürchten, die Website würde nicht richtig funktionieren, wenn sie Cookies ablehnten.

Empfehlungen des Forschungsteams

Insgesamt seien viele User dazu bereit, sich mit den Cookie-Hinweisen auseinanderzusetzen, vor allem diejenigen, die das Speichern der Daten nicht erlauben wollen. Nach jetzigem Stand bieten viele Websites ihnen aber diese Handlungsmöglichkeit nicht oder erschweren sie zumindest. Die Lösung wäre eine obligatorische „Privacy-by-default“-Einstellung, bei der die Daten erst dann erhoben werden, wenn die Nutzer einem Tracking explizit zugestimmt haben. Außerdem empfehlen die Wissenschaftler das Setzen von „zweck-basierten“ Cookie-Hinweisen, bei denen die Zustimmung zur Verarbeitung der Daten nach bestimmten Zwecken erfolgt. Dies entspräche den eigentlichen Vorgaben und dem Grundgedanken der DSGVO. „Würde sich diese Handhabung durchsetzen, würde das dazu führen, dass die Zustimmung zur Weitergabe der Daten an Dritte unter 0,1 Prozent fallen würde“, schlussfolgert Christine Utz.

Die Ergebnisse der Studie können für die weitere Entwicklung der Umsetzung der Europäischen Datenschutzgrundverordnung von großem Wert sein, denn sie ist die erste dieser Art, die sich auf reale Userinnen und User bezieht. So bleibt zu hoffen, dass die Handhabung von Cookie-Bannern sich in den nächsten Jahren verbessert, etwa durch die Einräumung wirklichen Entscheidungsspielraums für die Nutzer oder die Schaffung von Zustimmungsmechanismen im Browser, damit nicht jede Seite selbst um Zustimmung fragen muss.



Gefunden in:

ONLINEHÄNDLER NEWS

E-RECHT ONLINE-HANDEL E-COMMERCE-TRENDS DIGITAL TECH EVENTS

Die fünf häufigsten Fragen rund um das EuGH-Cookie-Urteil

Veröffentlicht: 04.10.2019 | Autor: Sandra May | Letzte Aktualisierung: 04.10.2019

© Sam72 / shutterstock.com

Anfang dieser Woche entschied der Europäische Gerichtshof (EuGH), dass Cookies in aller Regel nur noch mit der ausdrücklichen, freiwilligen und informierten Einwilligung des Besuchers gesetzt werden dürfen. Daraus ergaben sich eine Reihe von Fragen unter den Lesern, die wir hier beantworten.

I.) Reicht das Cookie-Banner, was ich bisher hatte?

Die Cookie-Banner, die bisher auf vielen Seiten zu finden waren, genügten schon vor der Entscheidung in der Regel nicht den rechtlichen Anforderungen. Die Einwilligung zum Setzen von Cookies muss informiert, aktiv und freiwillig erfolgen. Ein Banner, welches diese Voraussetzungen erfüllt, informiert also darüber, welche Cookies zu welchem Zweck gesetzt werden. Außerdem muss es die Möglichkeit der Einwilligung gewährleisten: Es dürfen also keine Kästchen vorausgewählt werden. Darüber hinaus muss die Möglichkeit bestehen, einzelnen Verwendungen zuzustimmen, und anderen wiederum nicht.

Freiwillig bedeutet in diesem Zusammenhang, dass die Seite auch nutzbar sein muss, wenn der Cookie-Banner oder das Consent-Tool vom Nutzer ignoriert wird. Hinzu kommt noch der Umstand, dass viele Banner wichtige Rechtstexte, wie das Impressum oder die AGB im Footer verdecken. Ignoriert der Besucher das Banner, ist nicht gewährleistet, dass alle wichtigen Informationen erreichbar sind.

Daher gilt, dass sich Webseitenbetreiber nicht auf den Bannern ausruhen sollten, die sie bereits integriert haben. Ein kritischer Blick lohnt sich aufgrund der eben genannten Punkte.

II.) Es gibt eine Ausnahme: Was sind notwendige Cookies?

Das Urteil macht klar, dass es einen grundlegenden Unterschied zwischen notwendigen und nicht-notwendigen Cookies gibt. Für erstere muss keine Einwilligung eingeholt werden. Hier reicht der Hinweis in der Datenschutzerklärung aus. Doch: Was sind denn überhaupt notwendige Cookies?

Darunter sind solche Funktionen zu verstehen, die überhaupt erst dafür sorgen, dass die Webseite genutzt werden kann. Das sind zum Beispiel:

- User-Input-Cookies, also sogenannte Session-Cookies, für die Dauer einer Sitzung
- Authentifizierungs-Cookies für Dienste, bei denen eine Authentifizierung erforderlich ist, für die Dauer einer Sitzung
- Multimedia-Player-Sitzungscookies wie Flash-Player-Cookies für die Dauer einer Sitzung

III.) Muss das Banner auch sein, wenn ich nur notwendige Cookies verwende?

Nein. Werden auf einer Seite tatsächlich ausschließlich notwendige Cookies gesetzt, so reicht ein Hinweis in der Datenschutzeklärung. Ein Banner oder Consent-Tool muss dann nicht eingebunden werden.

IV.) Ist das Urteil für den E-Commerce überhaupt relevant?

Ja, natürlich. Zum einen laufen auf jeder Seite zumindest notwendige Cookies. Das Urteil hat nun Klarheit darüber verschafft, dass hier kein Banner notwendig ist.

Darüber hinaus kommen im E-Commerce in der Regel aber zu den notwendigen Cookies noch verschiedene Analyse-Tools und Social-Media-PlugIns zum Einsatz. Werden dadurch Cookies gesetzt, ist jetzt sicher, dass und wie die Einwilligung durch den Besucher erfolgen muss.

V.) Gilt das Urteil überhaupt?

Viele lehnen sich jetzt zurück, denn: Im deutschen Telemediengesetz (TMG) steht, dass eine Einwilligung nicht benötigt wird. Es herrscht die Ansicht, dass erst das TMG geändert werden müsste, damit das Urteil wirkt. Das ist aber grundsätzlich falsch, denn: Die Urteile des EuGH gelten unmittelbar für alle Gerichte in der kompletten EU. Hierdurch soll eine schnelle und effektive Umsetzung von EU-Recht ermöglicht werden.

Würde es nun innerhalb Deutschlands zu einem Gerichtsverfahren kommen, müsste das zuständige Gericht den europäischen Richterspruch umsetzen – und dieser steht über dem TMG. Die nationalen Gerichte sind damit in ihrer Funktion auch eine Versicherung dafür, dass Gemeinschaftsrecht einheitlich angewendet wird.

Autorin: Sandra May *Experte für IT- und Strafrecht*

Sandra schreibt seit September 2018 als juristische Expertin für OnlinehändlerNews. Bereits im Studium spezialisierte sie sich auf den Bereich des Wettbewerbs- und Urheberrechts. Nach dem Abschluss ihres Referendariats wagte sie den eher unklassischen Sprung in den Journalismus. Juristische Sachverhalte anschaulich ... zu erklären.

Drittanfragen (Third Party)

32 Anfragen (32 sichere, 0 unsichere) bis **11** einmalige Hosts.

Ein "Third-party-request" ist ein Abruf von Ressourcen, die nicht von der Ursprungsdomain `onlinehaendler-news.de` oder einer ihrere Subdomains kommen.

Host	IP	Land	Einordnung
api.usercentrics.eu • https://api.usercentrics.eu/consent-templates/ad578071ca3b69e2625c8684... • https://api.usercentrics.eu/settings/Ei8albRA/latest/en.json	35.241.3.184		
app.usercentrics.eu • https://app.usercentrics.eu/latest/bundle.js • https://app.usercentrics.eu/latest/main.js	35.190.14.188	US	
cdn.jsdelivr.net • https://cdn.jsdelivr.net/npm/simplebar@3.1.5/dist/simplebar.min.js • https://cdn.jsdelivr.net/npm/js-cookie@2/src/js.cookie.min.js	151.101.122.109	FR	
cdnjs.cloudflare.com • https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js • https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/3.3.7/js/boot...	104.19.198.151	US	
fonts.gstatic.com • https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxK.woff2	216.58.204.131	US	Content (Google)

Host	IP	Land	Einordnung
graphql.usercentrics.eu • https://graphql.usercentrics.eu/graphql • https://graphql.usercentrics.eu/graphql • https://graphql.usercentrics.eu/graphql	216.58.209.243	US	
privacy-proxy.usercentrics.eu • https://privacy-proxy.usercentrics.eu/latest/uc-block-ui.bundle.js • https://privacy-proxy.usercentrics.eu/latest/uc-block.bundle.js	35.190.14.188	US	
use.fontawesome.com • https://use.fontawesome.com/releases/v5.1.0/webfonts/fa-solid-900.woff... • https://use.fontawesome.com/releases/v5.1.0/webfonts/fa-brands-400.wof... • https://use.fontawesome.com/releases/v5.1.0/css/all.css	23.111.9.35	US	
www.google.com • https://www.google.com/recaptcha/api2/bframe?hl=de&v=EQY1At-f1G9OIivZU... • https://www.google.com/recaptcha/api2/webworker.js?hl=de&v=EQY1At-f1G9... • https://www.google.com/js/bg/0rHA7P1bMVBxjJBUda1zfg2JJv6VLAn5MVgTiLYWN... • https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Le-6Z4UAAAAAMrrYc... • https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Le-6Z4UAAAAAMrrYc... • https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Le-6Z4UAAAAAMrrYc... • https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Le-	216.58.213.132	US	

Host	IP	Land	Einordnung
6Z4UAAAAAMrrYc... • https://www.google.com/recaptcha/api.js?onload=JoomlaInitReCaptcha2&re...			
www.googletagmanager.com • https://www.googletagmanager.com/gtm.js?id=GTM-PCZLWZS	172.217.18.200	US	Disconnect (Google)
www.gstatic.com • https://www.gstatic.com/recaptcha/releases/EQY1At-f1G9OIivZUYX73fK0/re... • https://www.gstatic.com/recaptcha/releases/EQY1At-f1G9OIivZUYX73fK0/st... • https://www.gstatic.com/recaptcha/api2/logo_48.png • https://www.gstatic.com/recaptcha/releases/EQY1At-f1G9OIivZUYX73fK0/st... • https://www.gstatic.com/recaptcha/releases/EQY1At-f1G9OIivZUYX73fK0/re... • https://www.gstatic.com/recaptcha/releases/EQY1At-f1G9OIivZUYX73fK0/re...	172.217.22.131	US	Content (Google)

Cookies

First-Party-Cookies (2)

Domain	Name	Wert	Verfällt am
.onlinehaendler-news.de	__cfduid	ddb4252dc89a8e49f549...	2020-10-17 14:03:38Z
www.onlinehaendler-news.de	412f67f5a37e7f99a9bf...	8473e1fff260cbe54d04...	session

3. September 2019, 17:01 Uhr Depression

Wie Hilfesuchende im Netz erfasst werden

Webseiten, auf denen Nutzer Informationen zu psychischen Erkrankungen finden können, geben reihenweise Nutzer-Daten zu Werbezwecken an Drittunternehmen weiter. Davor warnt eine Analyse der Nichtregierungsorganisation Privacy International.

- Das ist fragwürdig, weil Drittanbieter anhand der weitergegebenen Daten erkennen könnten, dass sich ein Besucher über psychische Erkrankungen informiert hat oder gar einen Depressions-Selbsttest gemacht hat.

Wer fürchtet, an einer Depression zu leiden und im Internet Hilfe sucht, wird dabei in vielen Fällen beobachtet. Ein Großteil beliebter Webseiten, auf denen sich Besucher über psychische Krankheiten informieren können, leitet Nutzungsdaten an andere Unternehmen weiter, die augenscheinlich gar nichts mit den Gesundheits-Webseiten zu tun haben. Unter den Unternehmen sind große Werbenetzwerke und Unternehmen wie Google, Amazon und Facebook. Drittanbieter könnten anhand der weitergegeben Daten erkennen, dass sich ein Besucher über psychische Erkrankungen informiert hat oder gar einen Depressions-Selbsttest gemacht hat. Das zeigt eine Analyse der Organisation Privacy International (PI), die *Süddeutscher Zeitung* und *NDR* exklusiv vorlag. In vielen Fällen werden diese Daten ohne die Zustimmung des Nutzers weitergegeben.

Heikel ist das vor allem, weil wenige Themen so schambesetzt sind wie psychische Krankheiten. Daten, die Rückschlüsse auf die Gesundheit Einzelner zulassen können, sollten deshalb nicht nur in der Krankenakte beim Arzt, sondern auch im Netz besonders geschützt sein.

Für ihre Analyse untersuchte PI, eine in London ansässige Organisation, 136 beliebte Webseiten für psychische Gesundheit in Deutschland, Frankreich und Großbritannien. Webseiten bestehen aus verschiedenen Software-Bausteinen. Nicht über alle davon hat der Betreiber der Seite die volle Kontrolle. Mehr als 97 Prozent der untersuchten Seiten enthielten Elemente von Drittanbietern.

Diese können harmlos ein und zum Beispiel nur visuelle Effekte auf der Seite steuern.

Andere werden aber eingesetzt, um Besuchern Werbung anzuzeigen, Daten über ihr Verhalten zu erfassen und an andere Firmen weiterzuleiten.

Die 44 untersuchten deutschen Seiten enthielten im Schnitt mehr als acht Elemente von Drittanbietern und übermittelten in mehr als sieben Fällen Tracking-Cookies solcher Firmen. Cookies sind Daten, die auf dem Gerät eines Internetnutzers gespeichert werden, wenn er eine Webseite besucht. Anhand einer eindeutigen Identitätsnummer können Cookies von Drittanbietern Nutzer über verschiedene Webseiten verfolgen. Ziel ist, ihm passgenau maßgeschneiderte Werbung anhand seiner vermuteten Interessen anzeigen zu können.

Viele Anbieter fragen nicht einmal um Erlaubnis, ob sie Daten speichern dürfen

Fast zwei Drittel der Elemente, die PI entdeckte, wurden von den Gesundheits-Webseiten für Werbung eingesetzt. Die Seiten ermöglichen es Werbenetzwerken, ihre ohnehin große Datensammlung um intime Details zu ergänzen. Vier von neun näher untersuchten Seiten fragen der Studie zufolge nicht um Erlaubnis, bevor sie einen Cookie beim Besucher hinterlegen. Ulrich Kühn, als stellvertretender Leiter der Hamburger Datenschutzbehörde unter anderem für die Aufsicht über Facebook zuständig, sagt: Ohne Einwilligung gebe es "keine Rechtsgrundlage" für die Datenweitergabe. Das sei "ein klarer Verstoß gegen die Datenschutz-Grundverordnung". Die DSGVO stellt Gesundheitsdaten auf eine Stufe mit Informationen über sexuelle Orientierung, genetische und biometrische Merkmale, sowie Informationen über "rassische und ethnische Herkunft", Religion und Weltanschauung.

PI empfiehlt, dass gerade Seiten, die sensible Themen wie psychische Gesundheit behandeln, komplett auf verhaltensorientierte Anzeigen verzichten. Die Organisation nahm auch Webseiten unter die Lupe, die Depressions-Selbsttests anbieten. In diesen Fällen wird auch die Adresse der Webseite an Werbetreibende weitergeleitet, wie etwa netdoktor.de/selbsttests/depressionstest-nach-goldberg oder nie-mehr-depressiv.de/depressionstest/. Anhand der Adresse könnten Werbetreibende den Inhalt der Webseite herausfinden und ihn Besuchern zuordnen - was viele Hilfesuchende sicher nicht möchten. Einige Selbsttests erwecken den Eindruck, man könne sie komplett anonym nutzen. Dem ist nicht so: Um die untersuchten Tests herum identifizierte Privacy International jeweils Dutzende Tracker, die Informationen speichern und diese wiederum mit Informationen anderer Webseiten verknüpfen können. Dadurch können personenbezogene Profile entstehen.

Immerhin: Die Antworten werden in den untersuchten deutschen Fällen nicht übertragen. Die Drittanbieter wissen im Zweifel nur, dass ein Nutzer einen Depressionstest gemacht hat und bis zu welcher Frage geklickt wurde. Für welche Antwortmöglichkeit sich der Nutzer entschieden hat, welche Symptome er also bei sich selbst beobachtet, kann aus den übertragenen Daten nicht geschlossen werden. Allerdings teilen mehrere französisch- und englischsprachige Webseiten die Antworten des Nutzers mit Drittanbietern, wie PI in der Analyse schreibt.

Die Webseite Netdoktor.de ist eine der beliebtesten digitalen Anlaufstellen für Gesundheitsfragen der Deutschen. Sie setzt Privacy International zufolge die meisten Drittanbieter-Elemente aller untersuchten deutschen Webseiten ein.

Darunter ist etwa ein Cookie der französischen Werbefirma Criteo, die eigenen Angaben zufolge Daten zum Besucherverhalten auf mehreren Webseiten sammelt, um "relevantere" Werbung zu präsentieren. Laut PI hat ein Drittanbieter wie Criteo dadurch auch Zugriff auf die Adresse der Webseite und damit auf die Information, dass der Besucher einen Test aufgerufen hat. Netdoktor erklärt, dass keine Speicherung gesundheitsbezogener Daten stattfinde. Genauso wenig würden entsprechende Daten an Dritte weitergegeben oder gar veräußert. Man halte sich an geltendes Datenschutzrecht.

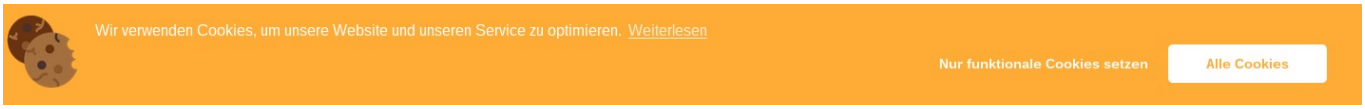
Auch deutsche Kliniken nutzen im Netz problematische Marketing-Werkzeuge

Allerdings kann beim Besuch der Webseite die IP-Adresse des Nutzers und der Inhalt seitenübergreifender Cookies an eine Vielzahl von Drittanbietern übermittelt werden. Die IP-Adresse gilt unter Datenschützern als personenbezogen. In Kombination mit anderen Daten wie besuchten Webseiten ist sie besonders wertvoll für Werber. Frederike Kaltheuner von PI sagt: "Das Problem bei diesen Webseiten ist, dass schon die Adresse der Webseite sehr viel über uns preis gibt: Test, Symptome, bin ich depressiv - das sagt das schon sehr viel über mich aus."

Auch die Internetseiten mehrerer deutscher Kliniken gehen laut der Untersuchung nicht sensibel genug mit den Daten ihrer Besucher um. Nach Anfragen von SZ und NDR erklärten mehrere der Kliniken, einzelne Marketing-Werkzeuge von Drittanbietern auf ihren Webseiten vorerst abzuschalten.

Erst vergangene Woche hatte eine Recherche der SZ gezeigt, wie problematisch Nachlässigkeit beim Umgang mit Informationen über die Gesundheit von Menschen im Internet sein kann. Die Webseite vom Blutspendedienst des Bayerischen Roten Kreuzes bietet eine Umfrage für potentielle Blutspender an, in der unter anderem nach HIV- und Hepatitis-Infektionen oder Schwangerschaftsabbrüchen gefragt wurde. Durch eine Fehlkonfiguration übertrug die Webseite wochenlang die Antworten an Facebook. Der Blutspendedienst hat diese Übertragung nun abgestellt. Das Bayerische Landesamt für Datenschutzaufsicht untersucht den Fall.

Nachtrag zu Seite: 1, Bild: 1 (Korrekur: Bildschirmabdruck vom 19. Oktober 2019)

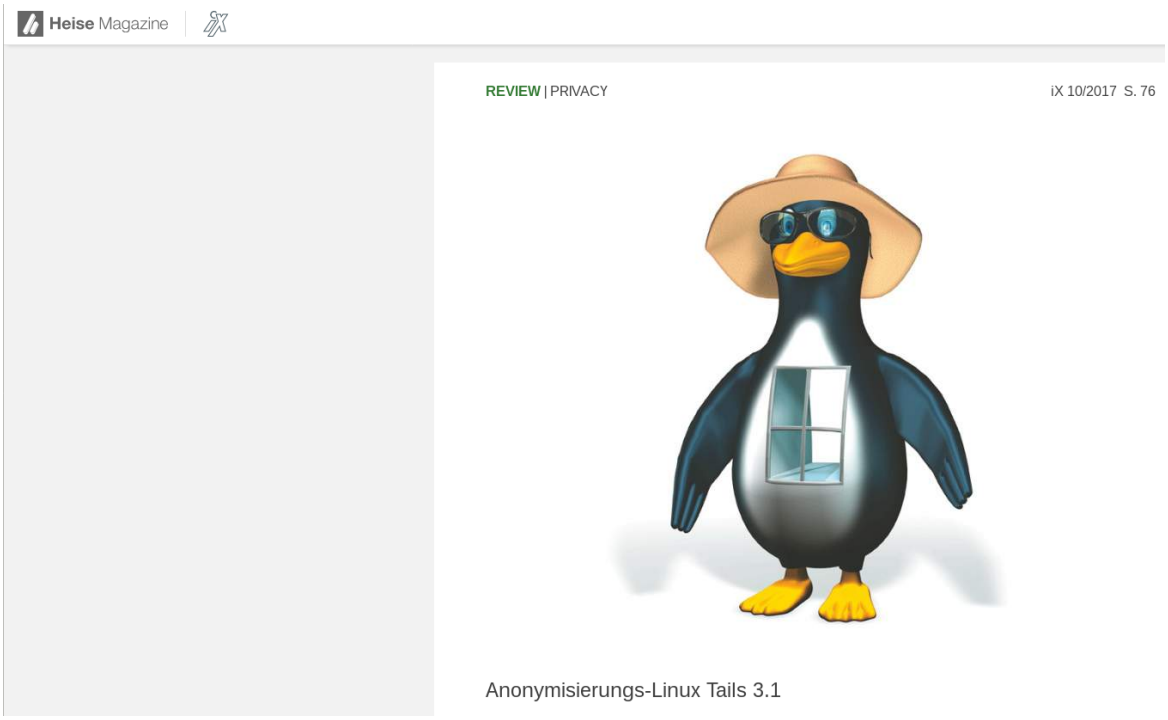


Wir verwenden Cookies, um unsere Website und unseren Service zu optimieren. Weiterlesen

---

„Weiterlesen“, „Nur funktionale Cookies setzen“ und „Alle Cookies“ sind Links! Was möchte die Webseitenbetreiberin mit der unterschiedlichen Darstellung damit erreichen?
Besser kann man ein „**Nudging-Verfahren**“ nicht darstellen!

Anhang: Die bessere Alternative / Nur anonym im Internet mit Tails-OS



Durchgeschaut / Jörg Riether

Das bekannteste amnestische Linux – spätestens seit Edward Snowden – ist wohl Tails, das im Sommer in der dritten Major Release erschien.

***iX*-Wertung**

⊕ einfache Gestaltung, triviale Bedienung

⊕ hohes Engagement der Entwickler für weitere Sprachen außer Englisch

⊕ sinnvolle Firewall-Konzeption

Gleich mehrere Linux-Distributionen versuchen, die Anonymität und Privatsphäre ihrer Benutzer zu wahren. The Amnesic Incognito Live System oder kurz Tails gehört dazu und darf sich bereits als alten Hasen bezeichnen, hat es doch schon gut acht Jahre auf dem Buckel. Im Juni 2017 erschien die neue Major Release 3.0, basierend auf Debian 9 „Stretch“ – vier Tage vor der offiziellen Stretch-Release. Dass das Debian-Team bereits im Juli die Version 9.1 folgen ließ, die einige Sicherheitslücken schloss, war für die Tails-Entwickler Grund genug, Anfang August ihre Version 3.1 nachzuschieben. Bei dieser Gelegenheit hoben sie den Tor-Browser auf 7.0.4 und den Linux-Kernel auf 4.9.30-2+deb9u3.
Anders als etwa Qubes OS ist Tails nicht zur dauerhaften Installation gedacht, sondern als pures Live-System konzipiert, das von einer DVD, einem USB-Stick oder einer SD-Karte startet. Auf beschreibbaren Medien kann man einen persistenten verschlüsselten Bereich einrichten, den Tails wenn gewünscht beim Booten einbindet. **Für USB-Sticks, die der Hersteller als festes Medium und nicht als entfernbares konfiguriert hat, kann man den Boot-Parameter *live-media=removable* auskommentieren.** Grundsätzlich läuft Tails auf einer breiten Palette unterschiedlicher Hardware. Etwaige Schwierigkeiten mit Rechnern und USB-Sticks skizziert das Entwicklerteam auf seiner Projektseite, die auch über die *iX*-Links am Ende des Artikels zu finden ist.

Seit der Version 3.0 läuft Tails allerdings nur noch auf 64-bittigen x86-kompatiblen Prozessoren. Dazu empfiehlt das Entwicklerteam 2 GByte RAM. Es begründet die bewusste Entscheidung gegen 32-Bit-Systeme damit, dass das die Sicherheit und Zuverlässigkeit erhöhe. Beispielsweise sei zum Schutz vor bestimmten Exploit-Typen die Nutzung des NX-Bits (No eXecute) nunmehr verpflichtend. Außerdem seien die meisten Binärdateien per PIE (Position-independent Executable) gehärtet, was wiederum ASLR (Address Space Layout Randomization) erlaube. / **T**ails soll keine digitalen Spuren auf der Hardware hinterlassen, auf der es läuft – außer man wünscht es. Die interne Festplatte fasst Tails von sich aus nicht an. Das Entwicklerteam rät den Anwendern dringend davon ab, selbst darauf zuzugreifen, denn es könnten Spuren zurückbleiben. Oder ein kompromittiertes Tails könnte die interne Festplatte infizieren. Möchte man sie dennoch einbinden, kann man beim Start von Tails ein Passwort setzen und danach im Dateimanager GNOME Files auf die Festplatten lesend wie schreibend darauf zugreifen. Das Kontextmenü bietet darüber hinaus Funktionen wie sicheres Löschen oder Verschlüsseln. Neu ist außerdem die Option des Umbenennens multipler Dateien.

Beim Herunterfahren füllt Tails zudem einen Großteil des Arbeitsspeichers mit Zufallswerten, um sich gegen sogenannte Cold-Boot-Angriffe zu schützen. Die Projektseite liefert eine detaillierte Beschreibung der Prozedur.

Die Wahl des Browsers

Bei der Wahl der Arbeitsumgebung hat sich das Team für GNOME entschieden. Das Anonymisierungsnetzwerk Tor ist fester Bestandteil von Tails. Das System versucht, sämtliche Verbindungen ins Internet über Tor zu lenken. Gelingt das nicht, blockiert es sie.

Der standardmäßig verwendete Tor-Browser 7.0.4 basiert auf Firefox 52.3.0. Als Erweiterungen sind NoScript zur Kontrolle über JavaScript, der Werbeblocker uBlock Origin sowie HTTPS Everywhere installiert, das zahlreiche Nicht-SSL-Anfragen transparent auf SSL umleitet. Die Applikationsisolation übernimmt AppArmor. Derzeit setzt Tails nur auf dateisystembezogene Isolation, sodass ein Programm etwa nicht den GnuPG-Schlüsselbund lesen kann. Setzt man beim Tails-Start ein Passwort, kann man sich mit den Befehlen *sudo –i* und *aa-status* einen Überblick über die Tails-internen AppArmor-Profile verschaffen.

Ohne Tor ins Web kommt man mit dem Unsafe Browser. Er ist etwa bei zahlreichen Login-Portalen von öffentlichen WLANs unumgänglich, will man die initiale Zugangsberechtigung erhalten. Deshalb läuft der Unsafe Browser mit den Rechten eines separaten Clearnet-Benutzers, der externe TCP-Verbindungen über beliebige Ports herstellen sowie jegliche UDP-DNS-Abfragen durchführen kann. Gleichzeitig sind lokale Dienste wie Tor für diesen Benutzer blockiert.

Startet man den Unsafe Browser, lädt Tails ihn in einer *chroot*-Umgebung und einem eigenen Wegwerf-Dateisystem. **Beides zerstört es beim Beenden des Browsers wieder.**

Die Entwickler weisen explizit darauf hin, dass es ein Leichtes sei, aus einer *chroot*-Umgebung auszubrechen und man dieses Konstrukt nicht aus Gründen der sicheren Dateiisolation benutze. Vielmehr solle das unsichere Konfigurationen, etwa einen DNS Resolver, eingrenzen.