Ergebnisse für **www.bitdefender.de**

Wiederholen
2021-12-10 23:08:12 Etc/UTC

HTTPS als Voreinstellung: ✔ Ja

Content Security Policy: ✘ implementiert, aber mit Fehlern ⓘ Berichte wurden übermittelt

Referrer Policy: ✘ Referrers werden übermittelt

Cookies: **70** (26 First-Party; 44 Third-Party)

Drittanfragen (Third-Party): **143** Anfragen an 64 einzigartige Hosts

IP-Adresse: 104.18.24.28 Nachschlagen

Überprüfte URL: http://www.bitdefender.de/
Weitergeleitet: https://www.bitdefender.de/

✔ HTTPS als Voreinstellung

`www.bitdefender.de` verwendet HTTPS als Voreinstellung.

Chromium hat folgendes entdeckt:

Status	Titel	Ergebnis	Beschreibung
✔	Certificate	valid and trusted	The connection to this site is using a valid, trusted server certificate issued by Sectigo RSA Domain Validation Secure Server CA.
✔	Connection	secure connection settings	The connection to this site is encrypted and authenticated using TLS 1.3, X25519, and AES_128_GCM.
✔	Resources	all served securely	All resources on this page are served securely.

Weitere Informationen zur TLS/SSL-Konfiguration dieser Website:

- Analysiere www.bitdefender.de bei SSL Labs
- Observatory by Mozilla
- Mozilla TLS Observatory
- testssl.sh

Anleitung

HTTPS verschlüsselt nahezu alle Informationen, die zwischen Client und Webservice ausgetauscht werden. Richtig konfiguriert, garantiert es drei Dinge:

- **Vertraulichkeit**. Eine Verbindung ist verschlüsselt und URLs, Cookies und andere sensible Metadaten sind geschützt.
- **Authentizität**. Ein Besucher befindet sich auf der "echten" Website und nicht auf irgendeiner, die etwas vorgibt zu sein oder auf der eines "Man-in-the-Middle".
- **Integrität**. Zwischen einem Besucher und dem Betreiber einer Website ausgetauschte Daten wurden nicht manipuliert oder verändert.

Einfache HTTP-Verbindungen können leicht überwacht, verändert oder nachgeahmt werden. Jede unverschlüsselte verschickte HTTP-Anfrage beinhaltet Meta-Informationen und ermöglicht Rückschlüsse auf das Verhalten. Das Mitlauschen und Nachverfolgen von unverschlüsseltem Surfen ist zur Selbstverständlichkeit geworden.

Ziel der Internet-Community ist es, die Verschlüsselung als Standard zu etablieren und die Verwendung unverschlüsselter Verbindungen auslaufen zu lassen.

DSGVO: Erwägungsgrund 83, Art. 5.1.f, Art. 25, Art. 32.1
Nach DSGVO Art. 25 ist ein Controller für die Durchsetzung des Datenschutzes bereits in der Entwicklung und in Standardeinstellungen auf dem aktuellen Stand der Technik verantwortlich. Verschlüsselte Verbindungen sind eine etablierte Technologie zum Schutz der Privatsphäre von Website-Besuchern vor Lauschangriffen.

✔ HTTP Strict Transport Security (HSTS)

HSTS-Richtlinie für https://www.bitdefender.de:

```
max-age=31536000; includeSubDomains; preload
```

HTTP Strict Transport Security (HSTS) ist ein breit unterstützter Standard zum Schutz eines Besuchers.

Status	Test
✔	`max-age` auf mindestens 6 Monate gesetzt
✔	`includeSubDomains` — Richtlinie betrifft auch Subdomains
➖	`preload` — fordert Einbindung in der Preload-Liste an [nur für die Hauptdomain relevant]

HSTS-Richtlinie für https://bitdefender.de:
`max-age=31536000; includeSubDomains; preload`

Status	Test
✔	`max-age` auf mindestens 6 Monate gesetzt
✔	`includeSubDomains` — Richtlinie betrifft auch Subdomains
✔	`preload` — fordert Einbindung in der Preload-Liste an

indem es sicher stellt, daß der Webbrowser eine Seite immer nur über HTTPS öffnen kann. Mit HSTS entfällt die unsichere Notwendigkeit der Weiterleitung eines Besuchers von `http://` - zu `https://` -URLs.

Wird dem Browser mitgeteilt, dass eine Domain HSTS nutzt, so macht er zwei Dinge:

- Verwendet immer eine `https://` -Verbindung, selbst wenn auf einen `http://` -Link geklickt wird oder wenn eine Domäne in der Adressleiste ohne Protokoll eingegeben wurde.
- Entfernt die Möglichkeit für Benutzer, Warnungen vor ungültigen Zertifikaten zu ignorieren.

Eine Domain teilt den Webbrowsern mit, dass sie HSTS aktiviert hat, indem sie einen HTTP-Header über eine HTTPS-Verbindung zurückgibt.

Anleitung

✖ Content Security Policy

Gesetzte Content Security Policy im HTTP-Header: `frame-src *.2checkout.com *.bitdefender.com *.bitdefender.biz *.bitdefender.net *.bitdefender.fr *.bitdefender.de *.bitdefender.com.au *.bitdefender.co.uk *.bitdefender.es *.bitdefender.it *.bitdefender.pt *.bitdefender.com.br *.bitdefender.ro *.bitdefender.nl *.bitdefender.be *.bitdefender.se bitdefender.marketing.adobe.com download.bitdefender.com *.facebook.com *.doubleclick.net *.adsrvr.org *.mathtag.com *.google.com *.google.ro *.flashtalking.com *.amazon-adsystem.com *.livechatinc.com *.twitter.com *.cedexis.com *.cedexis-test.com *.youtube.com *.soundcloud.com *.hubspot.com *.cookiebot.com *.vimeo.com *.edgecastcdn.net *.linkedin.com *.hsforms.com *.cloudfront.net *.edgecastdns.net *.hotjar.com *.zanox.ws *.zanox.com *.usemax.de usemax.de bitdefender.demdex.net dpm.demdex.net *.omniture.com widget.trustpilot.com *.2o7.net *.omtrdc.net *.demdex.net assets.adobedtm.com api-eu.boldchat.com livechat-eu.boldchat.com *.youtube-nocookie.com *.instagram.com instawidget.net`

> Eine Content Security Policy (CSP) bildet eine zusätzliche Sicherheitsebene, die hilft Angriffe zu erkennen und zu entschärfen, einschließlich Cross Site Scripting (XSS) und Data-Injection-Angriffen. Solche Art von Angriffen sind geeignet, eine Website zu verunstalten, und reichen bis hin zum Datendiebstahl und Verbreitung von Malware.
>
> Ein Hauptziel von CSP ist es, XSS-Angriffe zu minimieren und zu melden. XSS-Angriffe nutzen das Vertrauen des Browsers in die vom Server empfangenen Inhalte aus. Bösartige Skripte werden vom Browser des Opfers ausgeführt, weil der Browser der Quelle des Inhalts vertraut, auch wenn er nicht von dort kommt, wo er herzukommen scheint.
>
> Die CSP ermöglicht es Serveradministratoren, Angriffsvektoren durch XSS-Angriffe zu reduzieren oder zu eliminieren, indem dem Browser bestimmte Domains als gültige Quellen u.a. für ausführbare Skripte mitgeteilt werden. Ein CSP-kompatibler Browser führt dann nur noch Skripte aus, die von diesen Whitelist-Domänen empfangen wurde und ignoriert alle anderen Skripte (einschließlich Inline-Skripte und HTML-Attribute zur Ereignisbehandlung).
>
> *— MDN: Content Security Policy (CSP), Mozilla Contributors, CC BY-SA 2.5*

🔨 DSGVO: Erwägungsgrund 83, Art. 5.1.f, Art. 25, Art. 32.2
DSGVO Art. 32.2 stellt klar, daß Maßnahmen gegen

`consentcdn.cookiebot.com recommender.scarabresearch.com *.zenaps.com hal9000.redintelligence.net pixel.xonaz.com static-hello.bitdefender.com tags.dynamo.one *.redintelligence.net 20787700p.rfihub.com pixel.xonazz.com *.adobe.com *.outgrow.us bitdefender.applytojob.com *.alchemer.com *.adyen.com *.paypal.com paypal.com ad.ad-srv.net fullstory.com *.bitdefender.co.jp bitdefender.co.jp new.bitdefender.co.uk store.bitdefender.com bitdefender-html.test`

Content Security Policy (CSP) wurde unsicher implementiert. Das beinhaltet ein `'unsafe-inline'` oder `data:` innerhalb von `script-src`, zu weit umfasste Ressourcen wie beispielsweise `https:` in `object-src` oder `script-src` eine fehlende Eingrenzung auf Ressourcen bei `object-src` oder `script-src`.

Status	Test	Infos
✘	Schutz vor Clickjacking durch `frame-ancestors`	Zeigen
✘	Verbiete zuerst alles mit der Standardeinstellung `default-src 'none'`	Zeigen
✘	Eingeschränkte Verwendung von `<base>` durch `base-uri 'none'`, `base-uri 'self'`, oder spezifizierten Quellen	Zeigen
✘	Beschränkt die Zusendung von `<form>`-Inhalten durch `form-action 'none'`, `form-action 'self'` oder spezifische URIs	Zeigen
✔	Blockiert das Laden aktiver Inhalte via HTTP oder FTP	Zeigen
✔	Blockiert das Laden passiver Inhalte via HTTP oder FTP	Zeigen
–	Benutzt die CSP3 Direktive `'strict-dynamic'` für dynamische Skripte (optional)	Zeigen
✔	Blockiert die JavaScript-Funktion `eval()`, indem `'unsafe-eval'` innerhalb `script-src` nicht erlaubt wird	Zeigen
✘	Blockiert Ausführung von Inline-JavaScripts durch Verhindern von `'unsafe-inline'` innerhalb	Zeigen

unbefugte Weitergabe oder Zugriffe auf übermittelte, gespeicherte oder anderweitig verarbeitete personenbezogene Daten zu ergreifen sind. Eine CSP ist ein relativ einfacher Weg, um sicherzustellen, dass Webbesucher nicht unerwartet mit Dritten in Kontakt kommen.

Status	Test	Infos
	`script-src`	
✖	Blockiert Inline-Stilvorlagen durch Verhindern von `'unsafe-inline'` innerhalb `style-src`	Zeigen
✖	Blockiert das Ausführen von Plug-Ins durch Setzen von `object-src` -Beschränkungen	Zeigen

Anleitung

Die Tests für Content Security Richtlinen basieren auf dem Scanner des Mozilla HTTP Observatory Projektes (Mozilla Public License 2.0) von April King, von uns für Webbkoll implementiert. Die Beschreibungstexte sind von der Mozilla Observatory Website entnommen, CC-BY-SA 3.0. Für Fehler oder Ungenauigkeiten sind wir verantwortlich.

⚠ Berichte (CSP, Zertifikat-Transparenz, Netzwerkfehler-Protokolle)

Berichte werden an Dritte gesandt.

Die Direktive `report-uri` des Headers `Expect-CT` instruiert den Browser, Berichte über Expect-CT-Fehler an folgende URI eines Dritten zu senden:

- https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct

Siehe Original Header weiter unten für alle Einzelheiten.

Die Direktive `report-uri` oder `report-to` der Content Security Policy (CSP) in Kombination mit dem Header `Report-To` instruiert den Browser des Benutzers, einen Bericht über Verstöße an festgelegte URI(s) zu senden, wenn gegen die Content Security Policy verstoßen wird. Jeder Bericht ist ein JSON-Objekt, welches Informationen zum Verstoß enthält, u. a. die URL des Dokuments, wo dieser stattfand, und Referrer-Daten. Berichterstattung ist nützlich für Entwickler, um Fehler zu finden und zu beheben, jedoch kann es auch zur Verfolgung (Tracking) verwendet werden.

Der `Expect-CT` -Header kann verwendet werden, um Zertifikatstransparenz-Anforderungen durchzusetzen, und/oder optional Berichte von Verletzungen der Zertifikatstransparenz an einen spezifischen URI zu schicken.

Der Header `NEL` (Network Error Logging – Netzwerkfehler-Protokollierung) instruiert den Browser des Benutzers, Berichte über Netzwerkfehler (z. B. Fehler der DNS-Auflösung, TCP- oder TLS-Verbindungsfehler, HTTP-Statuscodes 4xx oder 5xx) an eine festgelegte URI zu senden. Er kann auch so konfiguriert werden, dass Berichte über erfolgreiche Netzwerk-Anfragen versendet werden. Siehe [1], [2] zu Privatsphäre-Erwägungen.

✖ Referrer Policy

Referrer-Richtlinie nicht gesetzt. Das bedeutet, dass vom Standardwert `no-referrer-when-downgrade` ausgegangen wird, was eine Preisgabe des Referrer in vielen Situationen bedeutet.

Wenn Du auf einen Link klickst, sendet Dein Browser in der Regel den HTTP-Referer - also die Adresse, von der Du kommst - an den Webserver, auf dem sich die Ziel-Website befindet. Auf diese Weise können Websites sehen, woher ihre Besucher kommen. Der Header wird auch gesendet, wenn externe

Anleitung

Ressourcen (wie Bilder, Schriften, JS und CSS) geladen werden.

Referrer-Header sind ein Alptraum für die Privatsphäre, da er es Webseiten und Diensten ermöglicht, Dich im gesamten Web zu verfolgen und Deine Surfgewohnheiten (und damit möglicherweise private, sensible Informationen) preiszugeben, insbesondere wenn dies in Kombination mit Cookies erfolgt.

Durch die Festlegung einer Referrer-Richtlinie ist es für Websites möglich, Browsern mitzuteilen, dass sie keine Referrer verlieren. Mit der Referrer-Richtlinie können Sie eine Richtlinie festlegen, die auf alle angeklickten Links sowie auf alle anderen von der Seite erzeugten Anfragen (Bilder, JS etc.) angewendet wird.

DSGVO: Erwägungsgrund 83, Art. 5.1.c, Art. 25, Art. 32.2
Das Setzen einer Referer Richtlinie ist ein schneller und einfacher Weg zur Datenminimierung (Art. 5.1.c) und stellt sicher, dass Daten nicht unnötigerweise oder unzulässigerweise übermittelt werden (Art. 32.2).

✖ Subresource Integrity (SRI)

Subresource Integrity (SRI) wurden nicht eingebunden. Externe Ressourcen werden über HTTP oder mit relativen URLs geladen src="//...".

Die folgenden Drittanbieter-Ressourcen werden ohne SRI geladen:

Typ	URL
script	`https://ad4m.at/r6rlkfsa.js`
script	`https://retrack-kupona.kuponacdn.de/customers/54025.min.js`
script	`https://download.bitdefender.com/resources/themes/draco/minimize/lite_v2/jslite_v2.v1140.min.js`
css	`https://cdnjs.cloudflare.com/ajax/libs/Swiper/4.5.0/css/swiper.min.css`
css	`https://download.bitdefender.com/resources/themes/draco/minimize/lite_v2/csslite_v2.v929.min.css`
script	`https://cdn.jsdelivr.net/npm/vanilla-lazyload@12.0.0/dist/lazyload.min.js`
script	`https://cdnjs.cloudflare.com/ajax/libs/Swiper/4.5.0/js/swiper.min.js`

> Subresource Integrity (SRI) ist ein Sicherheitsmerkmal, mit dem Browser überprüfen können, ob abgerufene Ressourcen (z.B. von einem CDN) ohne Manipulationen übertragen wurden. Es funktioniert, indem es Dir erlaubt, einen kryptographischen Hash bereitzustellen, mit dem eine geholte Ressource übereinstimmen muß.
>
> Die Verwendung von Content Delivery Networks (CDNs) zum Hosten von Dateien wie Skripten oder Stilvorlagen kann die Leistung einer Website verbessern und die Bandbreite reduzieren. Die Verwendung von CDNs birgt jedoch auch das Risiko, dass wenn ein Angreifer die Kontrolle über ein CDN erlangt, er beliebige bösartige Inhalte in eine Website injizieren kann.
>
> Subresource Integrity minimiert das Risko solcher Angriffe. Es stellt sicher, dass Dateien einer Webanwendung, die von CDN oder sonstigen Quellen stammen, auch ohne Manipulationen geladen werden können.
>
> *— MDN, Subresource Integrity, Mozilla Contributors, CC BY-SA 2.5*

DSGVO: Erwägungsgrund 83, Art. 5.1.f, Art. 25, Art. 32.2
Dies ist eine einfache Maßnahme gegen unbefugte Offenlegung oder Zugriff auf personenbezogene Daten, welche übertragen, gespeichert oder anderweitig verarbeitet werden könnten.

Typ	URL
css	https://fonts.googleapis.com/css?family=Roboto:300,400,400i,500,700,900|Exo+2:300,300i,400,700
script	https://assets.adobedtm.com/8a93f8486ba4/62c1fd5cdcbd/f72a4b9781f8/RC472316cf351947379963ff5bb35b079...
script	https://assets.adobedtm.com/8a93f8486ba4/62c1fd5cdcbd/f72a4b9781f8/RCcc4046503e554f9d879079476ec8932...
script	https://assets.adobedtm.com/8a93f8486ba4/62c1fd5cdcbd/f72a4b9781f8/RC8d5edc14e16f4ef98a5ffd8aa9e943c...
script	https://script.hotjar.com/modules.cbd9b920d05cd9e47f57.js
script	https://static.hotjar.com/c/hotjar-51808.js?sv=6
script	https://www.bitdefender.com/site/Main/TagIT/getparams/?callback=TagIT_getParams_callback&callback2=&...
script	https://www.googletagmanager.com/gtag/js?id=AW-674268845
script	https://assets.adobedtm.com/extensions/EPb56e12d7054b4acea984e91c910051cc/AppMeasurement_Module_Audi...
script	https://assets.adobedtm.com/extensions/EPb56e12d7054b4acea984e91c910051cc/AppMeasurement_Module_Acti...
script	https://assets.adobedtm.com/extensions/EPb56e12d7054b4acea984e91c910051cc/AppMeasurement.min.js
script	https://www.bitdefender.com/site/Main/TagIT/newsessioninit/?callback=&l=de&ch=1639177681
script	https://www.bitdefender.com/scripts/TagIT.v1.min.js?v=43

Typ	URL
script	//assets.adobedtm.com/8a93f8486ba4/62c1fd5cdcbd/launch-b77a56f2d5f1.min.js
script	//www.bitdefender.de/site/Main/generalDigitalData/?p=de:main:showhomepage&dl=de&t=&h=ip-10-122-2-189...
script	//cdn.bizible.com/scripts/bizible.js
script	https://cdn.ravenjs.com/3.26.2/raven.min.js
script	https://consent.cookiebot.com/uc.js
script	https://snap.licdn.com/li.lms-analytics/insight.min.js
script	//cdn.scarabresearch.com/js/198DE47607F5EBDB/scarab-v2.js
script	//static.scarabresearch.com/wpjs/wploader.js?ts=2710
script	https://www.googleadservices.com/pagead/conversion_async.js
script	//static.scarabresearch.com/wpjs/wpes6.js?ts=2710
script	https://cdn.bizible.com/xdc.js?_biz_u=702cbbe8c6dd4bdc9aefd039a526ab05&_biz_h=-417244810&cdn_o=a&jsV...
script	https://fls.doubleclick.net/json?spot=5165113&src=&var=s_3_Integrate_DFA_get_0&host=integrate.112.2o...
script	https://consent.cookiebot.com/4a55b566-7010-4633-9b03-7ba7735be0b6/cc.js?renew=false&referer=www.bit...
script	//www.dwin1.com/11660.js
script	https://sstats.bitdefender.com/b/ss/bitdefenderproduction/10/JS-2.22.3-LBWB/s58289688859250?AQB=1&nd...

Typ	URL
script	`https://tag.demandbase.com/ee38c350.min.js`

Anleitung

Der Subresource Integrity Test basiert auf dem Mozilla HTTP Observatory Scanner (Mozilla Public License 2.0) von April King, von uns für Webkoll implementiert.

HTTP-Kopfzeilen

Status	Kopfzeile	Wert	Ergebnis
✔	X-Content-Type-Options	nosniff	X-Content-Type-Options Header gesetzt auf "nosniff"
ⓘ	X-Frame-Options		X-Frame-Options (XFO) Header fehlt
ⓘ	X-XSS-Protection	1; mode=block	X-XSS-Protection Header gesetzt auf "1; mode=block"

Anleitung

Der Header-Test basiert auf dem Mozilla HTTP Observatory Scanner (Mozilla Public License 2.0) von April King, von uns für Webbkoll implementiert. Die Beschreibungstexte sind von der Mozilla Observatory Website entnommen, CC-BY-SA 3.0.

Ein `X-Content-Type-Options` HTTP Header eines Servers gibt an, dass der jeweils gesendete MIME Content-Type einer Datei nicht verändert werden kann. Das Verhindert ein Ausspähen durch manipulierten MIME-Types oder in anderen Worten: Der Webmaster weiß, was sein Server genau macht.

— MDN, X-Content-Type-Options, Mozilla Contributors, CC BY-SA 2.5

Ein `X-Frame-Options` HTTP Antwort-Header wird verwendet, um einem Browser mitzuteilen, ob eine Seite in einem `<frame>`, `<iframe>` oder `<object>` angezeigt werden darf. Websites können dieses nutzen, um Clickjacking-Angriffe zu verhindern.

Hinweis: Der HTTP-Header `Content-Security-Policy` hat eine Direktive `frame-ancestors`, die diesen veralteten Header in Browsern ersetzt, die das unterstützen.

— MDN, X-Frame-Options, Mozilla Contributors, CC BY-SA 2.5

Der `X-XSS-Protection` -Header wurde von modernen Browsern abgekündigt, die Verwendung kann **zusätzliche** Sicherheitslücken auf dem Client aufwerfen. Daher wird empfohlen, den Header auf `X-XSS-Protection: 0` zu setzen, um den XSS-Auditor abzuschalten und diesem nicht das Standardverhalten zu erlauben, dass der Browser die Antwort handhabt.

— OWASP Cheat Sheet Series, Cross Site Scripting Prevention Cheat Sheet, OWASP CheatSheets Series Team, CC BY 3.0

🔨 DSGVO: Art. 5.1.c, Art. 5.1.f, Art. 25, Art. 32.1-2. Diese Header helfen dabei, das Risiko eines Datenmissbrauchs zu minimieren.

Cookies

First-Party-Cookies (26)

Domain	Name	Wert	Verfällt am	HttpOnly	Secure	SameSite

Domain	Name	Wert	Verfällt am	HttpOnly	Secure	SameSite
.bitdefender.de	scarab.visitor	%226BAF4D54146BE74F%...	2022-12-10 23:08:00Z	✗	✗	✗
.bitdefender.de	aam_uid	24195451089898214994...	2022-03-20 23:08:00Z	✗	✗	✗
.bitdefender.de	s_cc	true	session	✗	✗	✗
.bitdefender.de	s_ppv	de%253Amain%253Ashow...	session	✗	✗	✗
.bitdefender.de	s_tp	2070	session	✗	✗	✗
.bitdefender.de	s_ips	1080	session	✗	✗	✗
.bitdefender.de	AMCV_0E920C0F53DA9E9...	-2121179033%7CMCIDTS...	2023-12-10 23:08:00Z	✗	✓	✓ (None)
.bitdefender.de	s_dfa	bitdefenderproductio...	2021-12-10 23:38:00Z	✗	✗	✗
.bitdefender.de	mbox	session#b63ca4409255...	2023-12-12 23:08:01Z	✗	✗	✗
.bitdefender.de	_biz_flagsA	%7B%22Version%22%3A1...	2022-12-10 23:08:00Z	✗	✗	✗
.bitdefender.de	_hjAbsoluteSessionIn...	1	2021-12-10 23:38:00Z	✗	✗	✓ (Lax)
.bitdefender.de	_hjSession_51808	eyJpZCI6IjUxMTI0MDIz...	2021-12-10 23:38:00Z	✗	✗	✓ (Lax)
.bitdefender.de	_hjFirstSeen	1	2021-12-10 23:38:00Z	✗	✗	✓ (Lax)
.bitdefender.de	_hjSessionUser_51808	eyJpZCI6IjI3OTc5MjQz...	2022-12-10 23:08:00Z	✗	✗	✓ (Lax)
.bitdefender.de	AMCVS_0E920C0F53DA9E...	1	session	✗	✓	✓ (None)
.bitdefender.de	_biz_pendingA	%5B%5D	2022-12-10 23:08:00Z	✗	✗	✗
.bitdefender.de	_biz_nA	1	2022-12-10 23:07:59Z	✗	✗	✗

Domain	Name	Wert	Verfällt am	HttpOnly	Secure	SameSite
.bitdefender.de	_biz_sid	1be0d9	2021-12-10 23:37:59Z	✗	✗	✗
.bitdefender.de	_biz_uid	702cbbe8c6dd4bdc9aef...	2022-12-10 23:07:59Z	✗	✗	✗
.bitdefender.de	at_check	true	session	✗	✗	✗
www.bitdefender.de	_hjIncludedInSession...	1	2021-12-10 23:10:00Z	✗	✗	✓ (Lax)
www.bitdefender.de	_hjIncludedInPagevie...	1	2021-12-10 23:10:00Z	✗	✗	✓ (Lax)
www.bitdefender.de	tagit_params	%7B%22obj%22%3A%5B%5...	session	✗	✗	✗
www.bitdefender.de	tagit_session	1	session	✗	✗	✗
www.bitdefender.de	ab_banner	2	2022-01-09 23:07:59Z	✗	✗	✗
www.bitdefender.de	PHPSESSID	gsp9fvlk49i7ust728p1...	session	✓	✗	✗

Cookies von Dritten (44)

Domain	Name	Wert	Verfällt am	HttpOnly	Secure	SameSite
.ad-srv.net	u8x7eovwf3h6_uid	e6f30fdcb5fa9659	2022-03-10 23:08:01Z	✗	✓	✓ (None)
.ad-srv.net	v930q3phzhqx_uid	516c790408852419	2022-03-10 23:08:01Z	✗	✓	✓ (None)
.adfarm1.adition.com	UserID1	7040214532231333093	2022-03-10 23:08:02Z	✗	✓	✓ (None)
.adform.net	uid	5052959187550399243	2022-02-08 23:08:03Z	✗	✓	✓ (None)
.adform.net	C	1	2022-01-10 23:08:02Z	✗	✓	✓ (None)
.ads.linkedin.com	lang	v=2&lang=en-us	session	✗	✓	✓ (None)

Domain	Name	Wert	Verfällt am	HttpOnly	Secure	SameSite
.adscale.de	cct	1639177685051	2022-12-08 15:34:45Z	✗	✓	✓ (None)
.adscale.de	uu	e4e2d5b2a0b0453d9066...	2022-12-08 15:34:44Z	✗	✓	✓ (None)
.bizible.com	_BUID	702cbbe8c6dd4bdc9aef...	2022-12-10 23:08:00Z	✗	✓	✓ (None)
.bizibly.com	_BUID	36e2fac526403b54641f...	2022-12-10 23:08:00Z	✗	✓	✓ (None)
.casalemedia.com	CMST	YbPd1WGz3dUA	2021-12-11 23:08:05Z	✗	✓	✓ (None)
.casalemedia.com	CMRUM3	0561b3ddd52760Y4LvVg...	2022-12-10 23:08:05Z	✗	✓	✓ (None)
.casalemedia.com	CMPRO	1865	2022-03-10 23:08:05Z	✗	✓	✓ (None)
.casalemedia.com	CMPS	209	2022-03-10 23:08:05Z	✗	✓	✓ (None)
.casalemedia.com	CMID	YbPd1bwiZDh1M653blwa...	2022-12-10 23:08:05Z	✗	✓	✓ (None)
.crwdcntrl.net	_cc_aud	"ABR4XmNgYGBI3Hz3ApC...	2022-09-06 23:08:01Z	✗	✓	✓ (None)
.crwdcntrl.net	_cc_cc	"ACZ4XmNQMDM1MUixMDB...	2022-09-06 23:08:01Z	✗	✓	✓ (None)
.crwdcntrl.net	_cc_id	6540d801b3279911ad79...	2022-09-06 23:09:01Z	✗	✓	✓ (None)
.crwdcntrl.net	_cc_dc	1	2022-09-06 23:09:01Z	✗	✓	✓ (None)
.demdex.net	dextp	60-1-1639177680292|7...	2022-06-08 23:08:00Z	✗	✓	✓ (None)
.demdex.net	demdex	24195451089898214994...	2022-06-08 23:08:01Z	✗	✓	✓ (None)
.doubleclick.net	IDE	AHWqTUksGrWH2mlws8--...	2023-01-04 23:08:00Z	✓	✓	✓ (None)

Domain	Name	Wert	Verfällt am	HttpOnly	Secure	SameSite
.dpm.demdex.net	dpm	24195451089898214994...	2022-06-08 23:08:01Z	✗	✓	✓ (None)
.ih.adscale.de	tu	4#2967558034#25~Y4Lv...	2022-12-08 15:34:45Z	✗	✓	✓ (None)
.linkedin.com	li_gc	MTswOzE2MzkxNzc2ODA7...	2023-12-09 21:51:27Z	✗	✓	✓ (None)
.linkedin.com	lang	v=2&lang=en-us	session	✗	✓	✓ (None)
.linkedin.com	lidc	"b=VGST06:s=V:r=V:a=...	2021-12-11 23:08:00Z	✗	✓	✓ (None)
.linkedin.com	bcookie	"v=2&5920401c-20f5-4...	2023-12-11 10:45:32Z	✗	✓	✓ (None)
.linkedin.com	AnalyticsSyncHistory	AQJcIVjXU7-o2gAAAX2m...	2022-01-09 23:08:00Z	✗	✓	✓ (None)
.linkedin.com	UserMatchHistory	AQJSURvxP0BueQAAAX2m...	2022-01-09 23:08:00Z	✗	✓	✓ (None)
.mathtag.com	mt_misc	mt_bt:1639177691	2022-01-09 23:08:12Z	✗	✓	✓ (None)
.mathtag.com	uuid	72a161b3-ddd1-4000-b...	2023-01-07 23:08:01Z	✗	✓	✓ (None)
.redintelligence.net	8lcfmzhxc8d6_uid	cafb645ffaf36484	2022-03-10 23:08:01Z	✗	✓	✓ (None)
.rlcdn.com	pxrc	CNC7z40GEgUI6AcQABIG...	2022-02-08 23:08:00Z	✗	✓	✓ (None)
.rlcdn.com	rlas3	ZJp4oX3Ae4E7TaWB9x2D...	2022-12-10 23:08:00Z	✗	✓	✓ (None)
.smartadserver.com	csync	132:Y4LvVgl4wVWDezqJ...	2023-01-09 23:08:06Z	✗	✓	✓ (None)
.smartadserver.com	TestIfCookieP	ok	2023-01-09 23:08:06Z	✗	✓	✓ (None)
.smartadserver.com	pid	571198213942159282 1	2023-01-09 23:08:06Z	✗	✓	✓ (None)

Domain	Name	Wert	Verfällt am	HttpOnly	Secure	SameSite
.twitter.com	personalization_id	"v1_O+0X8beqZhtsN1mC...	2023-12-10 23:08:01Z	✗	✓	✓ (None)
.www.linkedin.com	bscookie	"v=1&2021121023080 01...	2023-12-11 10:45:34Z	✓	✓	✓ (None)
recommender-eu.scarabresearch.com	cdv	691232578CBD3152	2022-12-11 04:57:13Z	✗	✓	✓ (None)
recommender-eu.scarabresearch.com	s	7E569512F58188CF	session	✗	✓	✓ (None)
recommender.scarabresearch.com	cdv	6BAF4D54146BE74F	2022-12-11 04:57:13Z	✗	✓	✓ (None)
recommender.scarabresearch.com	s	255834CFCC5499A1	session	✗	✓	✓ (None)

HttpOnly bedeutet, dass Cookies nur vom Server gelesen werden können und nicht durch JavaScript im Webbrowser. Das verhindert XSS (Cross-Site Scripting) Angriffe.

Secure bedeutet, dass ein Cookie nur über eine sichere (HTTPS) Verbindung gesendet wird. Das verhindert MITM (Man-in-the-Middle) Angriffe.

SameSite wird verwendet um dem Browser mitzuteilen, dass er nur dann Cookies senden darf, wenn die Anfrage von der gleichen Seite stammt. Das verhindert CSRF (Cross-Site Request Forgery) Angriffe.

GDPR: Erwägungsgrund 60, Erwägungsgrund 61, Erwägungsgrund 69, Erwägungsgrund 70, Erwägungsgrund 75, Erwägungsgrund 78, Art. 5.1.a, Art. 5.1.c, Art. 5.1.e, Art. 21, Art. 22, Art. 32.

e-PD (2002/58/EC). Rec. 24, 25, Art. 5.2.

e-PD revised (2009/136/EC). Rec. 65, 66.

Mehr Informationen

localStorage

LocalStorage verwendet:

Schlüssel	Wert
Demandbase.AdobeLaunch.demandbaseDataElement1	"(Non-Company Visi (Non-...
Demandbase.AdobeLaunch.demandbaseDataElement2	"(Non-Company Visi (Non-...
Demandbase.AdobeLaunch.demandbaseDataElement3	""

Wie Cookies speichern Web-Storage-Daten im Webbrowser eines Benutzers. Doch anders als Cookies wird ein Web Storage nicht über HTTP-Anfragen abgefragt, sondern immer nur direkt durch den Browser (mit JavaScript). Im Vergleich zu Cookies können deutlich mehr Daten gespeichert werden.

Es gibt zwei Arten: `LocalStorage` mit dauerhaft gespeicherten Daten (auch wenn der Browser geschlossen wird) und `SessionStorage` , das gelöscht wird sobald die Session einer Website beendet wird (anders Verhalten wie Session Cookies). Eine SessionStorage Sitzung gilt immer *pro Fenster/Tab*.

Dies kann verwendet werden, um Benutzer zu

Schlüssel	Wert
Demandbase.AdobeLaunch.demandbaseDataElement4	""
Demandbase.AdobeLaunch.demandbaseDataElement5	""
Demandbase.AdobeLaunch.raw	{"registry_company_name":"Hetzner Online GmbH","re...
_wp_storage_test	val
com.adobe.reactor.dataElementCookiesMigrated	true
sc_timings	{"ts":1639177680846,"t":"2,824,903,896,1637,1640|l...
wps-1	{}

verfolgen und Profile zu erstellen indem JavaScript-Code den Speicher ausliest und an einen Server sendet.

🔨 DSGVO: Gleiche Bestimmungen wie bei Cookies weiter oben.

Drittanfragen (Third Party)

143 Anfragen (143 sicher, 0 unsicher) an **64** einzigartige Hosts.

Eine "Third-Party-Anfrage" ist ein Abruf von Ressourcen von einer anderen Domain als `bitdefender.de` oder einer ihrer Subdomains.

Host	IP	Einordnung	URLs
5994599.fls.doubleclick.net	142.250.74.38	FingerprintingGeneral, Advertising (Google)	Zeigen (2)
6773135.fls.doubleclick.net	142.250.74.134	FingerprintingGeneral, Advertising (Google)	Zeigen (2)
a.twiago.com	85.215.5.31		Zeigen (1)
ad.ad-srv.net	138.201.63.150		Zeigen (4)
ad11.adfarm1.adition.com	85.114.159.112	Advertising (ADITION)	Zeigen (2)
ad13.adfarm1.adition.com	217.79.188.54	Advertising (ADITION)	Zeigen (2)
ad4m.at	104.21.192.121	Advertising (AdvancedStore)	Zeigen (1)

Host	IP	Einordnung	URLs
adservice.google.com	142.250.74.34	Content (Google)	Zeigen (2)
analytics.twitter.com	104.244.42.131	Social (Twitter)	Zeigen (1)
api.company-target.com	13.33.240.96	Analytics (Demandbase)	Zeigen (2)
as.ad4m.at	104.21.192.120	Advertising (AdvancedStore)	Zeigen (5)
assets.adobedtm.com	104.103.65.16		Zeigen (7)
bitdefender.demdex.net	52.48.8.186	FingerprintingGeneral, Advertising (Adobe)	Zeigen (1)
cdn.bizible.com	152.195.15.58		Zeigen (3)
cdn.bizibly.com	152.195.15.58		Zeigen (1)
cdn.jsdelivr.net	104.16.88.20		Zeigen (1)
cdn.ravenjs.com	151.101.130.217		Zeigen (1)
cdn.scarabresearch.com	13.33.240.52		Zeigen (1)
cdnjs.cloudflare.com	104.16.19.94		Zeigen (2)
cm.everesttech.net	52.51.88.158	FingerprintingGeneral, Advertising (Adobe)	Zeigen (1)
cm.g.doubleclick.net	142.250.74.34	FingerprintingGeneral, Advertising (Google)	Zeigen (2)
code.jquery.com	69.16.175.42		Zeigen (1)
consent.cookiebot.com	62.115.252.35		Zeigen (2)

Host	IP	Einordnung	URLs
consentcdn.cookiebot.com	23.61.226.50		Zeigen (1)
download.bitdefender.com	192.229.220.142		Zeigen (18)
dpm.demdex.net	34.253.56.231	FingerprintingGeneral, Advertising (Adobe)	Zeigen (7)
dsum-sec.casalemedia.com	104.103.65.27	Advertising (Casale Media)	Zeigen (2)
fls.doubleclick.net	142.250.74.134	FingerprintingGeneral, Advertising (Google)	Zeigen (1)
fonts.googleapis.com	142.250.74.74	Content (Google)	Zeigen (2)
fonts.gstatic.com	142.250.74.99	Content (Google)	Zeigen (5)
hal9000.redintelligence.net	88.99.165.19		Zeigen (2)
idsync.rlcdn.com	35.244.174.68	Advertising (TowerData)	Zeigen (2)
ih.adscale.de	54.93.80.4	Advertising (adscale)	Zeigen (2)
imagesrv.adition.com	217.79.188.60	Advertising (ADITION)	Zeigen (2)
in.hotjar.com	54.75.159.38	Analytics (Hotjar)	Zeigen (1)
mid.rkdms.com	34.236.203.109	Analytics, Advertising (Merkle)	Zeigen (2)
ml314.com	34.247.104.176	Analytics (Bombora)	Zeigen (1)
p1.zemanta.com	34.120.59.192	Advertising (Zemanta)	Zeigen (1)
pagead2.googlesyndication.com	142.250.74.66	FingerprintingGeneral, Advertising (Google)	Zeigen (1)

Host	IP	Einordnung	URLs
pixel.mathtag.com	104.103.64.237	FingerprintingGeneral, Advertising (MediaMath)	Zeigen (10)
px.ads.linkedin.com	144.2.12.5	Social (LinkedIn)	Zeigen (2)
r.adserver01.de	212.83.50.108		Zeigen (1)
recommender-eu.scarabresearch.com	52.57.60.131		Zeigen (1)
recommender.scarabresearch.com	18.185.10.202		Zeigen (1)
retrack-kupona.kuponacdn.de	18.159.68.209		Zeigen (1)
rtb-csync.smartadserver.com	185.86.137.133	Advertising (SmartAdServer)	Zeigen (1)
s2.adform.net	37.157.2.247	Advertising (Adform)	Zeigen (1)
script.hotjar.com	13.33.240.122	Analytics (Hotjar)	Zeigen (1)
snap.licdn.com	178.18.231.146	Social (LinkedIn)	Zeigen (1)
sstats.bitdefender.com	13.36.218.177		Zeigen (2)
starget.bitdefender.com	18.203.190.43		Zeigen (1)
static.hotjar.com	13.33.240.36	Analytics (Hotjar)	Zeigen (1)
static.scarabresearch.com	52.85.112.33		Zeigen (2)
sync.crwdcntrl.net	52.30.14.23	FingerprintingGeneral, Analytics (Lotame)	Zeigen (2)

Host	IP	Einordnung	URLs
tag.demandbase.com	52.85.112.52	Analytics (Demandbase)	Zeigen (1)
track.adform.net	37.157.6.252	Advertising (Adform)	Zeigen (7)
vars.hotjar.com	52.85.112.62	Analytics (Hotjar)	Zeigen (1)
vc.hotjar.io	13.33.240.109		Zeigen (1)
webchannel-content-service.scarabresearch.com	34.117.30.199		Zeigen (1)
www.bitdefender.com	104.18.169.222		Zeigen (3)
www.dwin1.com	13.33.240.50	FingerprintingGeneral, Advertising (Awin)	Zeigen (1)
www.googleadservices.com	216.58.207.226	FingerprintingGeneral, Advertising (Google)	Zeigen (1)
www.googletagmanager.com	216.58.211.8		Zeigen (1)
www.linkedin.com	13.107.42.14	Social (LinkedIn)	Zeigen (1)

Wir nutzen Mozillas Version der Open-Source-Tracker-Liste von Disconnect, um Hosts zu klassifizieren.

🔨 GDPR: Erwägungsgrund 69, Erwägungsgrund 70, Art. 5.1.b-c, Art. 25.

IP-Adresse

Der Server **www.bitdefender.de** hatte während unseres Tests die IP-Adresse **104.18.24.28**.

Informationen zu dieser IP-Adresse findest du bspw. mithilfe folgender Drittanbieter-Werkzeuge:

- bgp.he.net
- KeyCDN
- iplocation.io

Bei der Benutzung von Hilfsmitteln zur Geolokation ist zu beachten, dass das vermutete Land falsch sein kann, insbesondere bei Webauftritten, die CDNs verwenden.

ⓘ Einige Seiten nutzen ein CDN, Content Delivery Networks. In diesem Falle hängt der angezeigte Serverstandort vom Standort des Besuchers ab. Webbkoll als Tool ist auf einem Server in Finnland beheimatet.

🔨 Mit der DSGVO gelten alle EU/EWR-Länder als gleichermaßen vertrauenswürdig, so dass es keinen besonderen Grund gibt, ein EU-Land als mehr oder weniger zuverlässig oder vertrauenswürdig zu betrachten. Die Bedeutung des Standorts eines Servers kommt nur im Rahmen der DSGVO Art. 23, Beschränkung zum Tragen, bei denen sich die Mitgliedstaaten auf eine Reihe von Gründen, insbesondere auf die nationale Sicherheit, berufen können, die es ihnen ermöglicht, den Schutz für

Besucher oder Webseiten-Betreiber aufzuheben.

Für Nicht-EU/EWR-Gebiete hängt es von (DSGVO Art. 44) ab. Für eine Website sind Übertragungen wahrscheinlich auf Abwägungsentscheidungen nach (Art. 45) der Europäischen Kommission angewiesen, wenn in einem Drittland nach ihren Rechtsvorschriften angemessene Datenschutzmaßnahmen vorgesehen sind. Abwägungsentscheidungen können jedoch nicht immer heran gezogen werden wie der Europäische Gerichtshof 2015 (C-362/14) zeigt. Verbindliche Unternehmensregeln (Art. 47) oder Standardklauseln (Art. 46) können auch zur Datenübermittlung herangezogen werden. Das ist aber mangels ausreichender Gerichts- und Datenschutzurteile noch auf rechtlich wackeliger Basis.

Originalkopfzeilen

Kopfzeile	Wert
cache-control	no-store, no-cache, must-revalidate, post-check=0, pre-check=0
cf-cache-status	DYNAMIC
cf-ray	6bba21ee78c3f14e-ARN
content-encoding	gzip
content-security-policy	frame-src *.2checkout.com *.bitdefender.com *.bitdefender.biz *.bitdefender.net *.bitdefender.fr *.bitdefender.de *.bitdefender.com.au *.bitdefender.co.uk *.bitdefender.es *.bitdefender.it *.bitdefender.pt *.bitdefender.com.br *.bitdefender.ro *.bitdefender.nl *.bitdefender.be *.bitdefender.se bitdefender.marketing.adobe.com download.bitdefender.com *.facebook.com *.doubleclick.net *.adsrvr.org *.mathtag.com *.google.com *.google.ro *.flashtalking.com *.amazon-adsystem.com *.livechatinc.com *.twitter.com *.cedexis.com *.cedexis-test.com *.youtube.com *.soundcloud.com *.hubspot.com *.cookiebot.com *.vimeo.com *.edgecastcdn.net *.linkedin.com *.hsforms.com *.cloudfront.net *.edgecastdns.net *.hotjar.com *.zanox.ws *.zanox.com *.usemax.de usemax.de bitdefender.demdex.net dpm.demdex.net *.omniture.com widget.trustpilot.com *.2o7.net *.omtrdc.net *.demdex.net assets.adobedtm.com api-eu.boldchat.com livechat-eu.boldchat.com *.youtube-nocookie.com *.instagram.com instawidget.net consentcdn.cookiebot.com recommender.scarabresearch.com *.zenaps.com hal9000.redintelligence.net pixel.xonaz.com static-hello.bitdefender.com tags.dynamo.one *.redintelligence.net 20787700p.rfihub.com pixel.xonazz.com *.adobe.com *.outgrow.us bitdefender.applytojob.com *.alchemer.com *.adyen.com *.paypal.com paypal.com ad.ad-srv.net fullstory.com *.bitdefender.co.jp bitdefender.co.jp new.bitdefender.co.uk store.bitdefender.com bitdefender-html.test
content-type	text/html
date	Fri, 10 Dec 2021 23:07:59 GMT
expect-ct	max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"

Kopfzeile	Wert
expires	Thu, 19 Nov 1981 08:52:00 GMT
pragma	no-cache
server	cloudflare
set-cookie	PHPSESSID=gsp9fvlk49i7ust728p139ham0; path=/; HttpOnly bd112=i65WKi3KUbJSyigpKbCK0Y%2FRLy8v10vKLElJTUvNS0kt0ktJjdFX0lEqycxNLS5JzC1QsjI0M7Y0NDc3M7esjQUA; expires=Sat, 10-Dec-2022 23:07:59 GMT; path=/; domain=.bitdefender.com ab_banner=2; expires=Sun, 09-Jan-2022 23:07:59 GMT Section=0; expires=Fri, 10-Dec-2021 23:07:59 GMT; path=/; domain=.bitdefender.com
strict-transport-security	max-age=31536000; includeSubDomains; preload
x-content-security-policy	frame-src *.2checkout.com *.bitdefender.com *.bitdefender.biz *.bitdefender.net *.bitdefender.fr *.bitdefender.de *.bitdefender.com.au *.bitdefender.co.uk *.bitdefender.es *.bitdefender.it *.bitdefender.pt *.bitdefender.com.br *.bitdefender.ro *.bitdefender.nl *.bitdefender.be *.bitdefender.se bitdefender.marketing.adobe.com download.bitdefender.com *.facebook.com *.doubleclick.net *.adsrvr.org *.mathtag.com *.google.com *.google.ro *.flashtalking.com *.amazon-adsystem.com *.livechatinc.com *.twitter.com *.cedexis.com *.cedexis-test.com *.youtube.com *.soundcloud.com *.hubspot.com *.cookiebot.com *.vimeo.com *.edgecastcdn.net *.linkedin.com *.hsforms.com *.cloudfront.net *.edgecastdns.net *.hotjar.com *.zanox.ws *.zanox.com *.usemax.de usemax.de bitdefender.demdex.net dpm.demdex.net *.omniture.com widget.trustpilot.com *.2o7.net *.omtrdc.net *.demdex.net assets.adobedtm.com api-eu.boldchat.com livechat-eu.boldchat.com *.youtube-nocookie.com *.instagram.com instawidget.net consentcdn.cookiebot.com recommender.scarabresearch.com *.zenaps.com hal9000.redintelligence.net pixel.xonaz.com static-hello.bitdefender.com tags.dynamo.one *.redintelligence.net 20787700p.rfihub.com pixel.xonazz.com *.adobe.com *.outgrow.us bitdefender.applytojob.com *.alchemer.com *.adyen.com *.paypal.com paypal.com ad.ad-srv.net fullstory.com *.bitdefender.co.jp bitdefender.co.jp new.bitdefender.co.uk store.bitdefender.com bitdefender-html.test
x-content-type-options	nosniff
x-webkit-csp	frame-src *.2checkout.com *.bitdefender.com *.bitdefender.biz *.bitdefender.net *.bitdefender.fr *.bitdefender.de *.bitdefender.com.au *.bitdefender.co.uk *.bitdefender.es *.bitdefender.it *.bitdefender.pt *.bitdefender.com.br *.bitdefender.ro *.bitdefender.nl *.bitdefender.be *.bitdefender.se bitdefender.marketing.adobe.com download.bitdefender.com *.facebook.com *.doubleclick.net *.adsrvr.org *.mathtag.com *.google.com *.google.ro *.flashtalking.com *.amazon-adsystem.com *.livechatinc.com *.twitter.com *.cedexis.com *.cedexis-test.com *.youtube.com *.soundcloud.com *.hubspot.com *.cookiebot.com *.vimeo.com *.edgecastcdn.net *.linkedin.com *.hsforms.com *.cloudfront.net *.edgecastdns.net *.hotjar.com *.zanox.ws *.zanox.com *.usemax.de usemax.de bitdefender.demdex.net dpm.demdex.net *.omniture.com widget.trustpilot.com *.2o7.net *.omtrdc.net *.demdex.net assets.adobedtm.com api-eu.boldchat.com livechat-eu.boldchat.com *.youtube-nocookie.com *.instagram.com instawidget.net consentcdn.cookiebot.com recommender.scarabresearch.com *.zenaps.com hal9000.redintelligence.net pixel.xonaz.com static-hello.bitdefender.com tags.dynamo.one *.redintelligence.net 20787700p.rfihub.com pixel.xonazz.com *.adobe.com *.outgrow.us bitdefender.applytojob.com *.alchemer.com *.adyen.com *.paypal.com paypal.com ad.ad-srv.net fullstory.com *.bitdefender.co.jp bitdefender.co.jp new.bitdefender.co.uk store.bitdefender.com bitdefender-html.test
x-xss-protection	1; mode=block

Was genau prüft das Tool (und was nicht)

Dieses Tool simuliert den Aufruf einer Website mit einem typischen Webbrowser. Der Browser hat keine Addons/Erweiterungen und die Do-Not-Track Einstellungen sind nicht aktiviert, da das die Standardeinstellung in den meisten Browsern ist.

Dateien wie Bilder, Skripte und CSS-Stilvorlagen werden zwar geladen, das Tool führt jedoch keine Interaktionen mit der Website aus — es werden keine Links angeklickt und keine Formulare abgeschickt.

Hinweis: Fehler können passieren. Die Ergebnisse erheben keinen Anspruch auf 100% Richtigkeit. Dieses Tool ist auch nicht als Analyse gedacht sondern eher als Ausgangspunkt für Website-Betreiber zur weiteren Verbesserung.

Text zu HTTPS teilweise adaptiert von The HTTPS-Only Standard (Public Domain). Hier klicken für weitere Informationen.

Testergebnisse werden auf unserem Server für 24 Stunden im Arbeitsspeicher gehalten. Wir zeigen keine Liste zuletzt getesteter URLs. Wir verwenden keine URLs oder Testergebnisse. Wir loggen keine IP-Adressen. Wir verwenden einen essenziellen Session-Cookie, um CSRF-Attacken zu verhindern.

Entwickelt von dataskydd**.net**.

Der Quellcode ist auf GitHub verfügbar.

Feedback? Fragen? info@dataskydd.net

Twitter: @dataskyddnet

Unterstütze uns

e1f569b 2021-11-24 16:00:04 +0100