Hinweis: Dieser Demo-Report wurde aus einer echten Kundenseite zu Beginn der Zusammenarbeit generiert. Daher wurden aus Datenschutzgründen sämtliche externen Verlinkungen sowie Hinweise auf den Kunden entfernt.

Datenschutz- und Sicherheits-Report für Ihre Webseite

Website: www.Ihre Domain.de
Zeitpunkt des Scans: 22.01.2023 01:12

Risikobewertung

B	29	28	
Risiko-Score	Externe Dienste gefunden	Cookies gefunden	Datenschutzerklärung gefunden

Die Website läuft im Netzwerk von **Hetzner Online GmbH**. Der Serverstandort ist Deutschland.

Bei der Prüfung der Server-Sicherheit sind eine oder mehrere mögliche Sicherheitsrisiken gefunden worden. Wenn nicht schon geschehen, so sollten Sie dies durch Ihre Agentur oder einen Sicherheitsexperten prüfen lassen.

Sie setzen auf Ihrer Website die Consent Management Software **Borlabs Cookie** ein, um vom Benutzer eine Einwilligung zum Setzen von Cookies zu einzuholen.

Ihr Consent Management Software ist nicht korrekt konfiguriert - Ihre Website lädt ohne Einwilligung des Users nicht notwendige Dienste.

Wir konnten keine nicht notwendigen Cookies identifizieren, die ohne Einwilligung des Benutzers gesetzt werden. Achtung: Wir untersuchen nicht, ob das Einholen der Einwilligung DSGVO-konform erfolgt!

Ihre Website lädt ohne Einwilligung des Benutzers mindestens **4 nicht notwendige Dienste**. Dies ist nicht rechtssicher, da sowohl der Europäische Gerichtshof 2019 als auch der Bundesgerichtshof 2020 geurteilt haben, dass dafür (analog zum Setzen von Cookies) eine aktive Einwilligung erforderlich ist.

Ihre Website lädt mindestens 11 Externe Dienste, die per IP-Adresse und Cookies personenbezogene Daten aus dem Rechtsraum der EU in Drittstaaten ausleiten, ohne dass eine Einwilligung des Benutzers vorliegt.

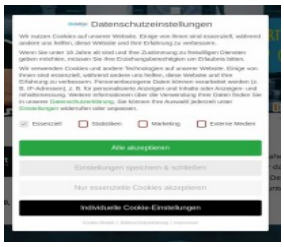
Sie setzen Google Analytics mit aktivierter IP-Anonymisierung ein.

Sie binden **4 Externe Dienste** in Ihre Website ein, zu denen wir in der Datenschutzerklärung keinen Hinweis finden konnten. Damit verstoßen Sie gegen Ihre Informationspflicht nach Art. 13 der DSGVO.

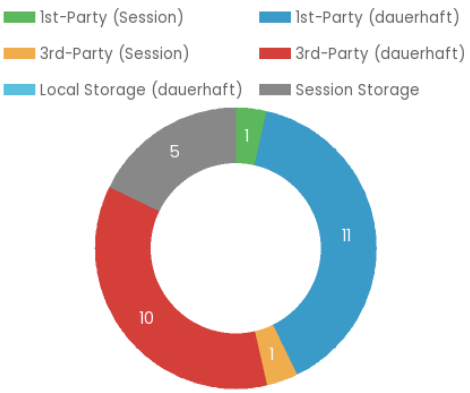
Bitte beachten Sie, dass trotz aller Sorgfalt bei der Untersuchung nicht ausgeschlossen werden kann, dass die Website Datenschutzschwachstellen aufweist, die in diesem Report nicht aufgezeigt werden. Wir können keine Haftung für die Vollständigkeit dieses Reports übernehmen.

Ansicht Startseite

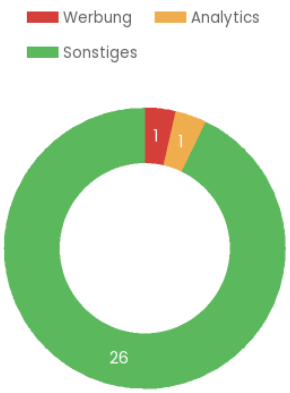
Hinweis:
Hier wird im Original-Report die Startseite des Kunden vor der Annahme aller Cookies dargestellt.



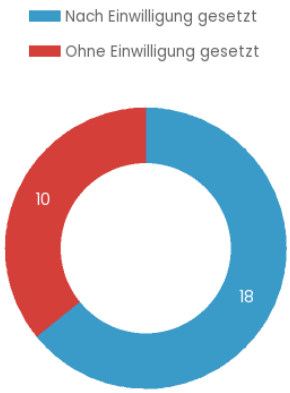
Cookies und Web-Speicher



Cookie-Typ



Verwendung



Einwilligung zum Setzen

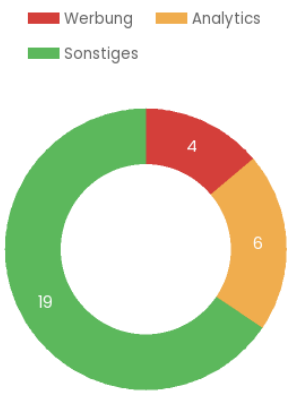
Cookies und Web-Speicher Übersicht

Name	Typ	Speicherdauer (Tage)	Domain	Quelle	Datentransfer	Zweck	Einwilligung erteilt
__cf_bm Auf Unterseite gefunden (6.01.23 04:15)	3rd-Party (dauerhaft)	1	vimeo.com	Unbekannt		Unbekannt	Nein
_fbp Auf Unterseite gefunden (6.01.23 04:15)	1st-Party (dauerhaft)	90	Ihre-Domain.de	Facebook Pixel	Ja (USA)	Werbung	Ja
_gcl_au Auf Unterseite gefunden (6.01.23 04:15)	1st-Party (dauerhaft)	90	Ihre-Domain.de	Unbekannt		Unbekannt	Ja
_rdt_uuid Auf Unterseite gefunden (6.01.23 04:15)	1st-Party (dauerhaft)	90	Ihre-Domain.de	Unbekannt		Unbekannt	Nein
_scid Auf Unterseite gefunden (6.01.23 04:15)	1st-Party (dauerhaft)	400	Ihre-Domain.de	Unbekannt		Unbekannt	Ja
_tt_enable_cookie Auf Unterseite gefunden (6.01.23 04:15)	1st-Party (dauerhaft)	390	Ihre-Domain.de	Unbekannt		Unbekannt	Ja

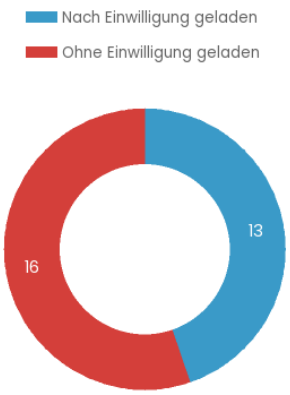
Name	Typ	Speicherdauer (Tage)	Domain	Quelle	Datentransfer	Zweck	Einwilligung erteilt
_ttp Auf Unterseite gefunden (6.01.23 04:15)	3rd-Party (dauerhaft)	390	tiktok.com	TikTok	Ja (China)	Soziale Medien	Ja
AnalyticsSyncHistory Auf Unterseite gefunden (6.01.23 04:15)	3rd-Party (dauerhaft)	30	linkedin.com	LinkedIn Widgets	Ja (USA)	Soziale Medien	Ja
bcookie Auf Unterseite gefunden (6.01.23 04:15)	3rd-Party (dauerhaft)	365	linkedin.com	LinkedIn	Ja (USA)	Funktional	Ja
borlabs-cookie Auf Unterseite gefunden (6.01.23 04:15)	1st-Party (dauerhaft)	365	Ihre-Domain.de	Unbekannt		Unbekannt	Ja
bscookie Auf Unterseite gefunden (6.01.23 04:15)	3rd-Party (dauerhaft)	365	linkedin.com	LinkedIn	Ja (USA)	Funktional	Ja
et_oip Auf Unterseite gefunden (6.01.23 04:15)	1st-Party (dauerhaft)	30	Ihre-Domain.de	Unbekannt		Unbekannt	Nein
fbssls_ Auf Unterseite gefunden (6.01.23 04:15)	Session Storage	0		Unbekannt		Unbekannt	Nein
lang Auf Unterseite gefunden (6.01.23 04:15)	3rd-Party (Session)	0	linkedin.com	LinkedIn Widgets	Ja (USA)	Soziale Medien	Ja
li_gc Auf Unterseite gefunden (6.01.23 04:15)	3rd-Party (dauerhaft)	180	linkedin.com	LinkedIn Widgets	Ja (USA)	Soziale Medien	Ja
lidc Auf Unterseite gefunden (6.01.23 04:15)	3rd-Party (dauerhaft)	1	linkedin.com	LinkedIn	Ja (USA)	Funktional	Ja
ln_or Auf Unterseite gefunden (6.01.23 04:15)	1st-Party (dauerhaft)	1	Ihre-Domain.de	LinkedIn Analytics	Ja (USA)	Analytics	Ja
PHPSESSID Auf Unterseite gefunden (6.01.23 04:15)	1st-Party (Session)	0	Ihre-Domain.de	Webserver		Funktional	Nein
player Auf Unterseite gefunden (6.01.23 04:15)	3rd-Party (dauerhaft)	365	vimeo.com	Vimeo	Ja (USA)	Audio/Video-Player	Nein
tl_9940_11716_7 Auf Unterseite gefunden (6.01.23 04:15)	1st-Party (dauerhaft)	30	Ihre-Domain.de	Unbekannt		Unbekannt	Nein
tlf_7 Auf Unterseite gefunden (6.01.23 04:15)	1st-Party (dauerhaft)	2	Ihre-Domain.de	Unbekannt		Unbekannt	Nein
tt_appInfo Auf Unterseite gefunden (6.01.23 04:15)	Session Storage	0		TikTok	Ja (China)	Soziale Medien	Ja
tt_pageId Auf Unterseite gefunden (6.01.23 04:15)	Session Storage	0		Unbekannt		Unbekannt	Ja
tt_pixel_session_index Auf Unterseite gefunden (6.01.23 04:15)	Session Storage	0		TikTok	Ja (China)	Soziale Medien	Ja
tt_sessionId Auf Unterseite gefunden (6.01.23 04:15)	Session Storage	0		TikTok	Ja (China)	Soziale Medien	Ja
tve_leads_unique Auf Unterseite gefunden (6.01.23 04:15)	1st-Party (dauerhaft)	30	Ihre-Domain.de	Unbekannt		Unbekannt	Nein

Name	Typ	Speicherdauer (Tage)	Domain	Quelle	Datentransfer	Zweck	Einwilligung erteilt
UserMatchHistory Auf Unterseite gefunden (6.01.23 04:15)	3rd-Party (dauerhaft)	30	linkedin.com	LinkedIn	Ja (USA)	Funktional	Ja
vuid Auf Unterseite gefunden (6.01.23 04:15)	3rd-Party (dauerhaft)	400	vimeo.com	Vimeo	Ja (USA)	Audio/Video-Player	Nein

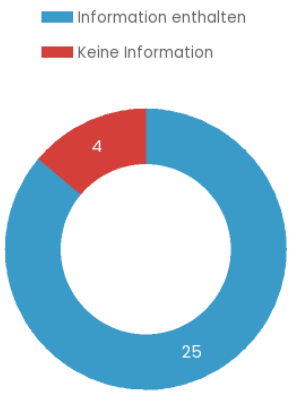
Externe Dienste



Verwendung



Einwilligung zum Laden



Information in Datenschutzerklärung

Externe Dienste Übersicht

Name	Domain	Quelle	Datentransfer	Zweck	Einwilligung erteilt	Information in Datenschutzerklärung
Akamai Technologies Auf 5 Unterseiten gefunden (6.01.23 04:15)	akamaized.net	Akamai Technologies	Ja (USA)	Web-Speicher	Nein	Nein
Borlabs Cookie	Ihre-Domain.de (*Lokaler Server*)	BORLABS		Consent Management		Ja
DoubleClick Auf Start- und 67 Unterseiten gefunden (6.01.23 04:15)	doubleclick.net	Google	Ja (USA)	Werbung	Ja	Ja
etracker Auf allen Seiten gefunden (6.01.23 04:15)	etracker.com	etracker GmbH		Analytics	Nein	Ja
Facebook CDN Auf 3 Unterseiten gefunden (6.01.23 04:15)	fbcdn.net	Facebook	Ja (USA)	Web-Speicher	Nein	Ja
Facebook Pixel Auf Start- und 67 Unterseiten gefunden (6.01.23 04:15)	connect.facebook.net/*/fbevents.js	Facebook	Ja (USA)	Werbung	Ja	Ja
Facebook Social Plugins Auf 3 Unterseiten gefunden (6.01.23 04:15)	www.facebook.com	Facebook	Ja (USA)	Soziale Medien	Nein	Ja
fontawesome.com Auf allen Seiten gefunden (6.01.23 04:15)	fontawesome.com			Web-Speicher	Nein	Nein
Google Auf Start- und 12 Unterseiten gefunden (6.01.23 04:15)	google.com	Google	Ja (USA)	Funktional	Ja	Ja
Google Analytics Auf Start- und 67 Unterseiten gefunden (6.01.23 04:15)	google-analytics.com	Google	Ja (USA)	Analytics	Ja	Ja
Google Fonts Auf Start- und 12 Unterseiten gefunden (6.01.23 04:15)	fonts.gstatic.com	Google	Ja (USA)	Funktional	Ja	Ja

Name	Domain	Quelle	Datentransfer	Zweck	Einwilligung erteilt	Information in Datenschutzerklärung
Google Photos Auf Start- und 12 Unterseiten gefunden (6.01.23 04:15)	ggpht.com	Google	Ja (USA)	Web-Speicher	Ja	Ja
Google Tag Manager Auf allen Seiten gefunden (6.01.23 04:15)	googletagmanager.com	Google	Ja (USA)	Funktional	Nein	Ja
Google Video Auf Unterseite gefunden (6.01.23 04:15)	googlevideo.com	Google	Ja (USA)	Externer Inhalt	Ja	Ja
Gravatar Auf 19 Unterseiten gefunden (6.01.23 04:15)	gravatar.com	Automattic	Ja (USA)	Soziale Medien	Nein	Ja
Instagram Auf Unterseite gefunden (6.01.23 04:15)	instagram.com	Facebook	Ja (USA)	Funktional	Nein	Ja
LinkedIn Ads Auf Start- und 67 Unterseiten gefunden (6.01.23 04:15)	ads.linkedin.com	Microsoft	Ja (USA)	Werbung	Ja	Ja
LinkedIn Analytics Auf Start- und 67 Unterseiten gefunden (6.01.23 04:15)	snap.licdn.com	Microsoft	Ja (USA)	Analytics	Ja	Ja
New Relic Auf 2 Unterseiten gefunden (6.01.23 04:15)	newrelic.com	New Relic	Ja (USA)	Analytics	Nein	Ja
Oribi (LinkedIn) Auf Start- und 67 Unterseiten gefunden (6.01.23 04:15)	oribi.io	Microsoft	Ja (USA)	Analytics	Ja	Nein
Proven Expert Auf allen Seiten gefunden (6.01.23 04:15)	provenexpert.com	Expert Systems AG		Soziale Medien	Nein	Ja
Reddit Auf allen Seiten gefunden (6.01.23 04:15)	redditstatic.com	reddit	Ja (USA)	Soziale Medien	Nein	Nein
Signalize Auf 69 Unterseiten gefunden (6.01.23 04:15)	signalize.com	etracker GmbH		Werbung	Nein	Ja
TikTok Auf Start- und 67 Unterseiten gefunden (6.01.23 04:15)	tiktok.com	Beijing Bytedance Technology Ltd.	Ja (China)	Soziale Medien	Ja	Ja
Twitter Auf Unterseite gefunden (6.01.23 04:15)	twitter.com	Twitter	Ja (USA)	Soziale Medien	Nein	Ja
Twitter Syndication Auf Unterseite gefunden (6.01.23 04:15)	syndication.twitter.com	Twitter	Ja (USA)	Soziale Medien	Nein	Ja
VG Wort Auf Start- und 36 Unterseiten gefunden (6.01.23 04:15)	vgwort.de	VG Wort		Analytics	Nein	Ja
Vimeo Auf Start- und 7 Unterseiten gefunden (6.01.23 04:15)	vimeo.com	Vimeo	Ja (USA)	Audio/Video-Player	Nein	Ja
YouTube Auf Start- und 12 Unterseiten gefunden (6.01.23 04:15)	youtube-nocookie.com	Google	Ja (USA)	Audio/Video-Player	Ja	Ja

Unbekannte Domains

Es wurden Aufrufe zu folgenden Domains gefunden, denen keine Dienste unserer Datenbank zugeordnet werden konnten. Bitte prüfen Sie, ob dies datenschutzrechtliche Auswirkungen hat.

- **digistore24.com** (https://Ihre Domain.de/xyz-kurs)
- **thrivethemes.com** (https://Ihre Domain.de/xyz-checkliste)
- **credly.com** (https://Ihre Domain.de/zertifizierungen-und-auszeichnungen)

- **vine.co** (https://Ihre Domain.de/xyz-strategie)

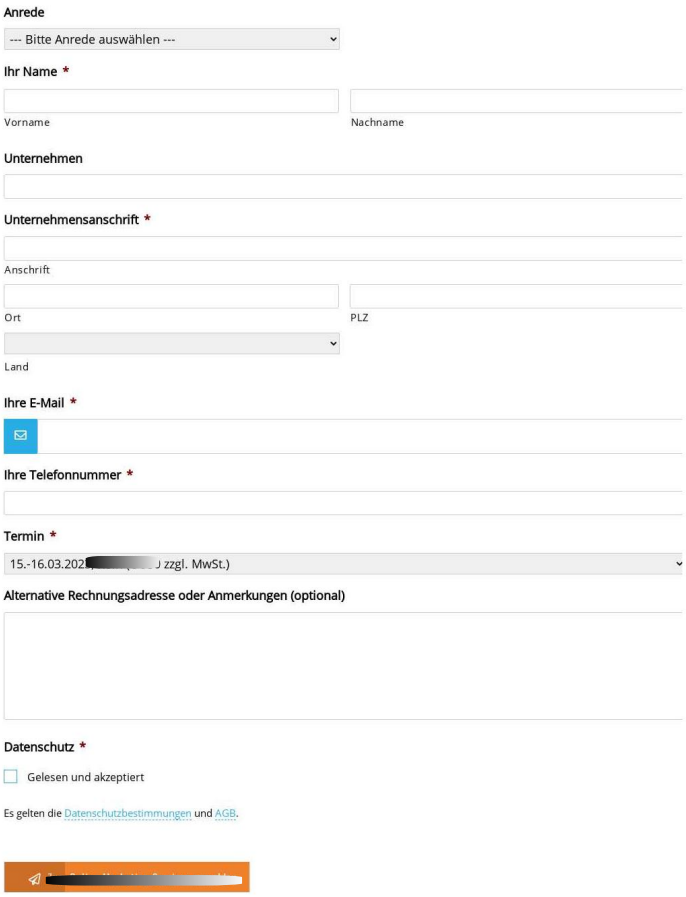
TLS/SSL-Verschlüsselung und Sicherheit des Webservers

✅ Das Zertifikat enthält korrekte und vollständige Informationen [1]
✅ Das Zertifikat ist zeitlich gültig bis 20.01.2023
✅ Das Zertifikat wird akzeptiert auf allen gängigen Plattformen (Apple, Android, Oracle/Java, Microsoft/Windows, Mozilla/Firefox) [2]
✅ Der Server ist geschützt gegen die verbreitetsten TLS/SSL-Angriffe [3]
✅ Der Webserver akzeptiert keine veralteten und unsicheren TLS/SSL-Protokolle. [4]
✅ Die aktuellen Protokolle TLS 1.2 bzw. TLS 1.3 werden akzeptiert [5]
⚠ Der Webserver setzt keine HTTP-Header für Content-Security-Policy [6]
✅ Für den Webserver ist HTTP Strict Transport Security ausreichend sicher konfiguriert [7]
⚠ Für den Webserver sind Umleitungen von HTTP zu HTTPS-Seiten eines anderen Servers konfiguriert, wodurch HSTS unterlaufen wird [8]
⚠ Der Webserver setzt keine Header für eine Referrer-Policy [9]
✅ Der Webserver setzt einen *X-Content-Type-Options*-Header [10]
⚠ Der Webserver setzt keinen *X-Frame-Options*-Header [11]

Zur Ermittlung der Sicherheit des Webservers verwenden wir Mozilla Observatory, für das komplette Scan-Ergebnis klicken Sie bitte hier.

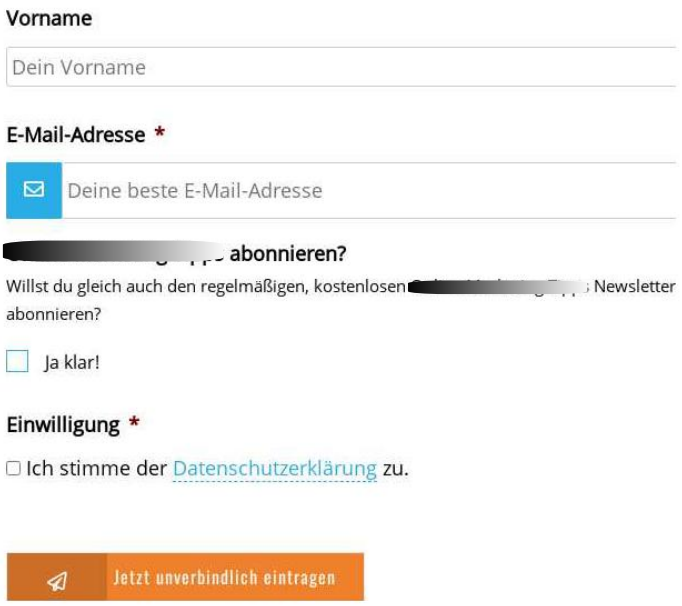
Formulare

Formular 1



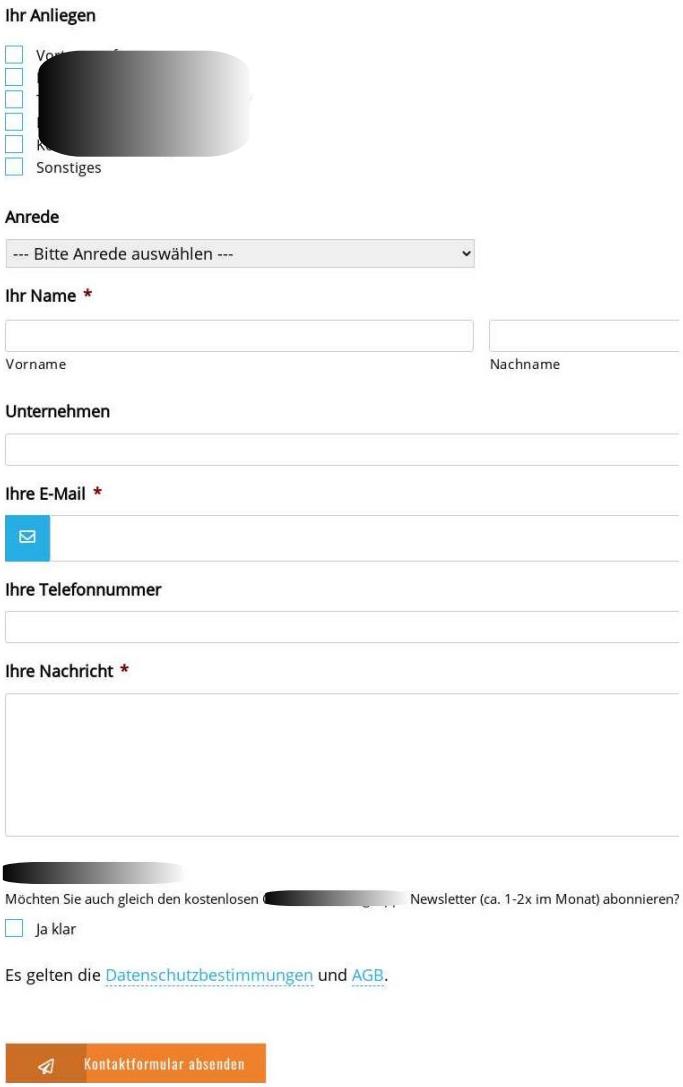
Fundstelle: XYZ Seminar 2022 in XYZ-Stadt & online und 2 weitere Seiten (Komplettliste).

Formular 2



Fundstelle: XYZ-Kurs: 5 ABC Tipps für

Formular 3



Fundstelle: Kontakt

Erläuterungen und Handlungsempfehlungen

[1] Wir untersuchen das TLS/SSL-Zertifikat darauf, ob der Server-Name im Zertifikat mit dem tatsächlichen Servernamen übereinstimmt, und ob das Zertifikat von einer vertrauenswürdigen Quelle stammt. Wenn eins von beiden nicht gegeben ist, zeigt ein Web-Browser normalerweise an, dass die Verbindung nicht sicher ist, weil in diesen Fällen sog. "Man-in-the-middle-Angriffe" möglich sind. Außerdem prüfen wir, ob die "Intermediate-Zertifikate" auf dem Server enthalten sind, die die Vertrauenswürdigkeit des Ausstellers nachweisen. Wenn diese fehlen, dann zeigen ältere Web-Browser möglicherweise Fehler an. Die Prüfungen zeigten keine Probleme.

[2] Die Zertifizierungsstelle, über die das Zertifikat des Webservers erworben wurden, muss von den großen Plattformen (Apple, Android, Oracle/Java, Microsoft/Windows, Mozilla/Firefox) als vertrauenswürdig eingestuft und in deren "Trust Store" aufgenommen worden sein. Wenn das nicht der Fall ist, dann stufen die Geräte dieser Plattformen das Zertifikat als nicht gültig ein. Im Fall dieses Webservers wird das Zertifikat von allen Plattformen als vertrauenswürdig eingestuft.

[3] Wir untersuchen den Server auf die Schwachstellen "Heartbleed", "CRIME" und "Downgrade". Alle drei stehen in Zusammenhang mit veralteter Systemsoftware oder dem Akzeptieren veralteter Verschlüsselungsprotokolle. Wir konnten bei dem Server diese Schwachstellen nicht feststellen.

[4] Veraltete TLS/SSL-Protokolle bieten keine sichere Verschlüsselung mehr, so dass Daten für Angreifer sichtbar sein können. Insbesondere die sehr alten Protokolle SSL 2.0 und SSL 3.0 sollten auf keinen Fall mehr eingesetzt werden, aber auch TLS 1.0 und TLS 1.1 sind nicht mehr sicher genug. Der Webserver ist korrekt konfiguriert und akzeptiert diese Protokolle nicht.

[5] Der Webserver sollte für ausreichende Sicherheit die neuen TLS/SSL-Protokolle TLS 1.3 und ggfs. TLS 1.2 unterstützen. Der Webserver ist korrekt konfiguriert und unterstützt diese.

[6] Die korrekte Konfiguration einer Content Security Policy (CSP) ist empfehlenswert, kann aber auch aufwändig einzurichten sein. Der Betreiber der Website sollte die Einführung einer CSP prüfen und mindestens sicherstellen, dass immer aktuelle Softwareversionen verwendet werden, bspw. bei Systemen wie Wordpress.
Hintergrund: Ein Content Security Policy (CSP)-HTTP-Header ist eine von mehreren möglichen Maßnahmen, um Websites gegen Angriffe durch Cross-Site-Scripting (XSS) zu schützen. Beim XSS injizieren Angreifer Javascript-Code in eine Seite (bspw. indem sie einen Blog-Kommentar schreiben, der Javascript-Code enthält). Wenn andere Besucher die Seite öffnen, wird das Javascript ausgeführt, was eine Vielzahl von Angriffsmöglichkeiten bietet, etwa das Auslesen und Versenden von Passwörtern während der Eingabe. Ein CSP-Header kann das verhindern, indem er das Ausführen von sog. "Inline-" Javascript grundsätzlich unterbindet, und nur Javascript von bestimmten Servern erlaubt, bzw. grundsätzlich das Laden von Ressourcen auf ausgewählte Server einschränkt. Bei der Einführung einer CSP muss möglicherweise der Anwendungscode angepasst werden, so ist u.A. der Einsatz des Google Tag Managers nicht mehr ohne Weiteres möglich. Die Herausforderungen bei der Einführung einer CSP beschreiben dieser und dieser Artikel.

[7] Der Parameter *max-age*, der angibt, wie lange per HSTS verschlüsselte Verbindungen erzwungen werde sollen, ist korrekt auf mehr als 6 Monate konfiguriert. Ein Wert von ein bis zwei Jahren ist optimal.
Hintergrund: HTTP Strict Transport Security (HSTS) ist ein Sicherheitsmechanismus, bei dem der Server einem Browser mitteilt, dass für eine bestimmte Zeit ausschließlich verschlüsselte Verbindungen verwendet werden dürfen. Bei so genannten Man-in-the-Middle Angriffen versucht ein Angreifer, den Aufbau einer verschlüsselten Verbindung zu verhindern, ohne dass der Benutzer etwas davon merkt. Der Angreifer kann dann unbemerkt alle übermittelten Daten mitlesen. Mit HSTS soll bereits am Beginn der Verbindung eine HTTPS Verschlüsselung erzwungen und damit die Gefahr solcher Angriffe minimiert werden. Ein Webserver sollte für optimalen Schutz immer HSTS in Verbindung mit einer HTTPS-Umleitung verwenden.

[8] Der Betreiber der Website sollte die Regeln für Umleitungen überprüfen.
Hintergrund: Der Server sollte so konfiguriert sein, dass unverschlüsselte Aufrufe sofort auf die entsprechende HTTPS-URL umgeleitet werden. Andernfalls könnte ein Benutzer bspw. verleitet werden, Formulardaten unverschlüsselt zu übertragen. Sobald die Umleitung stattgefunden hat, sollte der Browser per HSTS angewiesen werden, in Zukunft nur noch die verschlüsselte Verbindung zu benutzen. Dabei sollte die Umleitung nicht zu einer anderen Domain/Host führen (das würde HSTS aushebeln), sondern unmittelbar zur gleichen URL, aber mit HTTPS.

[9] Es ist zwar kein sehr großes Sicherheitsrisiko, keine Referrer-Policy festzulegen, aber auch nicht ideal. Die Browser verwenden dann eine eigene Policy, die möglicherweise etwas unsicherer ist als die empfohlene, das Verhalten ist aber auf jeden Fall unvorhersehbar.

Hintergrund: Der Referrer ist ein HTTP-Header, der bei einem Aufruf (auch an externe Ressourcen) die vorherige bzw. die aktuelle URL mitteilt. Da die URL sensitive Informationen enthalten kann, ist dies ein potentielles Sicherheitsrisiko. Eine Referrer-Policy legt deswegen fest, bei welchen Aufrufen dieser Header welchen Teil der URL enthält (oder leer ist). Als Best Practice gilt es, dass der Header die Policy *strict-origin-when-cross-origin* festlegt, dabei enthält dann der Referrer nur den eigenen Servernamen, wenn ein Aufruf an fremde Server stattfindet. Detaillierte Hinweise finden Sie hier.

[10] Es wurde ein *X-Content-Type-Options*-Header mit dem korrekten Wert *nosniff* gefunden.
Hintergrund: Der *X-Content-Type-Options*-Header mit dem Inhalt *nosniff* dient dazu, Cross-Site-Scripting-Attacken abzuwehren. Diese können auftreten, weil manche Browser (bspw. Internet Explorer) ein sog. "Content-Sniffing" durchführen. Dabei versucht der Browser selber herauszufinden, welchen Inhaltstyp eine Ressource hat, wenn der Content-Type-Header fehlt. Das ermöglicht es einem Angreifer, Javascript in eine Seite zu injizieren, etwa wenn er die Möglichkeit hat, selber Inhalte in ein Forum o.Ä. hochzuladen. Wenn andere Besucher die Seite öffnen, wird das Javascript ausgeführt, was eine Vielzahl von Angriffsmöglichkeiten bietet, etwa das Auslesen und Versenden von Passwörtern während der Eingabe. Es ist deshalb sinnvoll, diesen Header zu setzen.

[11] Der Betreiber der Website sollte einen *X-Frame-Options*-Header konfigurieren.
Hintergrund: Der *X-Frame-Options*-Header legt fest, ob die Website über ein iFrame auf einer anderen Website eingebettet werden kann. Letzteres kann ein Sicherheitsrisiko durch Clickjacking darstellen. Dabei werden Teile der eingebetteten Website durch Elemente des Angreifers überlagert, etwa um einem Besucher dazu zu bringen, auf scheinbar harmlose - aber tatsächlich gefährliche - Links zu klicken. Mit Hilfe des Headers kann derartiges Einbetten unterbunden werden. Alternativ ist der Content-Security-Policy-Header ebenfalls geeignet, ein Einbetten zu verhindern.