Unser Spezialgebiet? Die Sicherheit deiner Webseite!

Website: mitarbeitergewinnung.at/
Zeitpunkt des Scans: 24.04.2023 16:40

Risikobewertung

Zusammenfassung

Risiko-Score: D
8 Externe Dienste gefunden
9 Cookies gefunden
Datenschutzerklärung gefunden

Webserver-Standort und -Hosting

✅ Die Website läuft im Netzwerk von **netcup GmbH**. Der Serverstandort ist Deutschland.

Externe Dienste und Cookies

❗ Bei der Prüfung der Server-Sicherheit sind 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 setzt ohne Einwilligung des Users nicht notwendige Cookies und Dienste.

❗ Ihre Website setzt ohne Einwilligung des Benutzers mindestens **3 nicht notwendige Cookies**. Dies ist nicht rechtssicher, da gemäß §25 des TTDSG für das Setzen derartiger Cookies eine aktive Einwilligung erforderlich ist.

⚠ Ihre Website lädt ohne Einwilligung des Benutzers mindestens **3 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.

❗ Sie setzen **Google Fonts** ohne Einwilligung des Benutzers ein. Dies hat das Landgericht München mit Urteil vom 20.01.2022 als schadenersatzpflichtig bewertet. [1]

❗ Ihre Website lädt mindestens 4 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 **2 Externe Dienste** in Ihre Website ein, zu denen wir in der

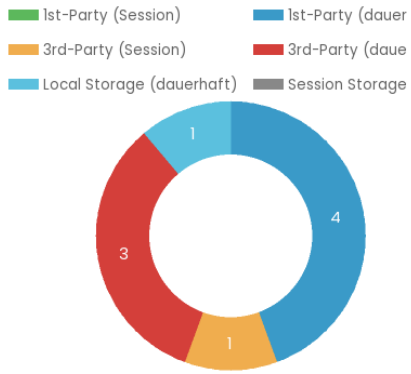
Datenschutzerklärung keinen Hinweis finden konnten. Damit verstoßen Sie gegen Ihre Informationspflicht nach Art. 13 der DSGVO.

Haftungsausschluss

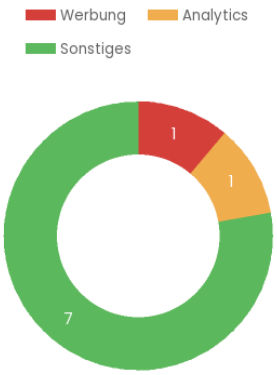
Bitte beachten Sie, dass trotz aller Sorgfalt bei der Untersuchung nicht ausgeschlossen werden kann, dass die Website Datenschutzschwachstellen aufweist, die in diesem Report nicht aufgezeigt werden. Wir können keine Haftung für die Vollständigkeit dieses Reports übernehmen.

Ansicht Startseite

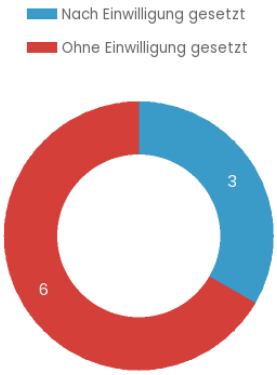
Cookies und Web-Speicher



Cookie-Typ



Verwendung



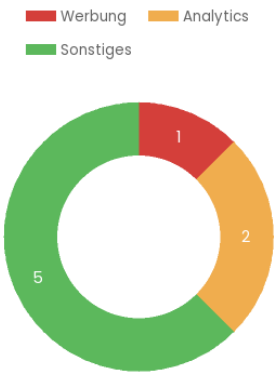
Einwilligung zum Setzen

Cookies und Web-Speicher Übersicht

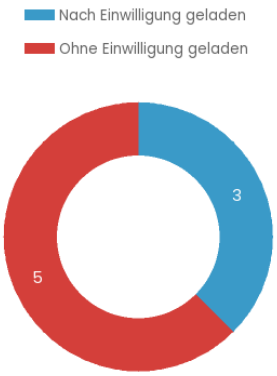
Name	Typ	Speicherdauer (Tage)	Domain	Quelle	Datentransfer	Zweck	Einwilligung erteilt
__cf_bm	3rd-Party (dauerhaft)	1	vimeo.com	Unbekannt		Unbekannt	Nein

Name	Typ	Speicherdauer (Tage)	Domain	Quelle	Datentransfer	Zweck	Einwilligung erteilt
_fbp Cookie ohne Einwilligung gesetzt, ist nicht notwendig, und leitet Daten aus dem Rechtsraum der EU aus	1st-Party (dauerhaft)	90	mitarbeitergewinnung.at	Facebook Pixel	Ja (USA)	Werbung	Nein
_ga	1st-Party (dauerhaft)	400	mitarbeitergewinnung.at	Google Analytics		Interaktion	Ja
_ga_1VM3T0H5L2	1st-Party (dauerhaft)	400	mitarbeitergewinnung.at	Google Analytics		Interaktion	Ja
borlabs-cookie	1st-Party (dauerhaft)	182	mitarbeitergewinnung.at	Borlabs Cookie		Consent Management	
elementor	Local Storage (dauerhaft)	unbegrenzt		Wordpress		Hosting	Nein
JSESSIONID	3rd-Party (Session)	0	nr-data.net	Unbekannt		Unbekannt	Nein
prism_651592375 Cookie ohne Einwilligung gesetzt, ist nicht notwendig, und leitet Daten aus dem Rechtsraum der EU aus	3rd-Party (dauerhaft)	30	app-us1.com	Active Campaign	Ja (USA)	Analytics	Nein
vuid Cookie ohne Einwilligung gesetzt, ist nicht notwendig, und leitet Daten aus dem Rechtsraum der EU aus	3rd-Party (dauerhaft)	400	vimeo.com	Vimeo	Ja (USA)	Audio/Video-Player	Nein

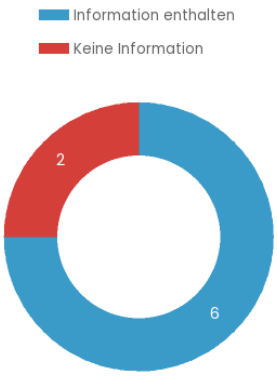
Externe Dienste



Cookie-Typ



Verwendung



Einwilligung zum Setzen

Externe Dienste Übersicht

Name	Domain	Quelle	Datentransfer	Zweck	Einwilligung erteilt	Information in Datenschutzerklärung

Name	Domain	Quelle	Datentransfer	Zweck	Einwilligung erteilt	Information in Datenschutzerklärung
Active Campaign Dienst ohne Einwilligung geladen, ist nicht notwendig, und leitet Daten aus dem Rechtsraum der EU aus Auf der Startseite gefunden	app-us1.com	Active Campaign	Ja (USA)	Analytics	Nein	Nein
Borlabs Cookie	mitarbeitergewinnung.at (*Lokaler Server*)	BORLABS		Consent Management		Ja
Facebook Pixel Dienst ohne Einwilligung geladen, ist nicht notwendig, und leitet Daten aus dem Rechtsraum der EU aus Auf der Startseite gefunden	connect.facebook.net/*/fbevents.js	Facebook	Ja (USA)	Werbung	Nein	Ja
Google Analytics Auf der Startseite gefunden	google-analytics.com	Google		Interaktion	Ja	Ja
Google Fonts [1] Auf der Startseite gefunden	fonts.googleapis.com	Google		Funktional	Nein	Ja
Google Tag Manager Auf der Startseite gefunden	googletagmanager.com	Google		Funktional	Ja	Ja
New Relic Dienst leitet Daten ohne Einwilligung aus dem Rechtsraum der EU aus. Auf der Startseite gefunden	newrelic.com	New Relic	Ja (USA)	Analytics	Nein	Nein
Vimeo Dienst ohne Einwilligung geladen, ist nicht notwendig, und leitet Daten aus dem Rechtsraum der EU aus Auf der Startseite gefunden	vimeo.com	Vimeo	Ja (USA)	Audio/Video-Player	Nein	Ja

TLS/SSL-Verschlüsselung und Sicherheit des Webservers

- ✅ Das Zertifikat enthält korrekte und vollständige Informationen [2]
- ✅ Das Zertifikat ist zeitlich gültig bis 22.06.2023
- ✅ Das Zertifikat wird akzeptiert auf allen gängigen Plattformen (Apple, Android, Oracle/Java, Microsoft/Windows, Mozilla/Firefox) [3]
- ✅ Der Server ist geschützt gegen die verbreitetsten TLS/SSL-Angriffe [4]
- ✅ Der Webserver akzeptiert keine veralteten und unsicheren TLS/SSL-Protokolle. [5]
- ✅ Die aktuellen Protokolle TLS 1.2 bzw. TLS 1.3 werden akzeptiert [6]
- ⚠ Der Webserver setzt keine HTTP-Header für Content-Security-Policy [7]
- ⚠ Für den Webserver ist HTTP Strict Transport Security nicht aktiviert [8]
- ✅ Für den Webserver sind Umleitungen von HTTP zu HTTPS korrekt konfiguriert [9]
- ⚠ Der Webserver setzt keine Header für eine Referrer-Policy [10]

⚠ Der Webserver setzt keinen *X-Content-Type-Options*-Header [11]
⚠ Der Webserver setzt keinen *X-Frame-Options*-Header [12]

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

Erläuterungen und Handlungsempfehlungen

[1] Der Betreiber der Website sollte die Google-Schriftdaten auf dem Webserver installieren, so dass keine Verbindung mehr zum Google-Server aufgebaut werden muss.
[2] 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.
[3] 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.
[4] 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.
[5] 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.
[6] 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.
[7] 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.
[8] Der Betreiber des Webservers sollte HSTS-Header für den Webserver aktivieren.
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.
[9] Alle Aufrufe zu unverschlüsselten URLs werden so umgeleitet, dass der Aufruf verschlüsselt erfolgt.
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.
[10] 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.
[11] Der Betreiber der Website sollte einen *X-Content-Type-Options*-Header konfigurieren.
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.

[12] 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.