Unser Spezialgebiet? Die Sicherheit deiner Webseite!

Website: www.mediapool.video/

Zeitpunkt des Scans: 24.04.2023 00:54

Risikobewertung

E	21	13	✓
Risiko-Score	Externe Dienste gefunden	Cookies gefunden	Datenschutzerklärung gefunden

Die Website läuft auf der Plattform **HubSpot CMS** (USA), ihr ist das Content Delivery Network von **CloudFlare** (USA) vorgeschaltet. Der Standort des CDN-Servers ist USA.
Es besteht das Risiko, dass Ihre Website nicht rechtssicher betrieben wird, da wegen der Standorte von Content Delivery Network, Plattform-Betreiber und CDN-Server personenbezogene Daten in einen unsicheren Drittstaat übertragen werden.

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 **Hubspot Consent Management** 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 **1 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 **1 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.

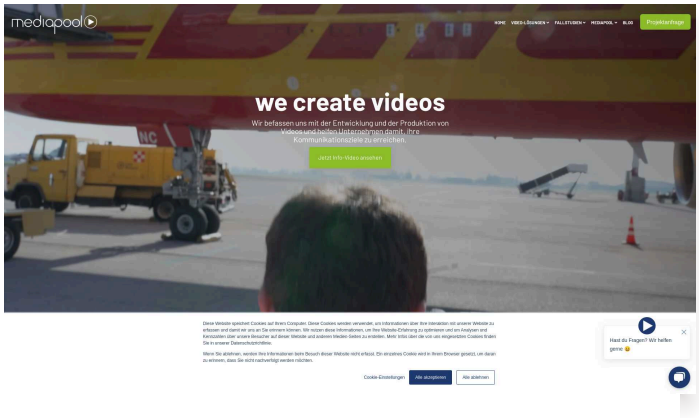
Sie setzen **Google Fonts** ohne Einwilligung des Benutzers ein. Dies hat das Landgericht München mit Urteil vom 20.01.2022 als schadenersatzpflichtig bewertet. [1]

Ihre Website lädt mindestens 8 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.

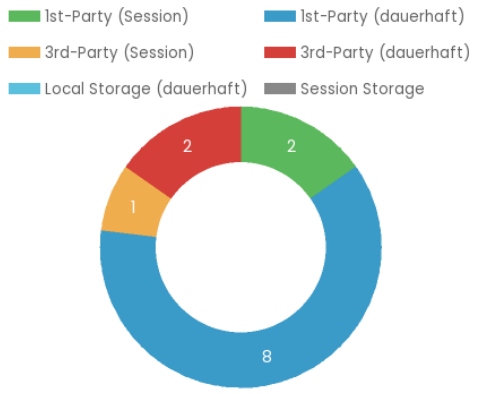
Sie binden **18 Externe Dienste** in Ihre Website ein, zu denen wir in der Datenschutzerklärung keinen Hinweis finden konnten. Damit verstoßen Sie gegen Ihre Informationspflicht nach Art. 13 der DSGVO.

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.

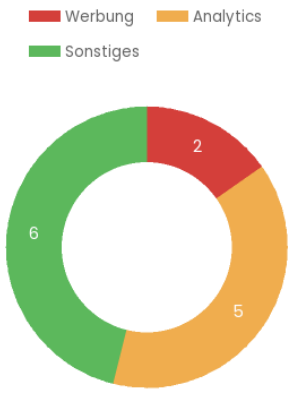
Ansicht Startseite



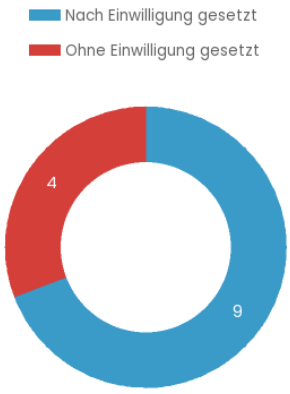
Cookies und Web-Speicher



Cookie-Typ



Verwendung



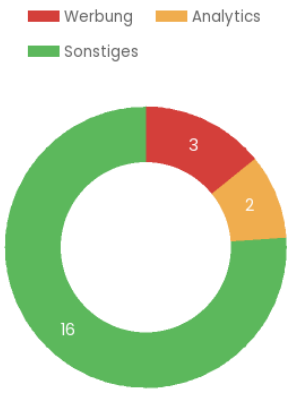
Einwilligung zum Setzen

Cookies und Web-Speicher Übersicht

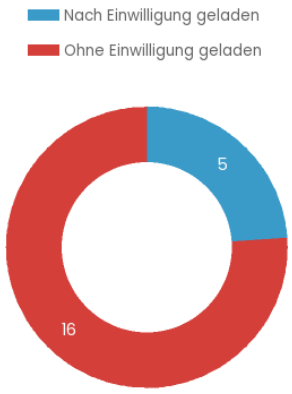
Name	Typ	Speicherdauer (Tage)	Domain	Quelle	Datentransfer	Zweck	Einwilligung erteilt
__cf_bm	1st-Party (dauerhaft)	1	mediapool.video	CloudFlare		Web-Speicher	Nein
__cfruid	1st-Party (Session)	0	mediapool.video	CloudFlare		Web-Speicher	Nein
__hs_cookie_cat_pref	1st-Party (dauerhaft)	180	mediapool.video	Unbekannt		Unbekannt	Ja
__hssc	1st-Party (dauerhaft)	1	mediapool.video	HubSpot	Ja (USA)	Analytics	Ja

Name	Typ	Speicherdauer (Tage)	Domain	Quelle	Datentransfer	Zweck	Einwilligung erteilt
__hssrc	1st-Party (Session)	0	mediapool.video	HubSpot	Ja (USA)	Analytics	Ja
__hstc	1st-Party (dauerhaft)	180	mediapool.video	HubSpot	Ja (USA)	Analytics	Ja
_fbp	1st-Party (dauerhaft)	90	mediapool.video	Facebook Pixel	Ja (USA)	Werbung	Ja
_gcl_au	1st-Party (dauerhaft)	90	mediapool.video	Unbekannt		Unbekannt	Ja
_GRECAPTCHA Auf Unterseite gefunden (11.04.23 13:47)	3rd-Party (dauerhaft)	180	google.com	Google Maps		Externer Inhalt	Nein
hubspotutk	1st-Party (dauerhaft)	180	mediapool.video	HubSpot	Ja (USA)	Analytics	Ja
IDE	3rd-Party (dauerhaft)	390	doubleclick.net	DoubleClick		Werbung	Ja
JSESSIONID Auf Unterseite gefunden (11.04.23 13:47)	3rd-Party (Session)	0	nr-data.net	Webserver		Funktional	Ja
messagesUtk	1st-Party (dauerhaft)	180	mediapool.video	HubSpot	Ja (USA)	Analytics	Nein

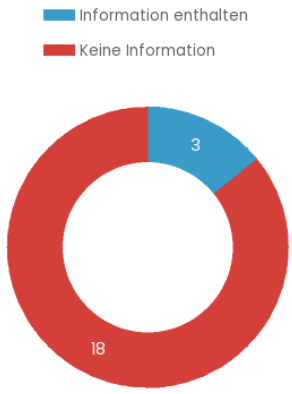
Externe Dienste



Verwendung



Einwilligung zum Laden



Information in Datenschutzerklärung

Externe Dienste Übersicht

Name	Domain	Quelle	Datentransfer	Zweck	Einwilligung erteilt	Information in Datenschutzerklärung
DoubleClick Auf allen Seiten gefunden (11.04.23 13:47)	doubleclick.net	Google		Werbung	Ja	Nein
Facebook Pixel Auf Start- und 494 Unterseiten gefunden (11.04.23 13:47)	connect.facebook.net/*/fbevents.js	Facebook	Ja (USA)	Werbung	Ja	Ja
Facebook Social Plugins Auf 10 Unterseiten gefunden (11.04.23 13:47)	www.facebook.com	Facebook		Soziale Medien	Nein	Nein
Google AdWords Conversion Auf Start- und 496 Unterseiten gefunden (11.04.23 13:47)	www.google.xxx/pagead	Google		Werbung	Ja	Ja
Google Fonts [1] Auf 10 Unterseiten gefunden (11.04.23 13:47)	fonts.gstatic.com	Google		Funktional	Nein	Nein

Name	Domain	Quelle	Datentransfer	Zweck	Einwilligung erteilt	Information in Datenschutzerklärung
Google Recaptcha Auf 22 Unterseiten gefunden (11.04.23 13:47)	www.google.com/recaptcha	Google		Interaktion	Nein	Nein
Google Tag Manager Auf allen Seiten gefunden (11.04.23 13:47)	googletagmanager.com	Google		Funktional	Ja	Nein
HubSpot Auf allen Seiten gefunden (11.04.23 13:47)	hubspot.com	HubSpot	Ja (USA)	Analytics	Nein	Ja
Hubspot Consent Management	mediapool.video (*Lokaler Server*)	HubSpot	Ja (USA)	Consent Management		Nein
HubSpot CMS Auf allen Seiten gefunden (11.04.23 13:47)	mediapool.video (*Lokaler Server*)	HubSpot	Ja (USA)	Hosting	Nein	Nein
HubSpot Forms Auf allen Seiten gefunden (11.04.23 13:47)	forms.hubspot.com	HubSpot	Ja (USA)	Interaktion	Nein	Nein
jQuery Auf allen Seiten gefunden (11.04.23 13:47)	jquery.com	JS Foundation	Ja (USA)	Web-Speicher	Nein	Nein
LinkedIn Widgets Auf 22 Unterseiten gefunden (11.04.23 13:47)	platform.linkedin.com	Microsoft	Ja (USA)	Soziale Medien	Nein	Nein
Mux Auf Start- und 45 Unterseiten gefunden (11.04.23 13:47)	litix.io	Mux		Audio/Video-Player	Nein	Nein
New Relic Auf Start- und 156 Unterseiten gefunden (11.04.23 13:47)	nr-data.net	New Relic	Ja (USA)	Analytics	Nein	Nein
Polyfill Auf allen Seiten gefunden (11.04.23 13:47)	polyfill.io	Polyfill.io		Funktional	Nein	Nein
Twitter Auf 22 Unterseiten gefunden (11.04.23 13:47)	twitter.com	Twitter	Ja (USA)	Soziale Medien	Nein	Nein
Twitter Syndication Auf 22 Unterseiten gefunden (11.04.23 13:47)	syndication.twitter.com	Twitter	Ja (USA)	Soziale Medien	Nein	Nein
Unknown Auf Start- und 51 Unterseiten gefunden (11.04.23 13:47)	hubspotvideo.com				Nein	Nein
Unknown Auf Start- und 51 Unterseiten gefunden (11.04.23 13:47)	mux.com				Nein	Nein
usemessages.com Auf allen Seiten gefunden (11.04.23 13:47)	usemessages.com			Unbekannt	Nein	Nein

TLS/SSL-Verschlüsselung und Sicherheit des Webservers

- Das Zertifikat enthält korrekte und vollständige Informationen [2]
- Das Zertifikat ist zeitlich gültig bis 27.06.2023
- 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 folgende veraltete und unsichere TLS/SSL-Protokolle: TLS 1.0, TLS 1.1 [5]
- Die aktuellen Protokolle TLS 1.2 bzw. TLS 1.3 werden akzeptiert [6]
- Der Webserver setzt zwar HTTP-Header für Content-Security-Policy, diese ist aber nicht ausreichend sicher konfiguriert [7]
- Für den Webserver ist HTTP Strict Transport Security ausreichend sicher konfiguriert [8]

✅ Für den Webserver sind Umleitungen von HTTP zu HTTPS korrekt konfiguriert [9]
⚠ Der Webserver setzt Header für eine mäßig sichere 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. Dies sollte vom Systemadministrator des Servers behoben werden.

[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 Content Security Policy (CSP) ist nicht ausreichend restriktiv. Sie enthält die Direktiven *unsafe-eval* oder *data* innerhalb der Direktive *script-src*, zu weit gefasste Einschränkungen wie *https:* innerhalb der Direktive *object-src*, oder sie schränkt die Quellen für *object-src* or *script-src* nicht ein.
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 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.

[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] Der HTTP-Header für Referrer-Policy ist *no-referrer-when-downgrade*, das entspricht nicht den Empfehlungen.
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.