fairwilly DSGVO Report

Website: www.fairwilly.de/
Zeitpunkt des Scans: 13.07.2021 02:12

Risikobewertung

A	2	0	
Risiko-Score	Externe Dienste gefunden	Cookies gefunden	Datenschutzerklärung gefunden

Die Prüfung der SSL-Verschlüsselung des Servers ergab keine Auffälligkeiten.

Wir konnten auf Ihrer Website keine uns bekannte Consent Management Software finden, mit der vom Benutzer eine Einwilligung zum Setzen von Cookies oder Externen Diensten eingeholt werden kann. Wir empfehlen den Einsatz, um Rechtssicherheit in Bezug auf Datenweitergabe zu erlangen.

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 **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.

Ansicht Startseite

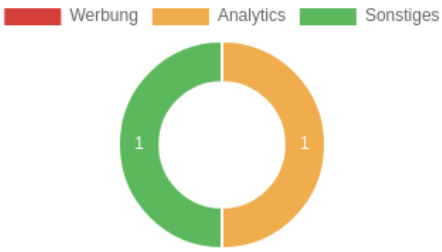
Cookies

Cookie-Typ | **Verwendung** | **Einwilligung zum Setzen**

Cookie-Übersicht

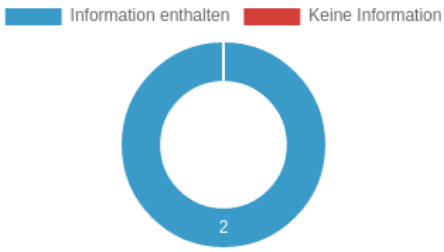
Name	Typ	Speicherdauer (Tage)	Domain	Quelle	Datentransfer außerhalb EU	Zweck	Einwilligung erteilt
No data available in table							

Externe Dienste



Verwendung

Einwilligung zum Laden



Information in Datenschutz-erklärung

Externe Dienste Übersicht

Name	Domain	Quelle	Datentransfer außerhalb EU	Zweck	Einwilligung erteilt	Information in Daten-schutzerklärung
etracker	etracker.com	etracker GmbH		Analytics	Nein	Ja
Proven Expert	provenexpert.com	Expert Systems AG		Soziale Medien	Nein	Ja

SSL-Verschlüsselung

Der Bereich Sicherheit und SSL-Verschlüsselung ist sehr komplex, bitte berücksichtigen Sie die Hinweise in unserer Dokumentation.

Gültigkeit des SSL-Zertifikats

- Der Servername im Zertifikat ist korrekt
- Die Zertifikatskette ist gültig

Ein falscher Servername im Zertifikat bzw. ein Fehler in Bezug auf die Zertifizierungsstelle deuten darauf hin, dass

- Das Zertifikat ist zeitlich gültig

Sie ein selbsterstelltes Zertifikat oder überhaupt keine Verschlüsselung verwenden. Ein abgelaufenes Zertifikat sollte umgehend aktualisiert werden.

Vertrauenswürdigkeit des SSL-Zertifikats

- Apple
- Android
- Windows
- Java

Wenn Ihr Zertifikat von einer Zertifizierungsstelle ausgestellt wurde, die von bestimmten Geräten bzw. Applikationen nicht erkannt wird, dann werden diese möglicherweise einen Fehler anzeigen.

Angriffsmöglichkeiten

- Der Server erzwingt Aufrufe mit https://
- Der Server ist geschützt gegen "Heartbleed"-Angriffe
- Der Server ist geschützt gegen "CRIME"-Angriffe
- Der Server ist geschützt gegen "Downgrade"-Angriffe

Fehlerhafte Konfiguration des Webservers oder veraltete Zertifikate erlauben es Angreifern, die Verschlüsselung zu umgehen oder brechen.

Verschlüsselungsprotokolle

- SSL 2.0 wird nicht akzeptiert
- SSL 3.0 wird nicht akzeptiert
- TLS 1.0 wird nicht akzeptiert
- TLS 1.1 wird nicht akzeptiert
- TLS 1.2 wird akzeptiert
- TLS 1.3 wird akzeptiert

Für optimale Sicherheit sollte Ihr Webserver so konfiguriert sein, dass er neue Verschlüsselungsprotokolle unterstützt, und die Verbindung über veraltete Protokolle verweigert.