Sicherheitsprüfung von Webseiten

Bisher hab ich die Sicherheitsüberprüfung nur mit ssllabs.com durchgeführt. Mit https://www.kuketz-blog.de/online-scanner-tools-fuer-sicherheit-und-datenschutz/ und der 2019 überarbeiteten Fassung https://www.kuketz-blog.de/empfehlungsecke/#online-bewertungstools habe ich ausführliche Artikel zur Überprüfung von Internetseiten entdeckt.

Anmerkung zur Version vom Sonntag, 1. Dezember 2024: Bei allen Werkzeugen wo dies möglich ist, wurde der Verknüpfung zur Internetseite hergestellt (Anklicken unterstrichenen Text in der ersten Spalte). Alle Links wurden auf Existenz und Aktualität geprüft. Leider sind Änderungen seit dem Sonntag, 1. Dezember 2024 möglich.

Anmerkung zur Version vom Donnerstag 25. Juli 2024: Observitory by Mozilla wurde durch *HTTP Observatory* ersetzt.

Eine regelmässige Prüfung wird empfohlen, da sich sowohl die geprüften Webseiten im Verlauf der Zeit ändern können, als auch die Prüfprogramme verbessert werden. *Diese Seite wird im Halbjahresrythmus fortgeschrieben.*

Bevorzugte Werkzeuge sind in ersten Feld grün markiert.

Mit der Fassung vom 01.12.2014 erfolgt auch ein Hinweis zur Überprüfung, ob Email-Adressen „gehackt" worden sind. Da das Ergebnis an die genannte Email-Adresse gesendet wird ist dies nur sinnvoll, wenn man Email an diese Adresse bekommt.

Am 21.009.2025 um pagespeed.web.de.dev ergänzt (siehe „Ladegeschwibdigkeiten der Webseiten").

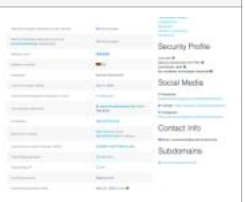
Wichtiger Hinweis: Einige der genannten Werkzeuge können inzwischen nicht mehr funktionieren und/ oder ihren Namen geändert haben. Die aufgeführten Links werden einmal im Jahr geprüft, letzte Prüfung 01.01.2025!

Mein Favorit bei diesen Webseiten-Test ist Webbkoll: Bei diesem Werkzeug werden auch Hinweise zur Fehlerbeseitigung aufgeführt. Wer mehrere Internetseiten auf einen Rutsch testen will sollte PrivacyScore verwenden, obwohl in der Betaphase noch einige Unstimmigkeiten auftreten und das Produkt z.Zt. nicht weiter verbessert wird. Aber beachten: Der Vorsatz http:// (bzw. https://) sollte verwendet werden und http Internetseiten sollten getrennt von https getestet werden.

Oftmals werden unnötigerweise externe Produkte verwendet, wie Google Fonts, Google Maps und Cloudflare. Solche Unzulänglichkeiten können mit entsprechenden Tipps leicht beseitigt werden, etwa für mit Wordpress erstellte Seiten für **Google Fonts** oder **Cloudflare**. Hinweise zur korrekten, DSGVO Einbindung von Google Fonts finden sich an mehreren Stellen im Internet, etwa unter https://kopfundstift.de/google-fonts-lokal-einbinden/ . Eine Alternative zum Einbinden von Karteninformationen statt **Google Maps** findet sich bei https://dr-dsgvo.de/google-maps/?z=330337370&msh=13048&ct=3389&ei=wasgeht.

Die Seite des **Authors** Mike Kuketz ist für Sicherheitsfragen ein Muss. Wichtige Links dazu sind: https://www.kuketz-blog.de und https://www.kuketz-blog.de/category/microblog/. Daneben sei auf die Seite von **Regina Stoiber** für eine DSGVO-konforme WEBSEITE hingewiesen, der letzte Hinweis führt zu einem Dienst, der aber zahlungspflichtig ist. Aus den oben genannten Seiten ergibt sich folgende Tabelle (URL Verknüpfung bei Anklicken in der ersten Spalte:

Eine weitere interessante Seite ist Dr. DSGVO: Dort wird auch unter dem Titel „*Cookie Consent Lösungen sind Bullshit*" auf den Nonsense und die Rechtsverstösse von bei den Einwilligungsabfragen von Cookies hingewiesen. Der Test von Cookieabfragen ist weiter unten beschrieben (in der Tabelle unter „*Chrome Browser*"). Dr. Klaus Meffert beschäftigt sich auf seiner Homepage https://dr-dsgvo.de/ mit der Prüfung auf Konformität zur DSGVO. Unter https://dr-dsgvo.de/webseiten-check/ findet sich die Möglichkeit seine Webseite auf Konformität zu überprüfen. Ebenso werden die vom Aufrufenden übermittelten Daten angegeben. Der Aufruf seiner Webseite lohnt sich auf jeden Fall um um interessantes zur aktuellen Datenschutzsituation zu erfahren. Unter https://dr-dsgvo.de/newsletter/ bietet er einen Newsletter an.

Webseite	**Kurzbeschreibung** (In der Spalte „Webseite" kann durch Antippen des unterstrichenen Textes direkt zur entsprechenden Webseite verlinkt werden)	**Beispiel**
Sicherheit		
Umfassende Prüfung auf DSGVO	Dieser Website DSGVO Check basiert nicht nur auf technischen Prüfungen, sondern berücksichtigt auch die Rechtslage. Nicht jeder, der einen Scanner programmieren kann, weiß etwas über Datenschutz. Der Check kann gefahrlos verwendet werden. Geprüfte Webseiten werden nicht nachverfolgt. Abgesehen von der moralischen Problematik: Was hätte ich auch davon? Es reicht, das Internet aufzumachen, um beliebig viele Webseiten zu finden, die Datenschutzprobleme aufweisen. Es besteht auch die Möglichkeit mehrere Webseiten in einer Liste zu überprüfen. Der Author freut sich über Spenden zur Unterstützung seiner Arbeit.	
Übersichtdarstellung	Detaillierte Informationen über die Website: Zusammensetzung der Technologie, Kontaktinformationen der wichtigsten Personen, Sprache, Land und vieles mehr. Suchen Sie nach Websites, die ähnliche oder konkurrierende Technologien verwenden.	

Sicherheitsprüfung von Webseiten

Webseite	**Kurzbeschreibung** (In der Spalte „Webseite“ kann durch Antippen des unterstrichenen Textes direkt zur entsprechenden Webseite verlinkt werden)	Beispiel
HTTP Observatory	Observatory von Mozilla funktioniert nun nicht mehr, es wurde durch HTTP Observatory ersetzt. Das 2016 gestartete HTTP Observatory verbessert die Web-Sicherheit durch die Analyse der Einhaltung bewährter Sicherheitsverfahren. Es hat durch 47 Millionen Scans Einblicke in über 6,9 Millionen Websites gewährt. Das von Mozilla entwickelte HTTP Observatory führt eine eingehende Bewertung der HTTP-Header und anderer wichtiger Sicherheitskonfigurationen einer Website durch. Der automatisierte Scan-Prozess liefert Entwicklern und Website-Administratoren detailliertes, umsetzbares Feedback, das sich auf die Identifizierung und Behebung potenzieller Sicherheitsschwachstellen konzentriert. Das Tool hilft Entwicklern und Website-Administratoren dabei, ihre Websites gegen gängige Sicherheitsbedrohungen in einer sich ständig weiterentwickelnden digitalen Umgebung zu stärken. Das HTTP Observatory bietet effektive Sicherheitseinblicke, die von Mozillas Fachwissen und Engagement für ein sichereres Internet geleitet werden und auf bewährten Trends und Richtlinien basieren.	
Qualys SSL Labs:	SSL Lab prüft die TLS-Konfiguration und das ausgelieferte Zertifikat eines Webservers auf Herz und Nieren. Der Scanner überprüft unter anderem die unterstützten Cipher-Suiten (PFS, AEAD), führt eine Handshake-Simulation durch und prüft auf (aktuelle) Bedrohungen wie Ticketbleed, Heartbleed oder BEAST.	
Hardenize: https://www.hardenize.com	Hardenize prüft nicht nur Webserver auf sicherheitsrelevante Einstellungen, sondern auch die Konfiguration von E-Mail-Servern und die DNS-Records (DNS, DNSSEC, CAA). Bei E-Mail-Servern prüft Hardenize unter anderem auf Sicherheitsfunktionen wie DANE, SPF, DMARC und MTA-STS. Ähnlich wie Observatory umfasst der Prüfkatalog ebenfalls sicherheitsrelevante Einstellungen des Webservers (TLS, Cookies, HSTS, CSP etc.).	
Security Headers:	Security Headers beschränkt sich auf die Prüfung von Security-Headern, wie Strict-Transport-Security (HSTS), X-Frame-Options, X-Content-Type-Options, Content Security Policy (CSP), Referrer-Policy und Permission-Police. Die Begriffe werden gut erklärt und es werden Hinweise zur Verbesserung gegeben..	
CryptCheck:	CryptCheck prüft die TLS-Einstellungen und die angebotenen Cipher-Suiten von Web-, E-Mail- und XMPP-Servern.	
My Email Communications Security Assessment (MECSA):	MECSA bewertet die Sicherheit der E-Mail-Kommunikation bzw. des eigenen Anbieters. Es werden Sicherheitsmechanismen wie SPF, DKIM, DMARC, DANE etc. geprüft. : Email Adresse und CAPCHTA eingeben! Eine Bestätigungsmail ist zu beantworten	
Datenschutz		
PrivacyMail:	PrivacyMail kann *unsichtbare Tracking-Methoden in Newslettern* sichtbar machen und die von Unternehmen genutzten Drittanbieter offenlegen. **Leider nicht für alle Browser verwendbar, nicht zu empfehlen.**	
Webbkoll: Bevorzugtes Werkzeug	Webbkoll simuliert, was im »Hintergrund« passiert, wenn ihr eine Webseite in eurem Browser aufruft. Die Stärke von Webbkoll liegt in der transparenten Darstellung, welche Ressourcen wie JavaScript, Cookies und/oder Schriftarten von Drittquellen (Google, Facebook etc.) in den Kontext einer Webseite eingebunden werden. Darüber hinaus prüft Webbkoll den Webserver unter anderem auf Security-Header wie HSTS, Content Security Policy (CSP) und Referrer-Policy. Der dort angebotene weitere Test „Observatory by Mozilla! Kann zwar noch aufgerufen, wurde aber durch HTTP Observatory ersetzt.	
PrivacyScore:	PrivacyScore prüft nicht nur sicherheitsrelevante Parameter, sondern auch, wie datenschutzfreundlich eine Webseite ist. PrivacyScore erkennt Analyse- und Werbedienste, eingebettete Ressourcen von Drittseiten und die Verwendung von Content Distribution Networks (CDN), die ebenfalls eine Gefahr für die Sicherheit und Privatheit darstellen können. Hinweis: **Erlaubt Überprüfung von mehrere Webseiten, die einer Textdatei stehen.** Noch im Beta-Stadium und wird zur Zeit nicht aktualisiert.	
App-Verkehr mit »Sniffer-Apps« mitschneiden		

Sicherheitsprüfung von Webseiten

Webseite	Kurzbeschreibung (In der Spalte „Webseite“ kann durch Antippen des unterstrichenen Textes direkt zur entsprechenden Webseite verlinkt werden)	Beispiel
Android	Mit der App HttpCanary lässt sich der App-Verkehr leicht mitschneiden. Es existiert eine werbebasierte Version und eine Pro-Version (4,49 €), die ohne Werbung auskommt und zusätzliche Funktionen bietet. Auf GitHub ist ebenfalls ein Tutorial verfügbar, das den Einsteig erleichtert. HttpCanary erzeugt ein lokales VPN, durch das der gesamte Netzwerkverkehr geschleust wird – es sind keine Remote-Server beteiligt. Zum Aufbrechen von TLS-verschlüsselten Verbindungen ist zusätzlich die Installation eines Root-CAs erforderlich. Anschließend lässt sich der App-Verkehr von einer oder mehreren Apps gezielt mitschneiden und analysieren. Sowohl die Anfrage- als auch Antwort-Pakete werden dargestellt. Für den Hobby-Analysten oder »Datenjäger« eine tolle App, um »schwarze« Schafe aufzudecken.	
iOS	Eine ähnliche Funktionalität bietet die App Charles Proxy (9,99 €) für iOS. Auch diese App ermöglicht den Mitschnitt des Datenverkehrs bzw. die Analyse von Metadaten, Request-Headern und -Bodys. Auch Charles Proxy erzeugt zunächst ein lokales VPN, durch das im Anschluss der gesamte Netzwerkverkehr geschleust wird – es sind keine Remote-Server beteiligt.	
Verschiedenes		
Browserleaks	Bei BrowserLeaks dreht sich alles um den Schutz der Privatsphäre beim Surfen und die Erstellung von Fingerabdrücken im Webbrowser. Hier finden Sie eine Galerie von Tools zur Prüfung der Sicherheit von Webtechnologien, die Ihnen zeigen, welche Art von persönlichen Identitätsdaten durchgesickert werden können und wie Sie sich davor schützen können. Standardmässig werden Informationen über den Provider angezeigt, die Tools müssen einzeln manuel angewählt werden.	
Abmahncheck	Lassen Sie jetzt Ihre Website sofort und kostenfrei rechtlich prüfen. Ihre Website wird hinsichtlich der derzeit häufigsten Abmahngründe gecheckt. Sie erhalten umgehend ein Prüfergebnis, das Ihnen das Gefährdungspotential Ihrer Website aufzeigt. Geben Sie hierfür einfach Ihre Internetadresse in die untenstehende Eingabemaske ein und klicken Sie auf „Go!“. Ihre Daten können von uns nicht eingesehen werden, eine Speicherung findet nicht statt – Sie bleiben also zu 100 % anonym.	
IP Location Finder und mehr	Diverse Tools wie Speed Test, IP Location Finder, Certificate Checker etc.	
Cloudflare Check	Cloudflare, Inc. ist ein US-amerikanisches Unternehmen, das ein Content Delivery Network, Internetsicherheitsdienste und verteilte DNS-Dienste (Domain Name System) bereitstellt, die sich zwischen dem Besucher und dem Hosting-Anbieter des Cloudflare-Benutzers befinden und als Reverse Proxy für Websites fungieren. In einem Bericht der Europäischen Kommission[47] wird dem Unternehmen vorgeworfen, nicht genug gegen Urheberrechtsverletzungen auf dessen Plattform zu unternehmen. Demnach schätzt der Bericht, dass Cloudflare von ca. 40 % aller Websites genutzt wird, die illegal urheberrechtlich geschütztes Material anbieten. Von den 500 urheberrechtsverletzenden Domains mit den meisten Besuchern, nach Alexa Rank, sind es 62 %. Die Reaktion seitens Cloudflare, auf Anfragen bezüglich der Urheberrechtsverletzungen, wird weiter als unzureichend eingestuft. Das Landgericht Köln urteilte (6 U 32/20) in einer einstweiligen Verfügung von Universal Music gegen Musikpiraterie in Deutschland, dass Cloudflare als Störer im Sinne der Störerhaftung angesehen wird, was erstmals einen Präzedenzfall für die Branche schuf.[48] Cloudflare kam der Aufforderung nicht nach und wurde im Berufungsverfahren vor dem Oberlandesgericht Köln aufgrund von Unterlassung verurteilte.	
Website Speed Test https://tools.pingdom.com	Pingdom offers cost-effective and reliable uptime and performance monitoring for your website. We use more than 70 global polling locations to test and verify our customers' websites 24/7, all year long. With Pingdom you can monitor your websites' uptime, performance, and interactions for a better end-user-experience.	
Webseite Audit GtMetrix	Test auf Ladegeschwindigkeit und struktureller Verbesserungsmöglichkeiten der Webseite.	
Cookie Rocks	Testet intensiv auf Cookies	
Chrome Browser	Der Test für Cookies mit dem Browser Chrome ist etwas umständlich zu erreichen. In der Befehlszeile  am rechten Rand das Feld ⋮ anklicken. In dem ausgeklappten Anzeige „weitere Tools“ und anschliessend „Entwicklertools“ und dann Cookies auswählen. Falls dort weiteren Text angezeigt wird diesen Anklicken auswählen	

Webseite	**Kurzbeschreibung** (In der Spalte „Webseite“ kann durch Antippen des unterstrichenen Textes direkt zur entsprechenden Webseite verlinkt werden)	**Beispiel**
Whats my IP	Allgemein verwendbares Tool zur Ermittlung der IP-Adresse und des Providers sowie weiterer interessanter Informationen, etwa Internetgeschwindigkeit und Infos ob ihre Email Adresse „geknackt“ wurde.	
Fehlende Links		
Integrity	Stand alone APP für den MAC. Von https://peacockmedia.software/mac/integrity/free.html herunter laden, installieren und aufrufen. Findet auch Links, die durch Zugriffsrechte geschützt und Links, deren Verknüpfung wegen time out nicht zustandekommen	
Linkchecker - finden defekte Links auf Ihrer Website. Eine Übersicht über solche Link Checker (entweder eigenständige Programme unter Windows oder Internetseiten) finden sich unter https://www.schulhomepage.de/webdesign/linkchecker**. Im folgenden Finden sich einige Linkchecker, die über den Browser aufgerufen werden:**		
Broken Link Check	Findet im Vergleich zu Integrity nur alle fehlenden Links. Die Prüfung kann bei vielen Internetseiten längere Zeit dauern.	
dead link checker	Prüft entweder eine einzelne Webseite oder die Gesamte Seite mit allen Unterseiten. In der kostenlose Version auf 2.000 Links beschränkt. Bietet diverse kostenpflichtige Versionen zur regelmässigen Prüfung von Webseiten	
Nextcloud Security Scan	Dieser Scan analysiert die Sicherheit Ihres privaten Nextcloud Servers und gibt einen Überblick darüber, was zu verbessern ist. **Nur für Nextcloud Server!**	
Ladegeschwindigkeit der Webseite		
Geschwindigkeitsprüfung Von Webseiten (PageSpeed Insight)	PageSpeed Insights (PSI) von Google gibt Aufschluss über die Nutzererfahrung einer Seite auf Mobilgeräten und Computern. Geräte und macht Vorschläge, wie die Seite verbessert werden kann. PSI stellt sowohl Lab- als auch Felddaten zu einer Seite bereit. Labordaten sind nützlich, um Probleme zu beheben, da sie in einer kontrollierten Umgebung erfasst werden. Tatsächliche Engpässe werden jedoch nicht immer erkannt. Felddaten sind bei der Erfassung der tatsächlichen Nutzererfahrung hilfreich. Die Anzahl der Messwerte ist bei diesen Daten jedoch eingeschränkt. Siehe Denkweise Über Speed Tools finden Sie weitere Informationen zu den beiden Datentypen.	
Zeit zum Aufbau der Webseite	PageSpeed Insights (PSI) enthält Berichte zur Nutzerfreundlichkeit von Seiten auf Mobilgeräten und Computern sowie Verbesserungsvorschläge. Aber Vorsicht: Nutz google Analytics und andere Tracker. Detaillierte Beschreibung siehe https://de.wikipedia.org/wiki/PageSpeed_Insights	

Zusätzlich bieten die Browser Addons zur Überprüfung von Webseiten beim Aufruf der Webseite ab. Zu diesen Programmen zählen Disconect, Ghoestery (für Tracker).

Ausspionieren von Email-Adressen

Empfehlenswert ist es Email-Adressen zu überprüfen, ob sie schon einmal gezielt angegriffen und dann „gehackt“ wurden. Überprüfungsmöglichkeiten finden sich auf den folgenden Internetseiten: https://leakchecker.uni-bonn.de/de/index und https://sec.hpi.de/ilc/?lang=de. Überprüfbar sind dabei nur Email Adressen auf die man Zugriff hat - keine „Fremdadressen“, da das Ergebnis an die eingegeben Email Adresse gesendet wird.

Ausspionieren durch Ki-Programme

Um das Ausspähen durch Chatcpt zu vermeiden sollte eine Datei Robot.TXT auf der Webseite einfügt werden. Siehe: https://www.eff.org/deeplinks/2023/12/no-robotstxt-how-ask-chatgpt-and-google-bard-not-use-your-website-training