

EDRI EUROPEAN DIGITAL RIGHTS

FAIRE WEBSITES

HANDBUCH FÜR ERFOLGREICHE
MACHERINNEN UND MACHER

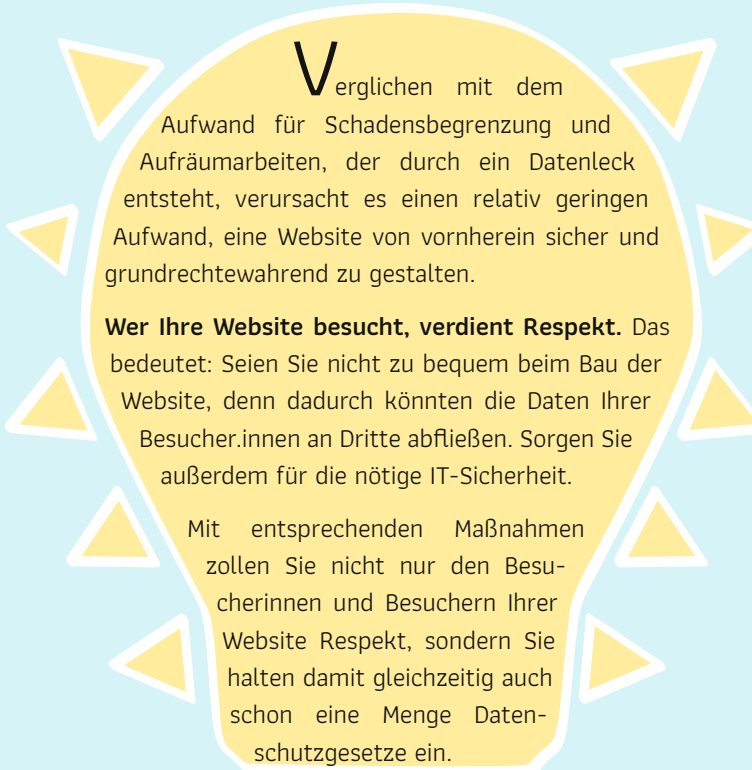


▶ digitalcourage

KURZ&MÜNDIG

ART D'AMEUBLEMENT

BAND 1



Verglichen mit dem Aufwand für Schadensbegrenzung und Aufräumarbeiten, der durch ein Datenleck entsteht, verursacht es einen relativ geringen Aufwand, eine Website von vornherein sicher und grundrechtewahrend zu gestalten.

Wer Ihre Website besucht, verdient Respekt. Das bedeutet: Seien Sie nicht zu bequem beim Bau der Website, denn dadurch könnten die Daten Ihrer Besucher:innen an Dritte abfließen. Sorgen Sie außerdem für die nötige IT-Sicherheit.

Mit entsprechenden Maßnahmen zollen Sie nicht nur den Besucherinnen und Besuchern Ihrer Website Respekt, sondern Sie halten damit gleichzeitig auch schon eine Menge Datenschutzgesetze ein.

IMPRESSUM:

Deutsche Fassung veröffentlicht mit der Unterstützung von

Digitalcourage e.V. / Art d'Ameublement 2020

Übersetzung: Meike Schüttkus

Überarbeitung: Christian Pietsch, Digitalcourage e.V.

Endredaktion: Claudia Fischer, verstandenwerden.de

Layout: Isabel Wienold, iwi-design.de

Bildrechte: Foto S. 37: dpa [Deutsche Presseagentur]

Screenshots: S. 28: openstreetmap.org | S. 29: fontsquidrel.com

S. 30: panzi.github.io/SocialSharePrivacy/index.de.html

S. 31: phpcaptcha.org/try-securimage/

Allle weiteren Bilder: iwi-design.de, Isabel Wienold CC BY-NC-SA 4.0



INHALT

1. EINFÜHRUNG 5

2. GRUNDLAGEN 8



Erwartungen der Nutzenden 8

Vertrauenswürdigkeit und Sicherheit 9

Personenbezogene Daten und Einhaltung der DSGVO 10

3. ALLGEMEINE EMPFEHLUNGEN 14

4. SICHERHEITSEMPFEHLUNGEN 17

ISO 18

Domain Name System Security Extensions [DNSSEC] 18

Tor-Browser 19

HTTPS 20

Content Security Polity [CSP] 21

Java Script 22

Schutz sensibler Daten 22

Schutz vor DDoS-Angriffen 24

Die Rückkehr statischer Websites 25



5. ALTERNATIVEN ZU KOSTSPIELIGEN

„KOSTENLOSEN“ DRITTANBIETER-SERVICES 26

Webanalytics	26
Videos	27
Maps	28
Schriften und Icons	29
Widgets der sozialen Medien	30
CAPTCHAs	31
... und weitere	32
Tools zur Organisation von Veranstaltungen	32
Websites für alle zugänglich machen	33
Damit das Web vernetzt bleibt	34
Ethische Werbung	35
Website-Suche	35

ÜBER DIGITALCOURAGE

37

ÜBER EDRI

38



1.

EINFÜHRUNG



bsites¹ sind wie Lebewesen: Meistens sind sie sehr dynamisch, ändern sich laufend, und auch ihr Umfeld ist einem ständigem Wandel unterworfen, was wiederum zu mehr Änderungen führt. Zudem wird eine Website von sehr unterschiedlichen Menschen besucht, die verschiedene Technologien nutzen und auch verschiedene fachliche Kompetenzen haben.

Viele Websites verlassen sich auf diverse **externe Dienste und Datenquellen**, z.B. Datenbanken oder Landkarten. Auch diese entwickeln sich weiter.

Wer Websites entwickelt, muss ständig wachsende Erwartungen der Nutzerschaft erfüllen. Gleichzeitig soll das alles nicht viel kosten. Dadurch entsteht die wachsende Tendenz, mehr externe Dienste und Ressourcen zu nutzen.

Immer häufiger werden daher in den Websites auch „kostenlose“ Angebote wie Schriften und Skripte genutzt. Diese sind zwar „kostenlos“ für den Entwickler, doch sie können **unerwünschte Nebenwirkungen** für die Nutzenden und die

1 Das Wort „Website“ ist übrigens kein Schreibfehler. „Site“ heißt Landschaft, und so bezeichnet „Website“ eine Sammlung von mehreren Webseiten/Internetseiten, die zu einem gemeinsamen Internetauftritt gehören. Die „Website“ heißt also zum Beispiel „digitalcourage.de“ und vereint viele „Webseiten“, also Unterseiten zu verschiedenen Themen [z.B. „digitalcourage.de/impressum“].

Betreibenden der Website haben. Einige Tools und Services – besonders die bestimmter datenhungriger Internetkonzerne – können den Datenschutz untergraben, andere wiederum haben möglicherweise negative Auswirkungen auf die IT-Sicherheit. Beides kann Ihren guten Ruf gefährden oder zu rechtlichen Problemen führen.

MÖGLICHE FOLGEN, WENN SIE „KOSTENLOSE“ RESSOURCEN VON DRITTANBIETERN IN IHRE WEBSITE EINBINDEN:

- 1** Sie haben **weniger Kontrolle** über Ihre eigene Website, denn wenn der Drittanbieter seine Regeln ändert, hängen Sie mit drin.
- 2** Sie werden **abhängig** von bestimmten Anbietern (Fachbegriff „vendor lock-in“).
- 3** Besuchende können von Dritten getrackt, also **erfasst und durchs Internet verfolgt** werden.
- 4** Wenn Sie mit Diensten [Tools] der großen Anbieter GAFAM [Google, Apple, Facebook, Amazon, Microsoft] arbeiten, arbeiten Sie für diese und **festigen deren Marktmacht**.

Klingt nicht gut, oder? Leider mangelt es dafür häufig an Problembewusstsein, deshalb binden viele externe Dienste ein. Ziel dieser Broschüre ist es, die damit verbundenen Probleme zu verdeutlichen und – wo möglich – brauchbare Lösungen anzubieten.

Dieser Leitfaden richtet sich an alle, die Websites entwickeln oder betreuen. Um den Leitfaden kurz und praktisch zu halten, verweisen wir, wenn notwendig, über Links auf weiterführende Informationen.

Wir hoffen, Webschaffenden damit zu helfen, das Internet wieder zu dem zu machen, was es mal sein sollte: ein dezentrales Netzwerk, das **Grundrechte, Demokratie und Meinungsfreiheit** stärken kann.

**DAS INTERNET GEHÖRT AUCH
UNS. WIR MÜSSEN DAFÜR
VERANTWORTUNG ÜBERNEHMEN.**



2.

GRUNDLAGEN



ERWARTUNGEN DER NUTZENDEN

Die Besucherinnen und Besucher Ihrer Website haben eine Reihe von berechtigten Erwartungen. Sie wollen **Sicherheit**, und sie möchten, dass weder ihren Endgeräten (Computer, Smartphone usw.) noch ihren Daten Schaden zugefügt wird. Sie wollen, dass ihre **Privatsphäre** respektiert wird. Einiges davon ist in Rechtsvorschriften wie der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union festgeschrieben worden.

Es reicht nicht aus, dass ein Dienst technisch einfach und zuverlässig funktioniert. Ein Service, der auch nur ansatzweise **fehlerhaft, schwerfällig oder unzuverlässig** ist, entspricht nicht den Wünschen der Nutzenden und sie werden ihn dann vielleicht meiden.

Viel wichtiger ist aber folgende Überlegung: Wenn sie diesen Dienst nicht meiden, sondern weiter nutzen, werden sie sich damit abfinden, Dinge zu tolerieren, die sie eigentlich nicht tolerieren sollten. Dinge, die eigentlich Warnzeichen für signifikante Probleme sind.

VERTRAUENSWÜRDIGKEIT UND SICHERHEIT

Im aktuellen gesellschaftlichen und politischen Klima beschäftigt viele Menschen auch die Frage nach Richtigkeit und Wahrhaftigkeit. Wie bereitwillig sollten Sie einer Software vertrauen, die Sie von einer Website herunterladen? Wie bereitwillig sollten Sie den Links auf einer Website vertrauen?

Und **über allem steht die IT-Sicherheit**: Im Englischen bezeichnet man als safety, dass ein System keinen Schaden verursacht, und als security, dass ein System vor Beschädigung geschützt ist. Die Sicherheit eines Systems ruht dabei auf drei Säulen: Verfügbarkeit, Integrität und Vertraulichkeit. Systeme, Dienste und Daten müssen auch bei einem Ausfall einzelner Komponenten oder bei einem Angriff verfügbar bleiben. Wer Websites verantwortet oder programmiert, muss Maßnahmen treffen, um den jeweiligen Dienst jederzeit aufrechtzuerhalten und die Unversehrtheit der Daten zu gewährleisten. Ist eine beschädigte Datenbank tatsächlich noch nützlich? Und natürlich sollten nur die Personen Daten sehen können, die dazu auch berechtigt sind.



PERSONENBEZOGENE DATEN UND EINHALTUNG DER DSGVO

Unternehmen in der Europäischen Union und Unternehmen, die Dienstleistungen für Menschen in der EU anbieten, müssen die Datenschutz-Grundverordnung (DSGVO) befolgen. Sie zielt in erster Linie darauf ab, Menschen die **Kontrolle über ihre eigenen Daten** zu geben. Sie vereinfacht das rechtliche Umfeld und regelt zudem die Weitergabe von Daten in Länder und Rechtssysteme außerhalb der EU.

Die DSGVO ist jedoch eine komplexe Rechtsvorschrift, und daher gibt es viele Unternehmen, die Beratung, Training, Checklisten und Hinweise zur Auslegung anbieten. Zudem hat jedes EU-Mitgliedsland seine eigene Datenschutzbehörde, die für die Auslegung und Durchsetzung der DSGVO zuständig ist.

Als **personenbezogene Daten** bezeichnet man Informationen, die durch bestimmte Identifikatoren eindeutig einem bestimmten Menschen zugeordnet werden können. Identifikatoren sind dabei Angaben wie Name, Kennnummer, Standortdaten oder Online-Kennung. Es kann sich aber auch um eines oder mehrere Merkmale handeln, die spezifisch für die physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität dieser natürlichen Person sind.



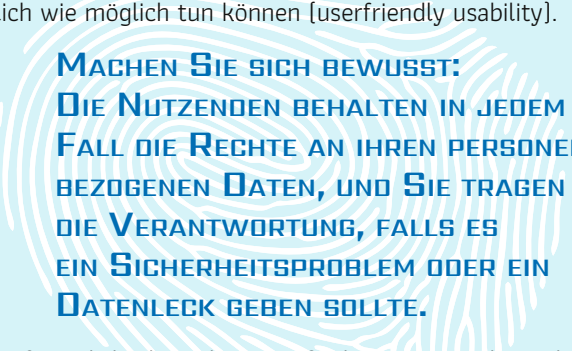
Wenn Sie sich mit einem Gerät im Internet anmelden, dann bekommt Ihr Gerät eine sogenannte „**IP-Adresse**“, eine lange Nummer zugewiesen, mit der es im Netz unterwegs ist. Gemäß DSGVO handelt es sich bei IP-Adressen um personenbezogene Daten, denn eine IP-Adresse kann eindeutig einer bestimmten Person zugeordnet werden. Dazu muss man nur die IP-Adresse mit weiteren Informationen [z.B. mit dem **Zeitpunkt der Anmeldung** beim Betreiber des Inter-

netzugs und dem **WLAN**, in dem Ihr Gerät sich aufhält] kombinieren. Wenn Drittanbieter, also andere Firmen, in eine Website eingebunden werden, um Funktionalitäten wie JavaScript oder Inhalte wie Bilder oder Landkarten bereitzustellen, dann bekommen diese Drittanbieter auch Zugriff auf Ihre IP-Adresse. Die DSGVO schreibt deshalb vor, dass die Betreiber einer Website mit jedem dieser Drittanbieter ggf. eine Datenverarbeitungsvereinbarung abschließen müssen. **Wenn Sie also auf Drittanbieter verzichten, ersparen Sie sich eine Menge Arbeit.**



Die DSGVO verlangt das Konzept „**Privacy by Default**“ [datenschutzfreundliche Voreinstellung]. Das bedeutet, dass die Privatsphäre schon bei der Konzeption und bei der Programmierung so gut wie möglich mitgedacht und gewahrt werden sollte. Konkret: Wenn Sie einen Dienst anbieten,

sollte jede Einstellung von vornherein so ausgewählt sein, dass die Privatsphäre der Nutzenden höchstmöglich respektiert wird. Auf Wunsch können Nutzende diese Einstellung ändern – und das sollten sie so bequem, klar und verständlich wie möglich tun können [userfriendly usability].



**MACHEN SIE SICH BEWUSST:
DIE NUTZENDEN BEHALTEN IN JEDEM
FALL DIE RECHTE AN IHREN PERSONEN-
BEZOGENEN DATEN, UND SIE TRAGEN
DIE VERANTWORTUNG, FALLS ES
EIN SICHERHEITSPROBLEM ODER EIN
DATENLECK GEBEN SOLLTE.**

Aufgrund der komplexen Anforderungen ist die Einhaltung der DSGVO ein Fachgebiet für Spezialisten. Wenn Sie allerdings die Grundsätze dieses Leitfadens beachten, halten Sie schon viele rechtliche Regeln ein und stellen dabei zudem sicher, dass Sie nach ethischen Prinzipien handeln. Außerdem gibt es eine Fülle von kostenlosen Diensten, die ebenfalls zur Einhaltung der DSGVO beitragen – das ist gut für Sie und für die Besucher Ihrer Website.

Weitere Informationen finden Sie in den Richtlinien für Web-Services beim Europäischen Datenschutzbeauftragten:

[https://edps.europa.eu/data-protection/our-work/
publications/guidelines/web-services_de](https://edps.europa.eu/data-protection/our-work/publications/guidelines/web-services_de)

3. ALLGEMEINE EMPFEHLUNGEN

Konzipieren Sie Ihre Website so, dass Sie nicht darauf angewiesen sind, die Daten Ihrer Besuchenden zu sammeln! Finden Sie ein Geschäftsmodell, das die Grundrechte Ihrer Kundinnen und Kunden wahrt! Nutzen Sie datenschutzfreundliche Einstellungen zu Ihrem Vorteil:

**WERBEN SIE DAMIT, DASS SIE IHRE
BESUCHENDEN NICHT TRACKEN,
KEINE GOOGLE-DIENSTE EINBINDEN,
KEINE DATEN IN LÄNDER
AUSSERHALB DER EU SENDEN USW.**

IM EINZELNEN KANN DAS BEDEUTEN:



Ermöglichen Sie, dass möglichst viele Daten schon auf dem Endgerät des Nutzenden verarbeitet werden, nicht im Netz.



Wenn Sie Nutzerdaten abfragen und verarbeiten, achten Sie auf Verschlüsselung. Ermöglichen Sie Ende-zu-Ende-Verschlüsselung für jede relevante Kommunikation, auch auf dem Transport der Datenpakete durchs Netz. Das Ziel sollte sein, dass vertrauliche Informationen grundsätzlich weder für Sie als Website-Betreiber noch für Dritte sichtbar sind.



Setzen Sie wo immer möglich Verfahren der Datenminimierung ein – fragen Sie nur Daten ab, die auch tatsächlich notwendig sind.



Nutzen Sie wann immer möglich First-Party-Ressourcen [d.h. Ressourcen, die Sie selbst verantworten] und vermeiden Sie Drittanbieter-Lösungen. Mit anderen Worten: Versuchen Sie, alles auf Ihrem eigenen Server anzubieten/zu hosten. Dies schließt Programmcode und Inhalte von Drittanbietern ein, wie zum Beispiel:

Cookies, CSS-Dateien, Bilder,
Video- und Audio-Dateien, JavaScript,
Frames mit Inhalten von Drittanbietern,
Schriftdateien



Wenn ein Anbieter Angebote wie JavaScripts oder Schriftdateien nicht ausdrücklich zum Download für das Selbsthosting freigibt, dann sind diese möglicherweise nicht datenschutzfreundlich und sollten daher vermieden werden. Wenn Sie dennoch auf Drittanbieter-Lösungen nicht verzichten wollen oder können, dann ist es evtl. sinnvoll, Subresource Integrity [SRI] zu nutzen.



Behalten Sie das Datentransfervolumen im Auge – unnötig datenintensive Websites, z.B. mit unnötig großen Bildern oder bewegten Animationen, schließen nicht nur Besuchende mit schlechter Internetanbindung aus, sondern verbrauchen auch unnötig viel Strom.



Seien Sie transparent – informieren Sie in einfacher Sprache.



Achten Sie auf Barrierefreiheit.



Nutzen Sie Webanwendungen, die Ihre Website automatisch auf einige Privatsphäre-Gefährdungen prüfen können und minimieren Sie danach die gefundenen Warnungen:

WebbKoll:

<https://webbkoll.dataskydd.net>

PrivacyScore:

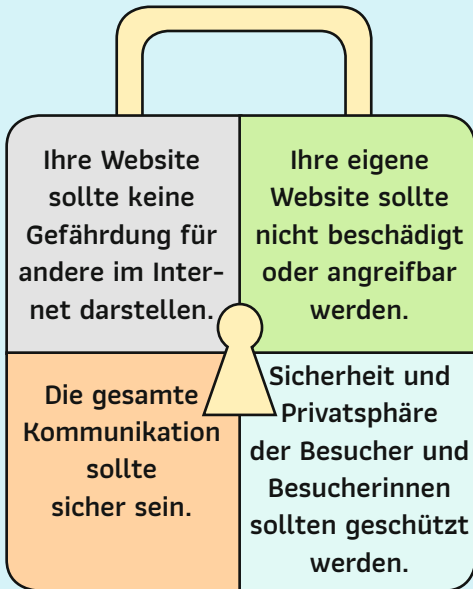
<https://privacyscore.org/>

4.

SICHERHEITSEMPFEHLUNGEN

IT-Sicherheit ist ein umfangreicher Prozess. Behalten Sie den Überblick. Sicherheitsentscheidungen müssen unterschiedliche, möglicherweise auch widersprüchliche Ziele berücksichtigen und können daher nicht unabhängig voneinander getroffen werden. Sie beeinflussen Eigenschaften wie Geschwindigkeit oder Benutzungsfreundlichkeit eines Dienstes, und sie können sich erheblich auf die benötigten Mittel – Budget und Arbeitszeit – auswirken.

GENERELL SOLLTEN SIE FOLGENDES GEWÄHRLEISTEN:



Diese Sicherheitsziele können in der Regel auf zwei Wegen erreicht werden: **Informationsaustausch und Standards**. Da sich Bedrohungen und Reaktionen immer wieder ändern, ist es wichtig, Informationen – z.B. über fachgebundene Mailinglisten – miteinander zu teilen. Zumindest sollten Sie Ihr zuständiges Computersicherheits-Ereignis- und Reaktionsteam [CERT] einbeziehen. Wenn Sie sich zudem an die entsprechenden **aktuellen technischen Standards** halten, stellen Sie sicher, dass Sie nicht das schwächste Glied in der Kette sind.

ISO

Die ISO, Internationale Organisation für Normung, hat eine ganze Reihe von Normen über Qualität und Sicherheit veröffentlicht:

ISO / IEC / IEEE 90003:2018 Software Engineering

ISO / IEC 27000

Family of Information Security Standards

In diesen Standards findet sich u.a. eine Terminologie, die den gemeinsamen Sprachgebrauch vereinheitlichen und damit vereinfachen kann. Damit wird auch der Nachweis der Umsetzung der DSGVO vereinfacht.

DNSSEC

DNSSEC [Domain Name System Security Extensions] sorgt unter anderem dafür, dass sich kein anderer Internet-Server als der Ihre ausgeben kann. Wenn Sie einen DNS-Server betreiben, dann konfigurieren Sie bitte DNSSEC!



TOR-BROWSER

Um den Schutz ihrer Daten und ihrer Privatsphäre zu gewährleisten, nutzen manche Menschen den Tor-Browser, mit dem sie anonym im Internet unterwegs sein können. Bei der Auswahl Ihres Hosting-Anbieters sollten Sie darauf achten, dass dieser Tor-Verbindungen erlaubt. Mit OnionShare kann man zudem mit nur wenigen Klicks eine anonyme und nicht zensierbare Version einer bereits bestehenden Website erstellen. <https://onionshare.org/>



Um Man-in-the-Middle- [MITM]² und Lauschangriffe zu vermeiden, lassen Sie keine unverschlüsselten Verbindungen zu Ihrer Website zu, und bieten Sie immer Verbindungen über HTTPS an. Der Hauptgrund für den Einsatz von HTTPS ist die Authentifizierung der aufgerufenen Website sowie der Schutz und die Unversehrtheit der ausgetauschten Daten. Prüfen Sie, ob Sie HSTS [HTTP Strict Transport Security] einsetzen können, um HTTPS zu erzwingen.

Von Let's Encrypt können Sie kostenlos Zertifikate für HTTPS bekommen [auch TLS- oder SSL-Zertifikat genannt]. Falls Sie Ihren Web-Server nicht selbst betreiben, sondern einen Dienstleister nutzen, dann achten Sie darauf, dass dieser Let's Encrypt unterstützt – sonst können TLS-Zertifikate teuer sein. <https://letsencrypt.org/>

Wenn Sie HTTPS nutzen, denken Sie daran, dass Sie nur sichere Verschlüsselungsverfahren zulassen. Einige ältere Versionen von HTTPS verwenden veraltete Verschlüsselungsverfahren und bieten daher keine optimale Sicherheit mehr.

.....
2 Als „Man in the Middle“-Angriff bezeichnet man zum Beispiel Internetseiten, mit denen versucht wird, Sie dazu zu bringen, Ihr Passwort einzugeben, obwohl Sie sich noch gar nicht auf der eigentlich gewünschten Login-Seite befinden [phishing].

Im Netz finden Sie frei zugängliche Tools zur Überprüfung der Sicherheit Ihres Webservers wie z.B.

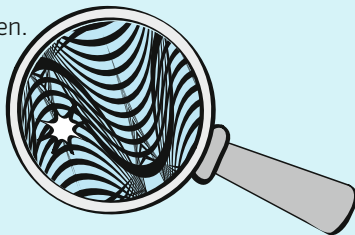
<https://www.ssllabs.com/ssltest/>

CSP

Implementieren Sie Content Security Policy. CSP ist eine Sicherheitsschicht des World Wide Web Consortium [W3C], die Sie auf Ihrem Server aktivieren können, um zu verhindern, dass externe Skripte, Stylesheets, Bilder usw. auf Ihrer Website geladen werden. CSP trägt zur Erkennung und Abmilderung von bestimmten Arten von Angriffen bei, z.B. Cross-Site-Scripting- [XSS-] und Injection-Angriffe. Diese Angriffe können für den unberechtigten Zugriff auf Daten oder die Veränderung von Daten auf Ihrer Website [Defacement oder Verbreitung von Schadsoftware] genutzt werden. Mit CSP können Sie Richtlinien für Ihre Website individuell festlegen, indem Sie bestimmte URLs in eine weiße Liste aufnehmen.

Sollten Sie keinen Zugriff auf die Webserverkonfiguration haben, können Sie eine CSP dennoch mit Hilfe einer .htaccess-Datei oder direkt im Header Ihrer Website aktivieren. Die Konfiguration Ihrer CSP lässt sich mit einem kostenlosen Tool von Mozilla überprüfen.

<https://observatory.mozilla.org/>



JAVASCRIPT

Manche vertreten die Auffassung, JavaScript sollte ganz vermieden werden, da es einen bestimmten Anwenderkreis ausschließen könnte und nicht barrierefrei sei. Zwar führt JavaScript selbst nicht dazu, dass bestimmte Inhalte nicht zugänglich sind – es ist jedoch Vorsicht geboten.

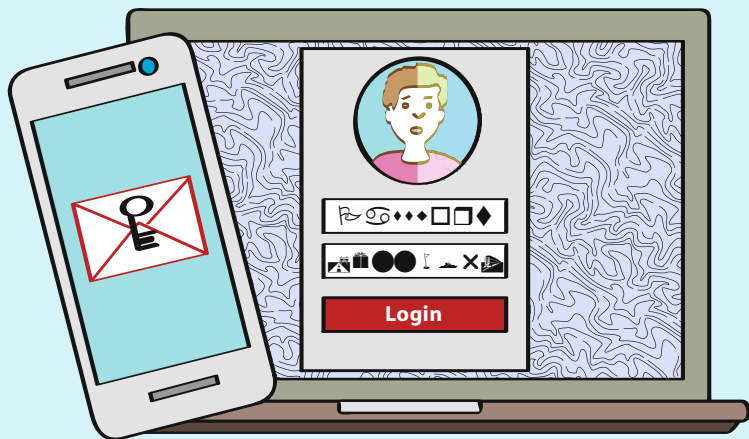
<https://webaim.org/techniques/javascript/>

Wenn Sie JavaScript verwenden, wird oftmals eine zusätzliche Version ohne JavaScript notwendig. Deshalb schlagen wir Ihnen vor, eine Website ohne JavaScript zu entwickeln und diese Funktionalitäten erst nachträglich einzubauen. Dadurch wird die Website für alle einfacher zugänglich. Fügen Sie ein `<noscript>`-Tag ein, um Inhalte bereitzustellen für den Fall, dass manche Menschen JavaScript nicht einsetzen möchten oder können.

SCHUTZ SENSIBLER DATEN

Falls die Website personenbezogene Daten der Nutzerinnen und Nutzer speichert, zum Beispiel bei der Einrichtung persönlicher Konten mit Login,

- ▶ setzen Sie die Verwendung **starker Passwörter** durch und erklären Sie direkt auf der Seite, welche Bedingungen sie erfüllen sollen.
- ▶ Speichern Sie Passwörter und andere sensible Informationen niemals im Klartext. Nutzen Sie für gespeicherte Daten immer **gesalzene Hashfunktionen** und Verschlüsselungsverfahren.



- ▶ Ermöglichen Sie Zwei-Faktor-Authentifizierung [2FA].
- ▶ Wenn Sie nur geringe Kapazitäten für die Betreuung der Webseite haben, können Sie die o. g. Aufgaben an einen Identity-Provider auslagern und mit Single Sign On [SSO] arbeiten. Beachten Sie dabei aber, dass die Zusammenarbeit mit einem Identity-Provider möglicherweise wiederum zu Lasten der Privatsphäre geht.

Wenn persönliche Nutzungskonten nicht notwendig sind, könnte die Kommentierung von Blogspots ein hilfreiches Feature sein. Integrieren Sie hierzu Open-Source-Plugins von Drittanbietern wie z.B. Discourse oder das Coral Project.

<https://www.discourse.org/> und <https://coralproject.net/>

Weitere Einzelheiten finden Sie unter

<https://darekkay.com/blog/static-sitecomments/>.

SCHUTZ VOR DDoS-ANGRIFFEN

Distributed Denial of Service Attacks (DDoS) sind Angriffe, die typischerweise den Zielservers durch eine Vielzahl von Anfragen von verschiedenen Quellen überfluten, um damit das System zu überlasten. Insbesondere wenn Sie eine Website für eine **Nichtregierungsorganisation** (NGO), einen **Verein**, eine aktivistische **Initiative** oder eine zivilgesellschaftliche Gruppe entwickeln, sollten Sie sich Gedanken über den Schutz vor einem DDoS-Angriff machen. Einige DDoS-Abwehrtechniken nutzen einen Drittanbieter, der sich zwischen die Besuchenden einer Website und den Website-Hoster schaltet – wie ein Reverse-Proxy für Websites. Andere DDoS-Abwehrtechniken brauchen keine Hilfe eines Drittanbieters, sondern arbeiten auf der Netzwerkebene.

Eine Open Source-Lösung hierfür ist Deflect, die von einer Non-Profit-Organisation für digitale Sicherheit entwickelt wurde.

<https://docs.deflect.ca/>

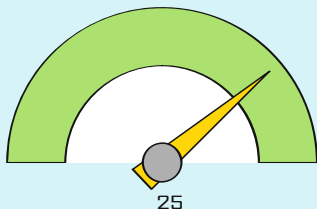
Wenn Sie den Schutz vor DDoS-Angriffen an einen Drittanbieter auslagern, heißt das auch immer, dass Sie die Kontrolle über Ihren Datenverkehr an Externe abgeben. Dies erfolgt unabhängig davon, ob der Anbieter nur im Falle eines Angriffs punktuell und sehr schnell eingreift, oder ob der Service rund um die Uhr in-line ist. Die sich daraus ergebenden Risiken sollten sorgfältig abgewogen werden.

DIE RÜCKKEHR STATISCHER WEBSITES

Brauchen Sie wirklich eine dynamische Website? Wenn Sie keine Datenbank einbinden müssen, stehen die Chancen gut, dass Sie mit aktuellen Webstandards wie HTML5 eine hochmoderne Website ausschließlich mit statischen Ressourcen (HTML, CSS und möglicherweise JavaScript sowie Schriftdateien) realisieren können.

Dies bedeutet aber nicht, dass Sie Navigationsleisten usw. von Hand programmieren müssen. Mit modernen statischen Websitegeneratoren wie Jekyll [bekannt geworden durch GitHub Pages], Hugo oder Pelican können Sie Ihre Websites in Markdown oder einfachem HTML erstellen und diese dann in vollständiges, verlinktes HTML umwandeln. Mit GitLab Pages kann die Konvertierung und Bereitstellung ganz einfach automatisiert werden.

Statische Websites erreichen unschlagbare Stabilität, weil sie keine Verbindung zu einer Datenbank benötigen. Ein einfacher Webserver, auf dem die statischen Dateien liegen, genügt. Dadurch sind sie weniger betroffen von Sicherheitslücken und zudem blitzschnell.



5. ALTERNATIVEN ZU KOSTSPIELIGEN „KOSTENLOSEN“ SERVICES VON DRITTANBIETERN

Die Verwendung von Tools [Diensten oder Bausteinen] von Google, Facebook, Amazon und anderen Datenriesen ist für viele **unvereinbar mit dem Schutz der Privatsphäre** ihrer Online-Services. Webentwickler, die sich dem Datenschutz ihrer Nutzenden verpflichtet fühlen, versuchen die Tools der Datengiganten oder ihrer Tochterunternehmen weder direkt noch indirekt zu nutzen. Es gibt eine Fülle von ethischen, benutzerfreundlichen und datenschutzbewussten Alternativen, von denen viele auf Prism Break aufgeführt sind.

<https://prism-break.org/>

Auch wir wissen, dass externe Dienstleistungen manchmal sehr nützlich sind. Wir möchten Ihnen daher einige Methoden zur Datenminimierung und Alternativen für die gängigen Dienste ans Herz legen:

WEBANALYTICS



Sicher ist es spannend und kann nützlich sein, zu wissen, wie Ihre Webseiten von Ihren Besucherinnen und Besuchern genutzt werden. Es ist uns aber wichtig darauf hinzuweisen, dass Webanalysen in der Regel fehlerbehaftet sind und von vielen Werbe- und Tracking-Blockern behindert werden. Wenn man Webana-

lyse betreibt, bedeutet dies also nicht notwendigerweise, dass man korrekte Informationen erhält.

Wenn Sie dennoch Auswertungen wünschen, dann können Sie statt mit Google Analytics [oder jedem anderen Drittanbieter-Tool] z.B. mit **Matomo [ehemals Piwik]** arbeiten. Matomo ist eine datenschutzkonforme Analyseplattform, die sich sehr einfach installieren und so konfigurieren lässt, dass sie Daten automatisch anonymisiert. Damit wird nur eine minimale Menge an personenbezogenen Daten verarbeitet. Und Sie bleiben innerhalb des vorgeschriebenen Rahmens der DSGVO.

<https://matomo.org/>

VIDEOS

YouTube gehört zu Google. Wenn Sie ein YouTube-Video einbetten, achten Sie bitte darauf, den Modus mit verbesserter Privatsphäre zu aktivieren. In diesem Modus platziert YouTube erst dann Co-



okies auf den Endgeräten Ihrer Seitenbesucher, wenn diese sich das Video tatsächlich ansehen. Die Option „Nach Ende des Videos vorgeschlagene Videos anzeigen“ sollte zudem deaktiviert werden. Wenn Sie lieber mit einem Plugin für Ihr Content Management System [Abkürzung CMS, damit fügen Sie Ihre Inhalte in Ihre Website ein] arbeiten, achten Sie darauf, dass dieses ebenfalls eine solche Option bietet.

Klicken Sie unter dem gewünschten Video auf „Teilen“ → „Einbetten“ → „Erweiterten Datenschutzmodus“ aktivieren, und dann bekommen Sie einen HTML-Code-Schnipsel angezeigt, den sie einsetzen können.

Eine noch bessere Idee wäre es, eine PeerTube-Instanz zu nutzen oder selbst eine zu betreiben. PeerTube ist ein dezentrales Netzwerk, bei dem alle teilnehmenden Instanzen gleichberechtigt sind. Dabei bleiben die Videos auf dem Server der Person oder Instanz, die das Video online stellt. Sie sind nicht mehr abhängig davon, ob ein zentraler Anbieter wie YouTube ihr Video womöglich löscht oder sperrt, weil irgendwer sich darüber beschwert. Und es wird auch keine Werbung eingeblendet. Allerdings können Sie so bei Peertube über Klickzahlen natürlich auch kein Geld verdienen.

Eine andere Alternative ist Vimeo. Vimeo bietet im Rahmen seiner kostenpflichtigen Pro-Mitgliedschaft die Möglichkeit, Videodateien ohne den Vimeo-Player (der Google Analytics beinhaltet) zu verwenden. Falls Sie PeerTube nicht nutzen können, wäre dies also eine Notlösung.

MAPS

Mit der Nutzung der Google-Maps-API zur Einbindung einer Karte in Ihre Website zwingen Sie Ihre Nutzerinnen und Nutzer, Googles Datenschutzrichtlinie zu akzep-



tieren. Bei **OpenStreetMap** ist das nicht der Fall – klare Empfehlung von uns. <https://www.openstreetmap.org/>

SCHRIFTEN UND ICONS

Statt Schriften von Google zu verwenden, mit denen die Besucher Ihrer Website ebenfalls Googles Datenschutzrichtlinien akzeptieren müssen, stehen auch andere Schriftarten zur Verfügung:



- ▶ Fork Awesome: eine sehr große Sammlung von Open Source-Icons <https://forkawesome.github.io/Fork-Awesome/>
- ▶ Fontello: hier können Sie Ihre eigene Auswahl an Icons erstellen <http://fontello.com/> <https://github.com/fontello/fontello/>
- ▶ Fontspring: ein Marktplatz für Fonts, der Lizenzen transparent und fair gestaltet, insbesondere werden keine Font-Tracker eingesetzt. Sie hosten Ihre Schriften selbst. <https://www.fontspring.com/fair-fonts>
- ▶ FontSquirrel bietet kostenlose Schriften auch für den kommerziellen Gebrauch. Es werden auch Schriften zum Selbsthosten angeboten. <http://www.fontsquirrel.com/>

Last but not least können Sie auch Google-Fonts-Downloader nutzen. Diese nehmen eine Google-Fonts-URL und erstellen daraufhin einen vollständigen lokalen Satz von CSS- und Schriftdateien, mit denen die Website arbeitet.

Dies ermöglicht Webschaffenden, Google-Fonts mit wenig zusätzlichem Aufwand zu verwenden, ohne sie direkt von Google einzubinden. Sie können die benötigte Schriftdatei herunterladen und sie **auf Ihrem eigenen Webserver hosten**.

WIDGETS FÜR SOZIALE MEDIEN



Wenn Sie „Gefällt mir“- oder „Teilen“- oder andere Social-Media-Schaltflächen auf Ihrer Website haben wollen, stellen **Facebook, Twitter, Instagram und Co** dafür Code-Schnipsel zur Verfügung. Diese senden Informationen über jeden Besuch auf Ihrer Website zurück an diese Sozialen Medien, selbst wenn die Buttons gar nicht angeklickt werden.

Es gibt jedoch zahlreiche Möglichkeiten, dies zu umgehen und die Funktionalität dennoch zu erhalten. Eine davon ist die Verwendung von Social Share Privacy, von dem eine JavaScript- und eine Nicht-JavaScript-Option verfügbar ist.

<https://panzi.github.io/SocialSharePrivacy/index.de.html>

Der Social-Buttons-Generator Sharingbuttons.io ist eine weitere Alternative zur Vermeidung von Tracking und JavaScript ist. Da für diese Buttons kein JavaScript genutzt wird, werden sie sehr schnell geladen und beeinträchtigen die Leistungsfähigkeit Ihrer Website nicht.

<https://sharingbuttons.io/>

Natürlich besteht auch die Möglichkeit, dass Sie Buttons selbst erstellen.

CAPTCHAS

Um Spam in usergenerierten Inhalten (z.B. Kommentaren) zu verhindern, werden gerne Captchas genutzt. Sie wissen schon, diese verzerrten Buchstaben oder Bildchen, wo wir Ampeln oder Zebrastrifen anklicken müssen. Das können Computer oder „Bots“ im Normalfall nicht lösen, deshalb zwingen Captchas Menschen, das zu tun. Es gibt allerdings eine Menge guter Gründe, Captchas nicht zu verwenden.

Zum einen können Captchas eine fast unüberwindbare Hürde für Menschen mit Behinderungen werden. Viele Captchas können von Menschen mit Seh-oder Hörproblemen nicht gelöst werden. [Siehe: Websites für alle zugänglich machen].

Zum anderen haben derzeit viele Captchas Probleme mit dem Datenschutz. Glücklicherweise gibt es Alternativen, bei denen Sie Ihre Website mit einfachen Captcha- oder Honeypot-Methoden schützen, ohne dass externer Java Script-Code geladen werden muss. Achten Sie beim Konfigurieren auf Benutzerfreundlichkeit und den Datenschutz. Einige Beispiele für alternative Captchas sind:



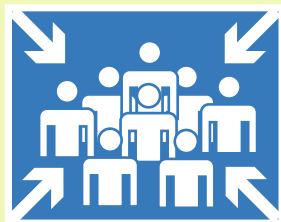
► Drupal: <https://www.drupal.org/project/captcha>

- ▶ Wordpress für Kontaktformular 7 mit Honeypot: <https://wordpress.org/plugins/contact-form-7-honeypot/>
- ▶ Wordpress Secure Image Captcha: <https://wordpress.org/plugins/securimage-wp/>
- ▶ Securimage: <https://www.phpcaptcha.org/>
- ▶ IndyCaptcha: <https://github.com/dyne/indycaptcha>
- ▶ PrivacyCaptcha: <https://privacy-captcha.net/>

Wenn Sie ein Captcha selbst programmieren, darf es einfach sein – bis jemand einen Bot speziell für Ihr Captcha programmiert, was hoffentlich nie passiert.

... UND WEITERE:

Tools zur Organisation von Veranstaltungen und zur Mitgliederverwaltung



Dreh- und Angelpunkt für politische oder soziale Bewegungen sind persönliche Treffen. Bei der Organisation solcher Veranstaltungen dürfen Informationen über die Teilnehmenden nicht an Dritte gelangen. Wir empfehlen:

- ▶ Odoo [ehemals OpenERP] ist eine umfangreiche Management-Software, die u.a. auch beim Veranstaltungsmanagement hilft. <https://www.odoo.com>
<https://www.odoo.com/page/events>

- ▶ Attendize ist eine Open-Source-Plattform für Ticketverkauf und Eventmanagement.
<https://www.attendize.com/>
- ▶ Pretix ist eine freie und quelloffene Software für Ticketverkauf. <https://pretix.eu>
- ▶ Pretalx ist eine freie und quelloffene Konferenzsoftware. <https://pretalx.com/>
- ▶ CiviCRM ist eine freie Software für Customer- bzw. Constituent-Relationship-Management auf Drupal-Basis. Digitalcourage setzt CiviCRM vielseitig ein: Um den E-Mail-Newsletter zu verschicken, aber auch für Aktionswebsites, mit denen Unterschriften für Petitionen und Beschwerden gesammelt werden.
<http://civicrm.org/>

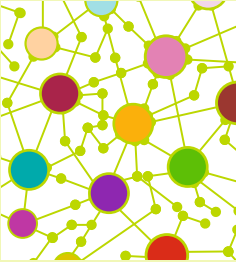
WEBSITES FÜR ALLE ZUGÄNGLICH MACHEN

Das barrierefreie Design von Websites trägt maßgeblich dazu bei, dass Menschen mit Behinderung uneingeschränkten Zugang zu Online-Diensten und Produkten haben. Das W3C hat diesbezüglich sehr nützliche Standards entwickelt:

- ▶ <https://www.w3.org/WAI/>
- ▶ <https://www.w3.org/standards/webdesign/accessibility>
- ▶ <https://www.washington.edu/accesscomputing/sites/default/files/30-Web-Accessibility-Tips.pdf>



DAMIT DAS WEB VERNETZT BLEIBT



Wir sprechen vom Internet als Netzwerk, weil die vielen Websites mit Links aufeinander verweisen können. Informationen, die Sie nicht selbst anbieten (z.B. Quellenangaben oder Wissensseiten wie Wikipedia) können Sie einfach verlinken und damit auf Ihrer Website zusammenführen. Allerdings kann es immer wieder

passieren, dass Websites, auf die Sie verweisen und die nicht in Ihrem Einflussbereich liegen, aus dem Internet verschwinden. Das kann viele Ursachen haben – z.B. Zensur oder DDoS-Angriffe (siehe oben), oder die Websites werden einfach nicht mehr gepflegt. Es liegt jedoch auch in Ihrer Verantwortung, dafür zu sorgen, dass man von Ihrer Website aus auf die von Ihnen verlinkten Inhalte zugreifen kann.

Dazu kann man zentrale Archivierungsdienste (z.B. das Internet-Archive oder perma.cc) nutzen oder ein eigenes Archiv mit dem Amber-Tool anlegen. Diese Dienste und Open Source-Tools erstellen eine Momentaufnahme jeder auf der Seite verlinkten Website und archivieren sie. So kann die Information, die Sie für Ihren Verweis verwenden wollen, nicht einfach verschwinden oder verändert werden.

► <http://amberlink.org/>

► <https://perma.cc/>



ETHISCHE WERBUNG

Sie sollten darüber nachdenken, ob Sie tatsächlich Online-Werbung auf Ihrer Website zulassen wollen, die Ihre Nutzer ausspioniert und deren Daten zum Verkauf anbietet. Es gibt Alternativen, mit denen sich dieses fragwürdige Geschäftsmodell umgehen lässt:

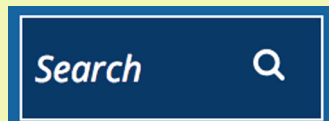
► <https://docs.readthedocs.io/en/latest/advertising/ethical-advertising.html>

WEBSITE-SUCHE

Wenn Sie eine Suchfunktion auf Ihrer Website anbieten, nutzen Sie Suchmaschinen, die Ihre Benutzer nicht ausspähen. Wir empfehlen z.B.:

► <https://metager.de>

► <https://yacy.net/>



Diese Broschüre

ist das Ergebnis einer umfangreichen Zusammenarbeit der Expertinnen und Experten des EDRI-Netzwerks [Anders Jensen-Urstad, Walter van Holst, Maddalena Falzoni, Hanno „Rince“ Wagner, Píksel], externer Beiträge [Gordon Lennox, Achim Klabunde, Laura Kalbag, Aral Balkan, Christian Pietsch] und der besonderen Hilfe von Sid Rao, Public Interest Technologist und Ex-Ford-Mozilla Fellow bei EDRI. Besonderer Dank geht an Joe McNamee, der die ursprüngliche Idee zu diesem Heft hatte und dieses Projekt zu einem erfolgreichen Abschluss brachte.



Produktion der englischen Fassung:

Projekt-Koordination:
Guillermo Peris, Community
Coordinator, EDRI

Layout: Heini Järvinen,
Senior Communications
Manager, EDRI

Veröffentlicht unter einer Creative-Commons-4.0-Lizenz:

<http://creativecommons.org/licenses/by-nc-sa/4.0/>



► digitalcourage

Digitalcourage e.V. engagiert sich seit 1987 für Grundrechte, Datenschutz und eine lebenswerte Welt im digitalen Zeitalter. Wir sind technikaffin, doch wir wehren uns dagegen, dass unsere Demokratie „verdatet und verkauft“ wird. Seit 2000 verleihen wir die BigBrotherAwards. Digitalcourage ist gemeinnützig, finanziert sich durch Spenden und lebt von viel freiwilliger Arbeit.

Wir sind Mitglied des EDRI-Netzwerks [siehe Seite 38] und organisieren mit anderen zusammen regelmäßig das jährliche Datenschutz-Barcamp „Freedom not Fear“ in Brüssel.

► Mehr zu unserer Arbeit finden Sie auf digitalcourage.de und bigbrotherawards.de.

Was ist EDRI?

EUROPEAN DIGITAL RIGHTS



EDRI wurde 2002 gegründet und ist die größte europäische Vereinigung von Organisationen, die sich für Datenschutz, Privatsphäre und Freiheit im Internet einsetzen.

Aktuell haben sich unter dem Dach von EDRI 42 Nicht-regierungsorganisationen zusammengeschlossen und weitere 30 Personen und Organisationen kooperieren im sog. Beobachterstatus eng mit uns.

Unser Ziel ist es, Menschenrechte und Rechtsstaatlichkeit auch im digitalen Umfeld zu fördern und zu schützen. Dies umfasst insbesondere das Recht auf Privatsphäre, Datenschutz, Meinungs- und Informationsfreiheit.

Unsere Vision ist ein Europa, in dem staatliche Behörden und private Unternehmen die grundlegenden Rechte und Freiheiten eines jeden Individuums auch und gerade in der digitalen Welt respektieren.

Unser wichtigstes Ziel ist es, Strukturen zu errichten, die es Zivilgesellschaften und Einzelpersonen ermöglichen, am technologischen Fortschritt teilzuhaben, und in denen die Einhaltung ihrer Rechte sichergestellt ist.

MASSENÜBERWACHUNG. WILLKÜRLICHE ZENSUR. INHALTSBESCHRÄNKUNGEN.

Unternehmen und Regierungen schränken
unsere Freiheiten zunehmend ein.

Spenden Sie jetzt:

<https://edri.org/donate>

PRIVATSPHÄRE! REDEFREIHEIT! ZUGANG ZU WISSEN UND KULTUR!

Wir verteidigen Rechte und Freiheiten online.



EUROPEAN DIGITAL RIGHTS

web: <https://edri.org>

Twitter: [@edri](https://twitter.com/edri)

mail: brussels@edri.org

FAIRE WEBSITES

KOMPAKTWISSEN FÜR PROGRAMMIERUNG UND REDAKTION

Wer Ihre Website besucht, verdient Respekt. Diese Broschüre erklärt, was Sie dafür tun können, dass keine Daten Ihrer Besucher:innen an Dritte abfließen. Außerdem geben wir Tipps für die IT-Sicherheit – und das beste: „Ganz nebenbei“ halten Sie damit auch schon eine Menge Datenschutzgesetze ein.



Digitalcourage e.V.
Marktstraße 18 | 33602 Bielefeld
mail@digitalcourage.de | digitalcourage.de
T: +49 521 1639 1639



9 783934 636255

2,50 Euro
3,00 SFR

 **digitalcourage**

ISBN 978-3-934636-25-5 | k&m001 Faire Websites