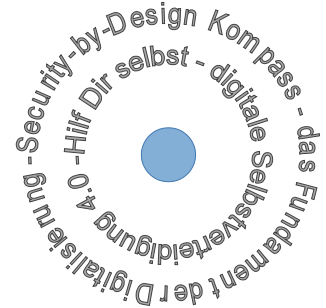




<p>- Daten sind das Gold des digitalen Zeitalters!</p> <p>- Wenn Du Dich im Internet bewegst, hinterlässt Du bei jedem Klick Spuren!</p> <p>- Daten sind ruckzuck verbreitet und es gibt viele Goldgräber mit verschiedensten Absichten!</p> <p>- Das Internet ist schnell, Daten sind leicht zu finden und auszuwerten! Löschen ist fast unmöglich!</p> <p>- Trotz Verschlüsselung gibt es viele Möglichkeiten, Dich zu erkennen und deine Aktivitäten auszuspionieren!</p> <p>- Wie Du anderen Goldgräbern das Handwerk legst!</p> <p>- In zehn Schritten zur Sicherung des Daten-Goldes!</p> <p>- Beuge dem Eigenleben Deiner Daten und dem Datenklau vor!</p>	<p>Das Problem</p> <hr/> <p>Das Ziel</p>
---	--



Die **digitale Selbstverteidigung** ist die Fähigkeit, die Herausforderungen durch die komplexe Medienlandschaft konstruktiv zu bewältigen.

Die angegebenen Maßnahmen sollen Schülerinnen, Schüler und Lehrerschaft in die Lage versetzen, den Mediengebrauch verantwortungsvoll und angemessen zu gestalten. Damit werden die Chancen der Digitalisierung bei gleichzeitiger Risikominimierung zur Wahrung der persönlichen Gestaltungsfreiheit genutzt.

**Weitere Empfehlungen und Kommentare:**  
[https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/empfehlungen\\_node.html](https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/empfehlungen_node.html)  
<https://www.kuketz-blog.de/kommentar-microsoft-google-apple-und-co-aus-bildungseinrichtungen-verbannen/> (Jan20)

**Hundertprozentige Sicherheit gibt es leider nicht, aber wer durchblickt, dem eröffnen sich neue Chancen! Beachten Sie den Hinweis (8)!**

*Dieser Kompass entstand datensparsam unter Verwendung von Linux/DarwinOS und Libreoffice. Die Recherche erfolgte mittels datensparsam konfigurierten Firefox-Browser mit den AddOns „NoScript“, „httpsEverywhere“ und „PrivacyBadger“. Die Abstimmung der Inhalte erfolgte mittels gpg-verschlüsselter E-Mail.*

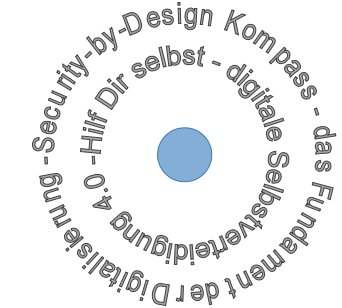
**(1) Betriebssysteme**

*Betriebssysteme kennen Dein Gerät und alles, was sich darauf befindet.*

**allgemeine Tipps:** (Jan19)  
<https://digitalcourage.de/digitale-selbstverteidigung/>, <https://ssd.eff.org/>  
**-Nutze datensparsame Betriebssysteme und konfiguriere sie so, dass:**  
 - kein Mikrofon/Kamera aktiv ist (Anschalten im Bedarfsfall für eine Anwendung, Ausschalten nicht vergessen!)  
<https://www.bim.de/files/pdf1/bim-selbstschutz.pdf>,  
<https://www.zeit.de/digital/datenschutz/2019-08/michael-waidner-it-sicherheit-technologie-kamera-mikrofon/komplettansicht> (Nov19)  
 - keine Telemetriedaten erhoben und versendet werden  
 - keine Clouddienste verwendet werden  
 - keine externe Sprach- und Sprechererkennung erfolgt  
**- Verwende datensparsame Anti-Virus-Programme**  
**- Sichere Deine Daten auf nur kurzzeitig angeschlossenen Systemen, sichere am Besten auf DVD (Schutz vor Ransomware)**

**Spezielle Tipps:**

- **Kennst Du Linux?** – PC (z.B. DebianEdu)  
<https://www.skolelinux.de/de/>, <http://www.linuxmuster.net/de/start/>,  
<https://schulnetzkonzept.de>, <https://digitalcourage.de/digitale-selbstverteidigung/gnulinux-now> (Nov 21),  
 Mobile (z.B. LineageOS, Ubuntu Touch)  
[https://de.wikipedia.org/wiki/Fairphone\\_2](https://de.wikipedia.org/wiki/Fairphone_2) oder  
<https://digitalcourage.de/digitale-selbstverteidigung/befreien-sie-ihr-smartphone> (Jan2019)  
**- Falls Du Windows 10 benutzen musst - erheblicher Konfigurationsbedarf!** Siehe [https://www.ti-sicherheit.mpg.de/Orientierungshilfe\\_Windows10.pdf](https://www.ti-sicherheit.mpg.de/Orientierungshilfe_Windows10.pdf)  
[https://www.datenschutzkonferenz-online.de/media/ah/20191106\\_wi10\\_pruefschema\\_dsk.pdf](https://www.datenschutzkonferenz-online.de/media/ah/20191106_wi10_pruefschema_dsk.pdf) (Dez19)  
 - benutzerdefinierte Installation  
 - bereitgestellte Datenschutzoptionen (u.a. zu Werbelid, Schreibverhalten, Nutzer-/App Protokollierung)  
 - lokale Konten (kein Microsoft-Konto)  
 - Apps Dritter (z.B. Browser, E-Mail)  
 - niedrigstes Telemetrieniveau (basic, trotzdem keine vollständige Sperrung)  
<https://www.heise.de/select/ix/2019/05/1908016054629797396> (Mai19)  
**- Beachte Deaktivierungshinweise zu Cortana, Spracherkennung, Verbindungs- und Fehlerberichterstattung, Clouddienste als Datenspeicher**  
**- Überprüfe Konfiguration nach Update!**

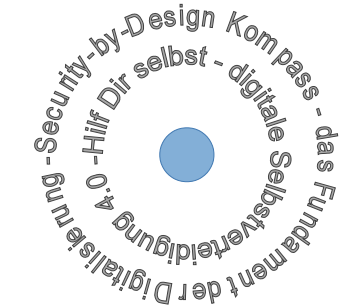


**(2a) Internetbrowser**

*Browser wissen viel über Dich und sind die „Tür zum Internet“.*

**Tipps zur Grundsicherung:**  
 - **Achte** bei Browserwahl auf datenarme Konfigurierbarkeit, Erweiterbarkeit und Updatefähigkeit, **Startseite** des Browsers und **neue Tabs auf leere oder lokale Seite** setzen! (about:blank)  
<https://digitalcourage.de/digitale-selbstverteidigung/>  
<https://www.youngdata.de/digitale-selbstverteidigung/allgemeines/browsersicherheit/> (Jan19)  
<https://restoreprivacy.com/secure-browser/>  
**-Schau mal bei den Anregungen** unter <https://restoreprivacy.com/secure-browser/> u. <https://www.kuketz-blog.de/umgang-mit-daten-im-privatleben-datensouveraenitaet-teil3/> (Jan19)  
**- Kennst Du z.B. - Firefox**  
<https://restoreprivacy.com/firefox-privacy/> und <https://www.kuketz-blog.de/firefox-ein-browser-fuer-datenschutzbewusste-firefox-kompendium-teil1/>  
 - Waterfox, Pale Moon, Brave <https://github.com/brave/brave-browser/issues/3479> (Nov19)  
**Achtung Konfigurationsbedarf und achte auf Aktualisierungen, Prüfe Korrektheit der Einstellungen nach Update**  
 Umgebungsvariable **SSLKEYLOGFILE** leeren/entfernen  
<https://www.heise.de/security/artikel/Browser-SSL-entschluesst-1948431.html> (Nov19)

- **Schau** Videos datensparsam über Proxy: <https://redirect.indivio.us/> (Mai21)  
 - **Blocken von Trackern z. B. mit:** Privacy Badger, NoScript, uBlock Origin, uMatrix, Decentraleyes  
**Achtung:** Alle Programme müssen konfiguriert werden! Ein Kompass für Konfiguration ist in Vorbereitung!  
 - **Anzeige von Verbindungen zu Servern und Erzwingen von Verschlüsselung z.B.:** HTTPS Everywhere  
 - **Cookie Management z.B.:** Cookie Autodelete, Clear Flash Cookie  
 - **Verstecken von Nutzern z.B.:** User Agent Platform Spoofers  
 - **Durchleuchte Webseiten z.B mit** Webdeveloper oder Test auf Tracker [privacyscore.org](https://privacyscore.org) bzw. [webbkoll.datakydd.net](https://webbkoll.datakydd.net)  
 - **Verwende strenge user.js Dateien**  
<https://www.kuketz-blog.de/firefox-aboutconfig-user-js-firefox-kompendium-teil10/>  
**- Teste Browser auf SSL-Sicherheit**  
<https://www.ssllabs.com/ssltest/viewMyClient.html> (Jan19)

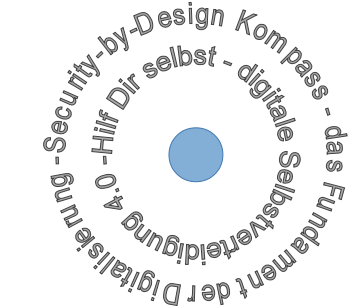


**(2b) Internetbrowser**

*Browser-URLs sind Postkarten (http) bzw. Briefe (https) - der Absender, der Empfänger und die Form des Briefumschlags sind immer erkennbar*

**- Konfiguriere, aktualisiere und nutze** Browser AddOns: <https://privacy-handbuch.de/download/privacy-handbuch.pdf> (Jan19)  
**Tipps zu speziellen AddOns:**  
 - Panopticon zeigt Dir, ob man Dich erkennt, Lightbeam zeigt Verbindungen  
 - Anonymisierungsdienste können die eigene Präsenz verschleiern helfen: [https://anon.inf.tu-dresden.de/helpp/jap\\_help/de/helpp/jondonym.html](https://anon.inf.tu-dresden.de/helpp/jap_help/de/helpp/jondonym.html)  
**- Anregung:** informiere Dich über Suchmaschinen **bevor** Du sie nutzt! Trage Dir eine datensparsame Suchmaschine als Default ein!  
<https://digitalcourage.de/digitale-selbstverteidigung/es-geht-auch-ohne-google-alternative-suchmaschinen> (Jan19)  
**- Schau mal:** Datenanalyse zur Schaffung von Transparenz von Datennutzung und -verwertung am Beispiel von Facebook  
<https://labs.rs/en/quantified-lives/>, [https://labs.rs/wp-content/uploads/2016/08/FacebookFactory01\\_gif](https://labs.rs/wp-content/uploads/2016/08/FacebookFactory01_gif) (Jan19)

**(3) Apps**  
*Die Apps kennen alle Daten, auf die sie Zugriff haben.*  
**Tipps:**  
 - **Überprüfe** App Zugriffe und Verbindungen vor dem Einsatz z.B. [exodus-privacy.eu.org](https://exodus-privacy.eu.org)  
 - **Konfiguriere** Apps datensparsam <https://digitalcourage.de/digitale-selbstverteidigung/mobil> (Jan19)  
 - **bevorzuge lokale Apps (Need-to-know)**  
**-Blockiere** Zugriffe durch App Einstellungen auf dem Telefon (z.B. auf Mikrofon, Kamera, Speicher)  
 - **Verwende z.B. BLOKADA** zur Sperrung von Trackern und SHELTER Sandbox <https://www.kuketz-blog.de/slugmap> (Mai20)  
 - **Blockiere** Zugriffe zu Positionsdaten (WLAN, IP, GPS)  
 - **Kennst du offene App-Downloads wie F-Droid?** [https://fdrii.org/files/defenders\\_v\\_intruders\\_de\\_web.pdf](https://fdrii.org/files/defenders_v_intruders_de_web.pdf) 01/19  
**Achtung!** Vermeide unbedingt Apps mit ständig aktivierten Mikrofon und Kamera im Unterricht, sie zeichnen Dich und die Umgebung auf, stören mit akustische Meldungen oder geben persönliche Nachrichten preis!



**(4) Suchmaschine**

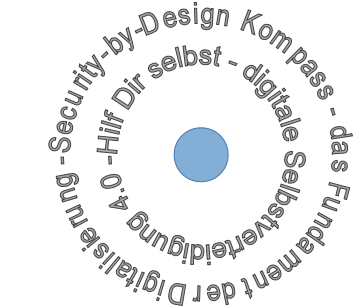
*Die meisten Suchmaschinen (durch-)suchen auch Dich.*

**Tipps:**  
 Kennst Du die Suchmaschinen?  
 - [lite.quant.com](https://lite.quant.com)  
 - [MetaGer.de](https://www.metager.de)  
 - [YaCy.net](https://www.yacy.net)  
 schau doch mal unter <https://digitalcourage.de/digitale-selbstverteidigung/es-geht-auch-ohne-google-alternative-suchmaschinen> (Jan19)  
 - Mit Suchanfragen und aktivierten Suchvorschlägen gibst Du Informationen über Dich preis (Profilbildung)  
**- Kennst Du die Kindersuchmaschinen:**  
 - [blinde-kuh.de](https://blinde-kuh.de) ? – Analytics-frei für den besonderen Schutz für Kinder (Jan2019)  
 - [quantjunior.com](https://www.quantjunior.com) (Mai2019)  
**Wichtig:** Empfohlen ist die direkte Suche, bei Drittanbietern gibt es oftmals personalisierte Ergebnisse.

*Auf Aktualisierungen achten!*

**(5) E-Mail**  
*E-Mails sind elektronische Postkarten, die ohne Gegenmaßnahmen von jedermann gelesen werden können.*

**Tipps:**  
 - **Interesse an sicheren E-Mail Anbietern?** Dann findest Du Infos hier: [https://www.privacy-handbuch.de/handbuch\\_31.htm](https://www.privacy-handbuch.de/handbuch_31.htm) (Jan2019)  
**- Kennst Du extra E-Mail Programme mit Verschlüsselung (z.B. Thunderbird mit Enigmail)?** siehe in [https://fdrii.org/files/defenders\\_v\\_intruders\\_de\\_web.pdf](https://fdrii.org/files/defenders_v_intruders_de_web.pdf) oder <https://www.kuketz-blog.de/umgang-mit-daten-im-privatleben-datensouveraenitaet-teil3/>  
[https://www.privacy-handbuch.de/handbuch\\_31a0.htm](https://www.privacy-handbuch.de/handbuch_31a0.htm)  
<https://digitalcourage.de/digitale-selbstverteidigung/pc> (Jan19)  
**- Lass Dir immer den langen E-Mail Briefkopf (Header) anzeigen und überprüfe die Email-Adressen**  
 - Verwende datenarme Virens Scanner!  
 - **Nutze** dienstl. nur. Dienst-Email, keine Weiterleitung, prüfen Sie eingehende Mail  
**- Empfohlen:** kein automatisches Nachladen von Bildern und Öffnen von Links im Webbrowser, keine html Mails



## Schulwebauftritt (6)



Mit Deinem Webauftritt übernimmst Du Verantwortung für IT-Sicherheit und Datenschutz für Dich und Deine Nutzer.

### Tipps:

- Nutze lokale Schriftarten,
- Übersetzungs-, Vorlesedienste
- Gib Löschrufen für gespeicherte Daten an und halte sie ein
- Prüfe auf voreingestellte, ungewollte Analytics-Funktionen der Software
- Verwende Opt-In anstelle von Opt-Out
- Verwende IP-Adressanonymisierung auf Metaebene [https://www.theregister.co.uk/2018/05/25/schrems\\_vs\\_back\\_facebook\\_google\\_get\\_served\\_gdpr\\_complaint/](https://www.theregister.co.uk/2018/05/25/schrems_vs_back_facebook_google_get_served_gdpr_complaint/) (Jan19)
- Vermeide Webfonts, Analytics
- Teste Deinen Webauftritt unter [privacyscore.org](https://privacyscore.org), [webbkoll.dataskydd.net](https://webbkoll.dataskydd.net), [sslabs.com/ssltest](https://sslabs.com/ssltest)
- Login Bereiche nur mit https!
- Nutze Videos nur vom genutzten Server bzw. lokal gespeichert
- Nutze Server-lokale Captcha Skripte

Bekannt genutzt?

## Soziale Netzwerke, Chat, Messenger, Navigationsdienste (7)

Soziale Netzwerke kennen Dich und Deine Freunde und Kontakte. Navigationsdienste kennen Deinen Standort und Reiseziele. Sie wollen Deine Daten.

### Tipps:

- Kennst Du dezentrale, Open Source basierte soziale Netzwerke? z.B. aus dem Fediverse <https://digitalcourage.de/blog/2018/kommt-mit-uns-ins-fediverse> <https://www.heise.de/download/specials/Die-besten-Facebook-Alternativen-4039433> (Jan2019)
- Kennst Du zum Beispiel datensparsame Messenger (z.B. Jabber/XMPP) <https://digitalcourage.de/digitale-selbstverteidigung/alternativen-zu-whatsapp-und-threema-instant-messenger/> (Jan19)
- Kennst Du zum Beispiel datensparsame IRC Klienten (z.B. Xchat)? siehe <https://privacy-handbuch.de/download/privacy-handbuch.pdf> oder <https://digitalcourage.de/digitale-selbstverteidigung/alternativen-zu-whatsapp-und-threema-instant-messenger/> (Jan19)
- Aktiviere Ende-zu-Ende-Verschlüsselung (OMEMO)

Bekannt genutzt?

## Internet-Gateway/Firewall (8)

Das Gateway ist das Tor zum Internet und die letzte Verteidigungslinie für die Systeme des Nutzers.

### Tipps:

- über DNS kannst Du unerwünschte Dienste ausblenden, deshalb konfiguriere und betreibe eigene DNS Server oder den des Providers, keine Drittanbieter, verwende verschlüsselte DNS Anfragen (DNS over HTTPS)
- Unterdrücke Telemetrie <https://github.com/crazy-max/WindowsSpyBlocker/blob/master/data/hosts/spy.txt> (Oct19)
- Konfiguriere und verwende Firewalls zur Filterung im Netzwerk
- Konfiguriere und betreibe Intrusion Prevention Systeme zum Schutz vor Schadcode
- Prüfe und konfiguriere App-Zugriffe z.B. bei [exodus-privacy.eu.org](https://exodus-privacy.eu.org) (u.a. Zugriffe auf Smartphone-Dienste) <https://exodus-privacy.eu.org/en/page/> (Jan19)

Bekannt genutzt?

## Passwort (9)



Passwörter sind eine wichtige Maßnahme zur Sicherung der digitalen Identität.

### Tipps:

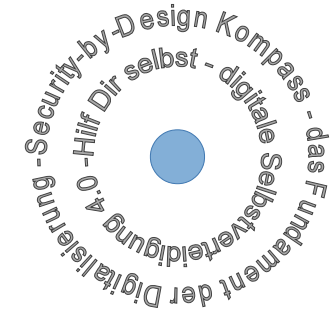
- Verwende lange Passwörter (mind. 10 Zeichen) mit Sonderzeichen und Zahlen ohne bekannte Wörter
- Verwende jedes Passwort nur für einen Dienst/Account
- Bilde und merke Dir einen geheimen Satz und erzeuge daraus das Passwort anhand z. B. der Anfangsbuchstaben und Zahlen, Beispiel: „Im Urlaub 2018 hatte ich einen blauen Badeanzug mit 17 Streifen und 8 Punkten!“ IU2hiebBm1Su8P! oder:
- Verwende lokale Passwortgeneratoren und lokale OpenSource Passwortmanager siehe auch: [https://www.bsi-fuer-buerger.de/BISFB/DE/Empfehlungen/Passwoerter/passwoerter\\_node.html](https://www.bsi-fuer-buerger.de/BISFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html) (Jan20)

## Konsequenzen

Mit Privacy-by-Design wird die Nachhaltigkeit aktiv unterstützt! Durch Blocken und Code-Reduktion werden Energiekosten gesenkt.

<https://www.sueddeutsche.de/digital/nachhaltig-surfen-wie-das-internet-strom-frisst-1.4578748> (Sep 19)  
Ohne Privacy-by-Design ergeben sich direkte und spürbare Konsequenzen! Das FBI warnt! <https://www.ic3.gov/media/2018/180913.aspx>

Bereits im Einsatz: Beeinflussung der Souveränität, z.B. nicht zur Wahl zu gehen, <https://qz.com/916801/americans-dont-know-their-neighbors-anymore-and-thats-bad-for-the-future-of-democracy/> (Sep19)  
dynamische, personalisierte Preisgestaltung:  
- Profibildung  
- Neuro Marketing  
- verhaltensbasiertes Marketing  
- algorithmische Entscheidungsfindung  
- Kreditwürdigkeit von Personen  
- personenbezogene Preisermittlung „Also besonders gut eignen sich all die Produkte, wo der Käufer kein Gefühl dafür hat, was sie kosten.“ [https://www.abida.de/sites/default/files/Gutachten\\_Handel\\_Bezahlsysteme.pdf](https://www.abida.de/sites/default/files/Gutachten_Handel_Bezahlsysteme.pdf) – E5 – Seite 77 (Jan19)



- Nutze lokale Suchfunktionen
- Kennst Du Open Data Karten- und Navigationsdienste? Bsp. Openstreetmap siehe in <https://www.schulportal-thueringen.de/np/resourcen/medien/38205?dateiname=Joeran-Muuss-Merhoiz-Freie-Unterrichtsmaterialien-Beltz-2018.pdf> (Jan10)
- Prüfe bei Webbaukästen auf integrierte Verbindungsaufbauten an Dritte und deaktiviere sie
- Informiere dich zu datensparsamen Terminplanern z.B. unter <https://www.fdm.uni-hamburg.de/service/werkzeuge.html> (Jan2019)
- Binde Vorlesedienste, Clouddienste, Übersetzungen lokal ein
- Vermeide eine Kombination von Drittanbietern bei Verwendung von anonymisierten Diensten z.B. anonymisierte Analytics und Webfonts

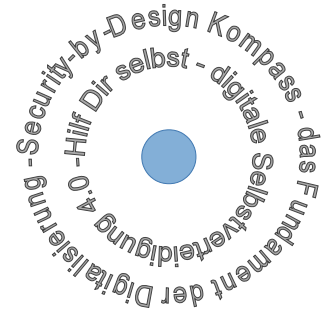
Bekannt genutzt?

- Kennst Du alternative Navigationsdienste? wie z.B. <https://www.openstreetmap.org/> <https://map.project-osrm.org/> <https://maps.metager.de/map/> <https://digitalcourage.de/digitale-selbstverteidigung/wege-finden-ohne-google-maps-openstreetmap/> (Mai20)

- Vermeide datenreiche Messenger (u.a.) WhatsApp zu WhatsApp in der Schule siehe in [https://www.gew-thueringen.de/index.php?eID=dumpFileStr&file=71477&token=aac68c7661509eb1cb976fedbc49461070011b5&download=&n=Datenschutz\\_in\\_der\\_Schule\\_Vortrag\\_des\\_T\\_hueringer\\_Datenschutzbeauftragten\\_auf\\_der\\_LVV\\_der\\_GEW\\_Thueringen\\_21092018.pdf](https://www.gew-thueringen.de/index.php?eID=dumpFileStr&file=71477&token=aac68c7661509eb1cb976fedbc49461070011b5&download=&n=Datenschutz_in_der_Schule_Vortrag_des_T_hueringer_Datenschutzbeauftragten_auf_der_LVV_der_GEW_Thueringen_21092018.pdf) S. 14 (Jan19)

Bekannt genutzt?

- Abmelden? Bsp. Whatsapp, Facebook: (Android) <https://faq.whatsapp.com/en/android/2119703?lang=de> (iOS) <https://faq.whatsapp.com/de/iphone/21325453?category=5245246> <https://de-de.facebook.com/help/359046244166395/>
- Informiere Dich über datensparsame und sichere Konferenzen! [https://www.datenschutz-berlin.de/fileadmin/user\\_upload/pdf/orientierungshilfen/2020-BinBDI-Empfehlungen\\_Videokonferenzsysteme.pdf](https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BinBDI-Empfehlungen_Videokonferenzsysteme.pdf) (Mai20) <https://www.baden-wuerttemberg.datenschutz.de/datenschutzfreundliche-technische-moeglichkeiten-der-kommunikation/> (Mai20) Selessa/Moodle: <https://lisa.sachsen-anhalt.de/unterricht/digitale-bildung/e-learning/selessa/> (Mai20)
- Erkenne und blockiere Zugriffs- und Tracking-techniken z.B. über Webfonts und APIs, nutze Hilfsmittel aus (2a), (2b) und (4) wie Privacy Badger, [webbkoll.dataskydd.net](https://webbkoll.dataskydd.net) zur Erkennung und BLOKADA zur Unterbindung

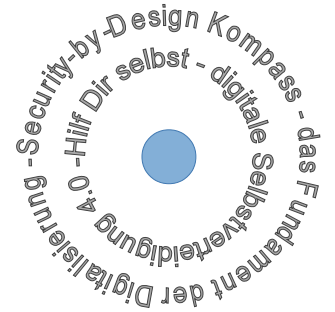


- Blockiere unerwünschte DNS, z.B. [https://www.reddit.com/pihole/comments/930gz2/pisa\\_google\\_services\\_including\\_ads\\_and\\_others\\_try/](https://www.reddit.com/pihole/comments/930gz2/pisa_google_services_including_ads_and_others_try/)
- Teste ssl-Sicherheit für eigene Server (z.B. Webauftritt) mit ssl-Labs <https://www.sslabs.com/ssltest/> (Jan19)
- Kennst Du eigene, lokale Server für Messengerdienste? Achte auf die Absicherung! <https://digitalcourage.de/digitale-selbstverteidigung/alternativen-zu-whatsapp-und-threema-instant-messenger/> (Jan19)
- Teste Verbindungen z.B. mit Wireshark

Bekannt genutzt?

### Wichtig:

Die Informationen und Referenzen stellen einen ersten Einstieg zum Thema dar. Die Inhalte sind vor dem Hintergrund der Informatik erstellt und mit größter Sorgfalt recherchiert. Es kann dennoch keine Haftung für die Richtigkeit, Vollständigkeit und Aktualität der bereitgestellten Informationen übernommen werden. Die Informationen sind insbesondere auch allgemeiner Art und stellen keine Rechtsberatung im Einzelfall dar. Bei Benutzung der Werkzeuge kann keine Haftung für Schäden erfolgen und die Nutzung erfolgt ausschließlich auf eigenes Risiko.



## Büroanwendungen (10)



Die Büroanwendungen kennen alle Daten, die sie verarbeiten.

### Tipps:

- Kennst Du lokal installierte Open Source Anwendungen? z.B. siehe in <https://www.kuketz-blog.de/umgang-mit-daten-im-privatleben-datensouveraentaet-teil3/> (Jan19)
- LibreOffice, GIMP
- Verwende lokale Rechtschreib- und Übersetzungsunterstützung
- Kennst Du digitale Medienschranke? Achte bei Cloud-basierten Anwendungen mit Abo-Modell (u.a. Office 365) und Microsoft Office auf die Datenschutzanalyse <https://www.rikssoverheid.nl/binaries/rikssoverheid/documenten/rapporten/2018/10/07/data-protection-impact-assessment-op-microsoft-office/OPA+Microsoft+Office+2016+and+365+-+20191105.pdf> und <https://www.heise.de/select/ix/2019/5/1907710505118147453> (Mai19)
- Hinweis Die angegebenen Links sind bewusst kleingedruckt und sollten im Digitalen nachgeschlagen werden.

Bekannt genutzt?

„When you shop, your data may be the most valuable thing for sale.“ <https://iripodcast.org/season4/episode1/> (Jan19)  
„Der Regulierer kann gerne eingreifen. Die Frage ist nur, wie man den Unternehmen die Verwendung von personalisierten Preisen nachweist. Ich glaube, es wird sehr schwierig, entsprechende Nachweise zu finden... der Regulierer müsste schnell eingreifen können. Und das bei der schieren Masse an Transaktionen, die am Markt auftreten.“ (...)  
„Und ein Kunde, den ich als reinen Smart-Shopper identifiziere, als relativ untreuen Kunde, der stark auf Aktionen geht, den möchte ich auch nicht unbedingt aktivieren.“ (...)  
„meine Schwester bekommt immer zehnfach Punkte, wieso bekomme ich das nicht? ...“ (...)  
[https://www.abida.de/sites/default/files/Gutachten\\_Handel\\_Bezahlsysteme.pdf](https://www.abida.de/sites/default/files/Gutachten_Handel_Bezahlsysteme.pdf) E5 – Seite 78 und E6 – Seite 81 (Jan19)  
Bei Nichtgefallen des Kunden kann auch das Angebot entzogen werden (getarnt z.B. als Verbindungsabbruch). [https://crackdelabs.org/dl/CrackedLabs\\_Christi\\_CorporateSurveillance.pdf](https://crackdelabs.org/dl/CrackedLabs_Christi_CorporateSurveillance.pdf) Seite 32 (Jan19)