

Digitalcourage e.V., AG Digitale Selbstverteidigung

HOMEOFFICE

Mit Datenschutz und freier Software



▶ digitalcourage

KURZ & MÜNDIG

ART D'AMEUBLEMENT

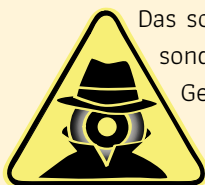
KOSTENFREI

BAND 7

Bei der **Online-Zusammenarbeit** sind schnelle Lösungen oft nicht die besten: Viele Online-Dienste arbeiten nicht Ende-zu-Ende-verschlüsselt oder "verpetzen" die Nutzungsdaten an die Werbeindustrie oder Geheimdienste.

NUTZEN SIE BITTE NICHT DIE DIENSTE DER SOFTWARE-GIGANTEN!

Sie legen nicht nur Ihre Inhalte und Kontakte, sondern unter Umständen auch Ihre kompletten Arbeitsstrukturen gegenüber Geheimdiensten und Firmenkonsortien offen.



Das schadet nicht nur Ihnen und Ihrer Arbeit, sondern mittel- und langfristig der gesamten Gesellschaft. Wir zeigen Ihnen praktische, sichere und häufig kostenlose Alternativen zu den etablierten Diensten.

IMPRESSUM

1. Auflage 03-21, Art d'Ameublement, cc-by 4.0, ISBN 978-3934636-35-4

Erstellt vom Team der AG Digitale Selbstverteidigung,
Maintainer:innen: Sarah Bollmann, Hartmut Göbel und Christian Pietsch

Redaktion: Claudia Fischer, verstandenwerden.de

Layout: Isabel Wienold, iwi-design.de

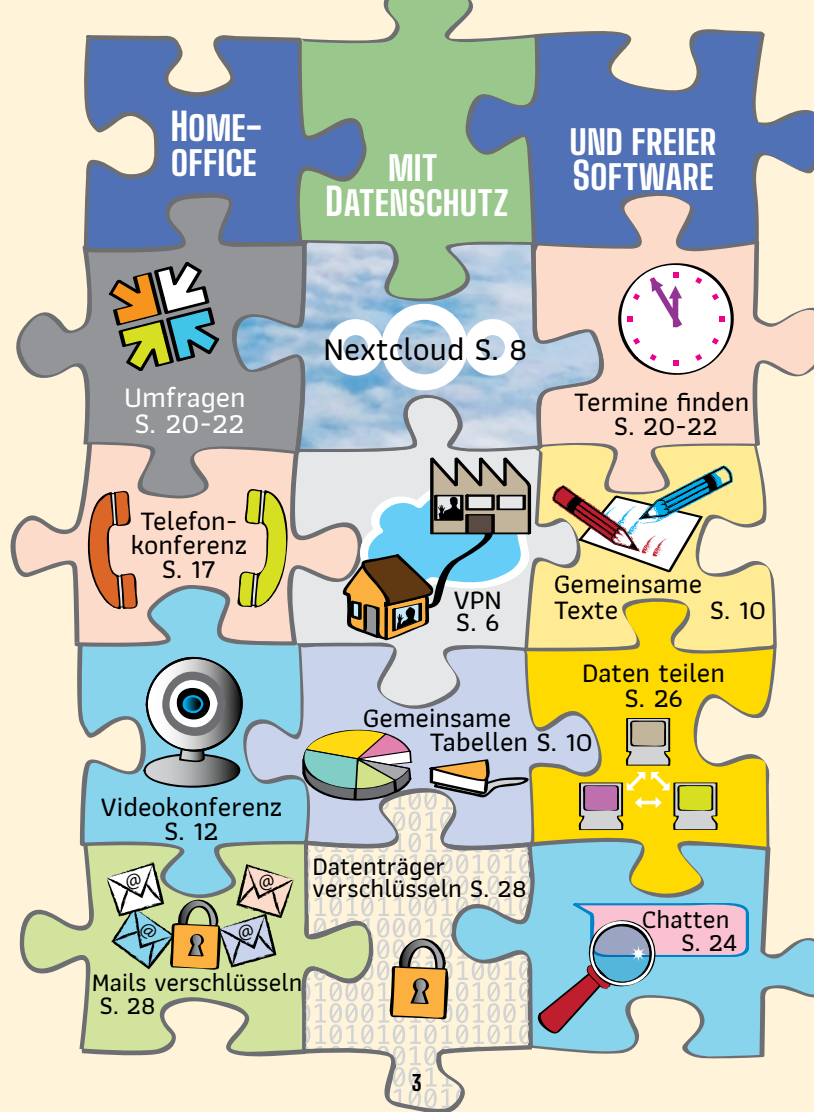
Bildlizenzen: S. 13: Digitalcourage, cc-by 4.0; S. 19: Boston Public Library

on Unsplash; S. 23: screenshot entraide.chatons.org;

S. 26: Ura Design cc-by 3.0; S. 30 oben: Fabian Kurz cc-by 4.0;

S. 30-31: Panthermedia;

Alle weiteren Bilder: iwi-design.de, Isabel Wienold cc-by 4.0



WARUM FREIE SOFTWARE?

Wir empfehlen Ihnen in dieser Broschüre **Freie Software**. Bei Freier Software geht es nicht darum, dass Software kostenlos ist („frei wie Freibier“), sondern darum, dass Software Ihnen nicht Ihre Freiheiten und Rechte raubt („Frei wie Freiheit“).

Woran erkennt man also Freie Software, die Ihre Rechte respektiert? An der Lizenz. Die bekannteste ist die GNU General Public License (GNU GPL). Für eine vollständige Liste fehlt hier leider der Platz.

Freie Software nach Definition der Free Software Foundation räumt ihren Nutzenden per Lizenz vier Freiheiten ein:

”**Freiheit 0**“¹: Die Freiheit, das Programm auszuführen, wie man möchte, für jeden Zweck.

”**Freiheit 1**“: Die Freiheit, die Funktionsweise des Programms zu untersuchen und eigenen Bedürfnissen der Datenverarbeitung anzupassen.

”**Freiheit 2**“: Die Freiheit, das Programm weiterzubreiten und damit seinen Mitmenschen zu helfen.

”**Freiheit 3**“: Die Freiheit, das Programm zu verbessern und diese Verbesserungen der Öffentlichkeit freizugeben, damit die gesamte Gemeinschaft davon profitiert.

¹ Programmierer:innen beginnen beim Zählen gern mit einer Null.

Für die Freiheiten 1 und 3 ist der Zugang zum Quelltext Voraussetzung, da sonst das Verändern eines Programms kaum möglich ist. Darum ist Freie Software immer quell-offen (open source).

Sind diese Freiheiten auch für Menschen relevant, die nicht programmieren können? Ja! Sie können eine unabhängige Firma oder Expertin Ihrer Wahl damit beauftragen, den Quelltext zu prüfen. Nicht selten wird durch Crowdfunding Geld für solche Gutachten (Audits) gesammelt.

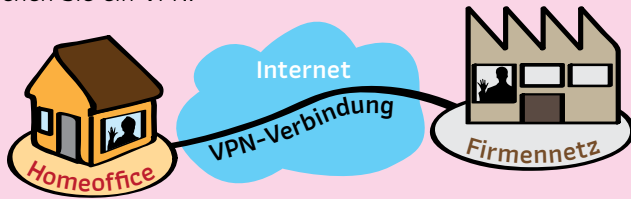
Diese vier Freiheitsrechte ermöglichen die mündige und souveräne Nutzung von Programmen und helfen auch dabei, die Privatsphäre zu wahren.

Ein weiterer großer Vorteil ist die Anbieterunabhängigkeit (kein „vendor lock-in“). Sollte der Anbieter vom Markt verschwinden oder die Software in eine unerwünschte Richtung entwickeln, kann die Weiterentwicklung von anderen übernommen werden („fork“).

Reproducible Builds: Damit können Technik-Kundige mit vertretbarem Aufwand nachprüfen, ob die installierte Hardware wirklich den veröffentlichten Quelltexten entspricht. Wenn Sie Software angeboten bekommen, fragen Sie nach, ob sie reproduzierbar gebaut wurde. Vorreiter sind hier die GNU/Linux-Distribution Debian und der freie App-Store F-Droid, die wir auch deshalb empfehlen.

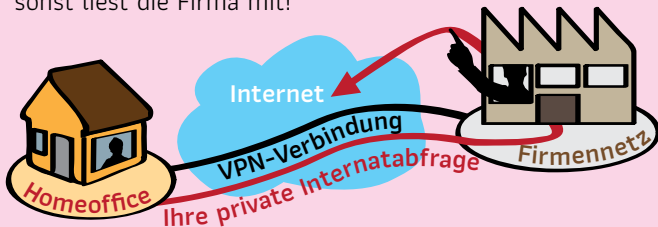
VPN: VOM HOMEOFFICE INS FIRMENNETZ

Wenn Sie von Zuhause auf das Firmennetzwerk zugreifen müssen, weil Sie dortige Dienste oder Dateien brauchen, Kunden- oder sensible Firmendaten austauschen, brauchen Sie ein VPN.



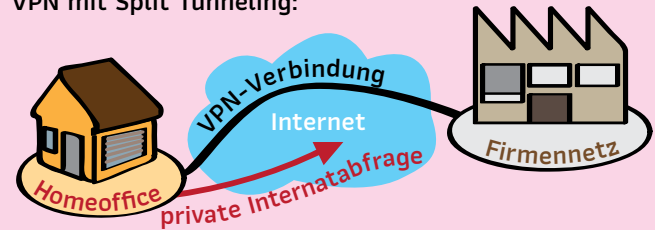
VPN steht für "Virtual Private Network". Das ist meist eine Software, die dafür sorgt, dass sich Ihr Computer so verhält, als sei er direkt ans Netzwerk Ihrer Firma angeschlossen. Dadurch können Sie Dienste im internen Netz ihrer Firma nutzen, als wären Sie selbst dort. Es gibt aber auch Fallen:

VPN kann alle Netzwerkaktivitäten durchs Firmennetz leiten. Vermeiden Sie also private Internet-Aktivitäten, während Sie das VPN aktiviert haben, sonst liest die Firma mit!



Fortgeschrittene können die Option "Split Tunneling" nutzen [siehe unten] – dann wird das VPN nur für Kontakte mit bestimmten IP-Adressbereichen genutzt und Sie können parallel andere Dinge tun, ohne über das Firmennetzwerk zu gehen.

VPN mit Split Tunneling:



Nutzen Sie keine kommerziellen VPN-Dienste!

Viele kommerzielle VPN-Dienstleister werben mit falschen Versprechen wie IT-Sicherheit, Datenschutz oder Anonymität. Fallen Sie nicht darauf rein! Für anonymes Surfen empfehlen wir den Tor-Browser [siehe Seite 27].

Nutzen Sie quelloffene, Freie Software!

Auch wenn Ihre Firma kommerzielle Software einsetzt, müssen Sie das zuhause nicht unbedingt tun. Wer Linux hat, kann `vpnc` nutzen, um sich mit einem Cisco-VPN zu verbinden. Wer per SSH Direktzugriff auf einen Firmenserver hat, kann sich mit `sshuttle` ein eigenes VPN bauen.

EINE LÖSUNG FÜR ZIEMLICH VIELE FRAGEN: NEXTCLOUD

Nextcloud ist eine Open-Source-Software, die viele Zusatz-Module enthält und kleinere Teams bis zu ein paar Dutzend Leuten mit ziemlich vielen Dingen versorgt:

- ▶ Eine verschlüsselte Cloud für die gemeinsame Nutzung und den Austausch von Dateien, Texten, Tabellen, Bildern usw.
- ▶ Pads zum gemeinsamen, gleichzeitigen Arbeiten an Texten
- ▶ Gemeinsame Kalender und Chats
- ▶ Ein Kanban für die Arbeitsorganisation und Aufgabenverteilung
- ▶ Komplette Online-Office-Suite für Textdokumente [siehe nächste Seite]
- ▶ Umfragen und Formulare
- ▶ Nextcloud Talk für Videokonferenzen bis zu vier Personen [mehr werden holprig, ist unsere Erfahrung]

Eine Nextcloud kann man auch selbst aufsetzen, wenn man einen eigenen Server betreibt und z.B. eine IT-Abteilung oder eine.n IT-Administrator.in im Team hat. Hilfestunden gibt's im Internet.

Auf unserer Homepage digitalcourage.de finden Sie unter dem Suchwort "Nextcloud-Hosting" aber auch eine Tabelle mit empfehlenswerten Anbietern, bei denen Sie eine Nextcloud mieten können.

GEMEINSAM TEXTE SCHREIBEN IN DER NEXTCLOUD

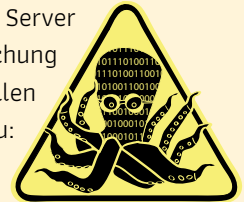
Vorteile: Wenn Sie eine Nextcloud haben und hier Texte gemeinsam bearbeiten, brauchen Sie keine weitere Instanz. Sie finden die Dateien dann auch direkt in Ihrem Dateisystem wieder.

Nextcloud bietet mehrere Varianten:

- 👍 "Text" mit Formatierungsmöglichkeiten einer einfachen Textverarbeitung, ähnlich wie ein Pad [siehe Seite 10].
- 👍 "OnlyOffice", das auch in CryptPad enthalten ist [siehe Seite 10].
- 👍 Und "Collabora Online". Das integriert die Online-Version von LibreOffice.

Nachteil: Sie brauchen halt eine Nextcloud dafür. Alternativen finden Sie auf der nächsten Seite.

Was wir nicht empfehlen: Google-Docs und Microsoft 365 Werfen Sie Ihre sensiblen Daten – zumal im laufenden Arbeitsprozess – nicht den größten Datensammlern der Welt in den Rachen. Zumal Google und Microsoft – genau wie Dropbox übrigens – seine Server im Zweifel auch für eine Durchsuchung durch US-Behörden zur Verfügung stellen muss [Suchwort für Hintergründe dazu: FISA].



GEMEINSAM TEXTE SCHREIBEN

CRYPTPAD

Vorteile: CryptPad verfügt nicht nur über einen Texteditor, sondern unter anderem auch über eine Tabellenkalkulation, Umfragen und ein Whiteboard. Größter Vorteil: Alle Dokumente liegen verschlüsselt auf dem Server – selbst die Admins des jeweiligen CryptPad-Servers können sie nicht einsehen. Bei Bedarf lässt sich ein Account erstellen, mit dem sich Inhalte und sogar ganze Teams verwalten lassen.

Nachteile: Es gibt es keine „sprechenden“ Links, mit denen sich Inhalte eines Dokuments in der URL benennen lassen. Einige Funktionen sind in den Texteditoren nicht so komfortabel und umfassend benutzbar wie z.B. bei Etherpad. Da alle Inhalte im Browser ver- und entschlüsselt werden, belastet CryptPad den eigenen Computer beim Aufruf eines Pads stärker als vergleichbare Lösungen.

Wie Sie CryptPad nutzen können:

Bei freien Instanzen [z. B. bei Digitalcourage: cryptpad.digitalcourage.de oder bei der „Heimatinstanz“ cryptpad.fr. Kundige können CryptPad auch selbst aufsetzen.



ETHERPAD LITE

Vorteile: Wie CryptPad erlaubt Etherpad das gemeinsame Arbeiten, beschränkt sich aber auf Texte. Hierdurch ist es oft einfacher zu nutzen. Farben zeigen, wer was geändert hat, und es gibt eine Versionskontrolle.

Nachteile: Layout, Zeilenabstand, Überschriften-Gestaltung etc. sind nicht so komfortabel wie bei einem Textverarbeitungsprogramm. Zur Formatierung muss der Text, wenn er fertig ist, aus dem Etherpad in ein anderes Programm kopiert oder exportiert und dort bearbeitet werden. Alle Texte liegen unverschlüsselt auf dem Server.


Wie Sie Etherpads nutzen können: Ein eigenes Pad-System aufzusetzen, empfehlen wir auch bei Etherpad nur Technik-Kundigen. Es gibt aber offene Pads, bei denen Sie sich kostenlos eine eigene Unter-Instanz einrichten können. Beachten Sie, dass Sie damit ihre Texte, aber auch die Daten Ihrer Team-Mitglieder [vermutlich Mailadressen und IP-Adressen] diesen Anbietern überlassen – wägen Sie ab, wie groß dieses Risiko ist und wem Sie vertrauen, z.B. pad.systemli.org oder etherpad.wikimedia.org.


VIDEOKONFERENZEN


Eine kurze Überlegung: Brauchen Sie wirklich eine Videokonferenz? Oder ist nicht in vielen Fällen ein Telefonat zu zweit oder mit mehreren Menschen völlig ausreichend [siehe Seite 17ff.]? Videokonferenzen sind für viele quasi ein Reflex – dabei spart Audiotelefonie viel Datenverkehr und damit Strom, wenn Sie nicht unbedingt ein Bild brauchen.

Wenn Sie mehr Informationen zu Videokonferenzen suchen, als diese Broschüre bieten kann, und evtl. sogar selbst einen Server aufsetzen wollen, finden Sie auf digitalcourage.de weitere Informationen [Suchwort „Videokonferenzen“].

WIR EMPFEHLEN

 **Jitsi Meet** Jitsi Meet für Videokonferenzen mit maximal 10 bis 15 Teilnehmenden komfortabel komplett im Webbrowser oder per App auf dem Smartphone. [siehe nächste Seite]

 **BigBlueButton**, ein browserbasiertes Open-Source-Tool für Videokonferenzen und virtuelle Klassenräume [siehe Seite 14]

 **Nextcloud Talk** für Videokonferenzen mit bis zu vier Kontakten [siehe Seite 15]

JITSI MEET

Vorteile: Die Konferenzen sind durch bewährte Verfahren transportverschlüsselt. Die Software ist zu 100 % quell-offen und viele Instanzen bieten eine kostenlose Nutzung.

Nachteile: Je mehr Teilnehmende ihre Kamera aktivieren, desto stärker belastet Jitsi Meet Ihren PC. Daher kann bei mehr als 10 bis 15 Videostreams die Zuverlässigkeit und Qualität je nach Leistung Ihres PCs deutlich nachlassen. Breakout-Rooms für Kleingruppen bietet Jitsi Meet nicht.

Wie Sie Jitsi Meet nutzen können: Es gibt zahlreiche öffentliche Instanzen, die man ohne Anmeldung im Browser benutzen kann. Zwei davon sind meet.osna.social vom Chaostreff Osnabrück e.V. und bitogether.bitel.de der BITel Gesellschaft für Telekommunikation mbH.

UNSER TIPP: Am besten läuft Jitsi Meet in einem aktuellen Mozilla Firefox oder Webbrowser auf der Basis von Chromium. Für Mobilgeräte gibt es passende Apps.



BIGBLUEBUTTON

BigBlueButton eignet sich besonders für Online-Seminare, also wenn Sie einen Bildschirm teilen und damit lehren wollen.

Vorteile: Unter bestimmten Umständen sind auch Gruppen mit sehr vielen Teilnehmer*innen möglich. BigBlueButton hat sinnvolle und erfreuliche Zusatz-Tools wie Handheben, Chat, Whiteboard, Untergruppenräume [sog. Breakout-Rooms] usw.

Nachteile: Bei BigBlueButton sind zwar alle Verbindungen zum Server transportverschlüsselt, d.h. auf dem Weg zum Server kann niemand den Inhalt Ihrer Videostreams einfach so mitlesen, aber auf dem Server selbst sind alle Daten lesbar - und sie werden bei manchen Anbietern 14 Tage lang gespeichert. Das finden wir sehr lang. Sie sollten also Wert auf vertrauenswürdige Serverbetreiber.innen legen. Eine Ende-zu-Ende-Verschlüsselung der Daten findet nicht statt.

Wie Sie BigBlueButton nutzen können: Verwenden sie einen aktuellen Mozilla Firefox oder einen Webbrowser auf Basis von Chromium. Mit senfcall.de steht eine datenschutzfreundliche Instanz zur Verfügung, die ohne Registrierung nutzbar ist.

NEXTCLOUD TALK

Nextcloud Talk eignet sich für Videokonferenzen mit bis zu vier Kontakten.

Vorteil: Wer eine Nextcloud betreibt [siehe Seite 8], kann diese Video-Konferenz in die sowieso genutzten Nextcloud-Tools integrieren.

Nachteil: Bei mehr als vier Videostreams kommt Nextcloud Talk an seine Grenzen. Wer höhere Kapazitäten braucht, kann einen eigenen Signaling-Server hosten oder das kostenpflichtige Backend der Nextcloud GmbH in Anspruch nehmen.

Wie Sie Nextcloud Talk nutzen können: Nur in Verbindung mit einer selbst eingerichteten oder gemieteten Nextcloud.



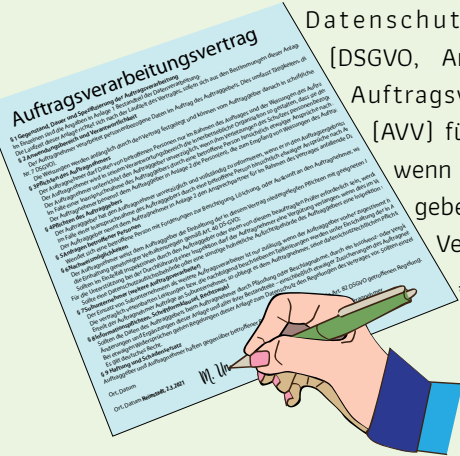
DATENSCHUTZ IN VIDEOCALLS

Wenn Sie Videokonferenzen nutzen, vertrauen Sie Ihre Gesprächs- und Verbindungsdaten dem Betreiber der entsprechenden Plattform an. Dafür brauchen Sie laut

Datenschutzgrundverordnung [DSGVO, Art. 28 Abs. 3] einen Auftragsverarbeitungsvertrag [AVV] für Ihre Daten. Das gilt, wenn Sie für Ihren Arbeitgeber, Ihre Schule, Ihren Verein oder Ihre Firma

„videofonieren“. Nur wenn Sie Videokonferenzen rein privat nutzen, ist kein Vertrag nötig.

Was wir nicht empfehlen: Für US-Dienste wie Zoom, Microsoft Skype oder Teams, Google Meet, Cisco Webex, Discord und wie sie alle heißen, gibt es derzeit kein gültiges Datenschutzabkommen, seit das EU-US-Abkommen „Privacy Shield“ für ungültig erklärt wurde. Schützen Sie Ihre sensiblen Arbeitsdaten vor US-Geheimdiensten und Firmenspionage!



TELEFONKONFERENZEN DREIER-TELEFONKONFERENZ

Mal schnell jemand Drittes mit ins Gespräch zu holen, geht fast immer.

Vorteil: Es genügt ein geeignetes Telefon, das Sie wahrscheinlich sowieso nutzen.



Nachteile: Wenn Sie keine Flat-Rate haben, fallen Gebühren an. Meist können auf diesem Weg höchstens drei Menschen teilnehmen.

Wie Sie eine Dreier-Telefonkonferenz nutzen können:

Eigentlich sollten alle Handys, Smartphones und Büro-Tischtelefone Dreier-Konferenzen können. Da die Systeme sehr unterschiedlich sind, schauen Sie bitte in die Bedienungsanleitung Ihres Gerätes.



KLASSISCHE TELEFONKONFERENZ

Mit mehr als drei Leuten brauchen Sie eine Telefonkonferenz. Die Systeme sind sehr unterschiedlich, hier können wir kaum allgemeingültige Tipps geben. Oft genügt auch hier die bestehende Telefonanlage oder Ihr vorhandener Telefonanbieter – machen Sie sich schlau.

Vorteil: Ein Telefon genügt, um an einer Telefonkonferenz teilzunehmen. Sie können also auch von unterwegs konferieren, und Gäste können problemlos dazukommen.

Nachteile: Wenn Sie keine Flat-Rate haben, fallen Gebühren an. Wenn mehrere Menschen an einem Anschluss gleichzeitig an Konferenzen teilnehmen, belegt jede Person eine Leitung – das kann schnell eng werden.

Wie Sie klassische Telefonkonferenzen nutzen können: Schauen Sie als erstes in die Bedienungsanleitung Ihrer Telefonanlage, wenn Sie eine haben.

Zweiter Schritt: Falls Ihr Telefonanbieter keine Telefonkonferenzen anbietet, gibt es einige Anbieter für Telefonkonferenzen, viele davon auch kostenlos.

Wir können diese leider nicht prüfen und daher keinen Anbieter empfehlen. Immerhin: Anbieter aus Deutschland unterliegen den gleichen Gesetzen wie Anbieter von Telefonanschlüssen – ein gewisses Grundvertrauen können Sie diesen also entgegenbringen.

MUMBLE

Wenn Sie sowieso viel am Rechner arbeiten oder viel mit anderen Ländern telefonieren, können Sie diese Internet-Telefonie benutzen.

Vorteil: Mumble funktioniert auch mit vielen Teilnehmenden – mit Mumble können Sie sogar Großveranstaltungen digital abhalten. Es ist ein offener Standard und die Programme zur Teilnahme sind als freie Software erhältlich. Die Übertragung erfolgt mit sicherer Verschlüsselung zwischen Server und Client [damit ist das Programm des/der Nutzer.in gemeint].

Nachteile: Für Mumble müssen Sie eine eigene Software installieren. Gäste können zwar leicht teilnehmen, benötigen dafür aber auch eine Software auf ihren Geräten.

Wie Sie Mumble nutzen können: Wir empfehlen Ihnen die Websites wiki.freifunk.net/mumble und mumble.info.



KOORDINIEREN UND ABSTIMMEN

TERMINE FINDEN

”Heute schon genuudelt?“ Nuudel heißt das Digitalcourage-Angebot, mit dem Sie ganz einfach und datenschutzfreundlich Termine finden und Abstimmungen organisieren können: [🔗nuudel.de](https://nuudel.de).

Vorteil: Betrieben von Digitalcourage e.V. und garantiert grundrechtewahrend. Nachteile sind uns keine bekannt.

Wie Sie Nuudel nutzen können: Auf [🔗nuudel.de](https://nuudel.de) können Sie wählen, ob Sie eine Terminumfrage oder Ja-Nein-Vielleicht-Umfrage erstellen wollen. Der Rest sollte selbsterklärend sein.

The screenshot shows the nuudel website interface. At the top, the logo 'nuudel' is displayed with the tagline 'nicht speicherndes Termintool'. Below the logo, there is a poll titled 'Umfrage - Heute schon genuudelt?'. The poll content includes the question 'Heute schon genuudelt?' and a 'Speichern' button. The poll is attributed to 'Autor:in der Umfrage: Claudia'. Below the question, there is a table for voting. The table has columns for 'ja', 'Nein', and 'Mach ich noch'. The rows list the names of the voters: Claudia, Katharina, Thorsten, and 'Ihr Name'. The 'ja' column has 3 votes, 'Nein' has 2 votes, and 'Mach ich noch' has 1 vote. A 'Speichern' button is located to the right of the table. Below the table, there is a 'Hinzufügen' button and a '3 Stimmen' indicator. At the bottom of the screenshot, there is a button labeled 'Ergebnisgrafik anzeigen' and the text 'Beste Alternative'.

NEXTCLOUD FORMS

Komplexere Umfragen mit mehreren Fragen, Einfach- oder Mehrfachauswahl, Freitext, etc. erstellen Sie in Ihrer Nextcloud [siehe Seite 8]. Die Antworten werden grafisch aufbereitet und Sie können sie einfach als Tabelle herunterladen. War Nextcloud Forms anfangs nur ein Aschenputtel, ist es inzwischen eine stolze Prinzessin.

Vorteil: Wenn Sie eine eigene Nextcloud selbst betreiben, bleiben alle Antworten auf Ihrem Server.

Nachteil: Alle Fragen erscheinen auf einer Seite, wodurch lange Umfragen genau das werden: lang.

Wie Sie Nextcloud Forms nutzen können: Nur innerhalb einer Nextcloud, in der die App „Forms“ installiert ist.



Seit dem Frühsommer 2021 können Formblätter und einfache Umfragen über den Dienst „Foorms“ von Digitalcourage erstellt werden. [🔗digitalcourage.de/foorms](https://digitalcourage.de/foorms).

CRYPTPAD-UMFRAGE

Vorteil: Wenn Sie CryptPad benutzen, brauchen Sie kein weiteres Tool. [siehe Seite 10]


Nachteil: Es kann nur Ja-Nein-Enthaltung-Fragen und ist nicht sonderlich hübsch.

Wie Sie CryptPad Umfrage nutzen: Klicken Sie auf der Startseite eines CryptPads oder in Ihrem „CryptDrive“ nach dem „+“ für „Neues Pad“ in der Auswahl auf „Umfrage“.



Was wir nicht empfehlen:

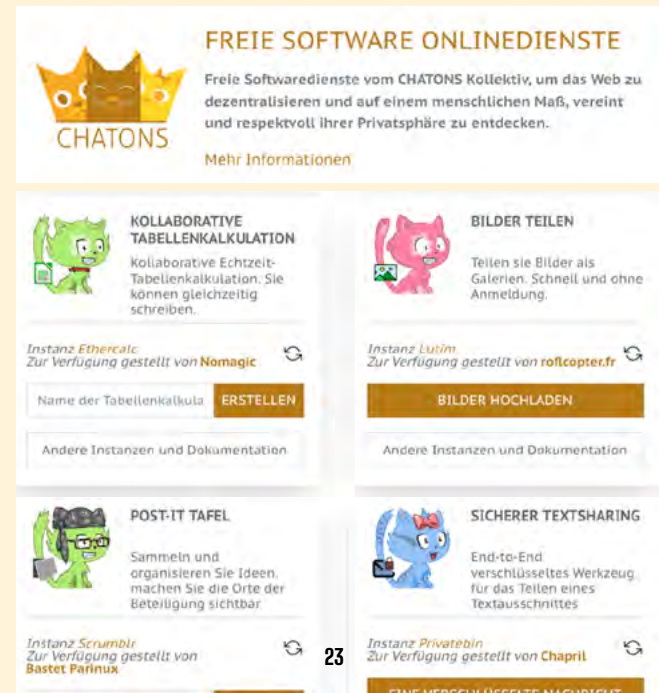
 Doodle, denn die Website enthält nach unserer Untersuchung mindestens 11 Tracker. [Stand März 2021]

 Google Forms, denn es kommt ja von der Datenkrake Google.

POST-IT-TAFELN, BILDER TEILEN, TEXT-SCHNIPSEL TEILEN

Es gibt noch eine Unmenge weiterer, spezialisierter Online-dienste. Beispielsweise, um ein Brainstorming mit Karteikarten auf einer Tafel zu machen und in ein einfaches Kanban umzuwandeln. Oder um Bilder oder Text-Schnipsel zu teilen, die nach einiger Zeit wieder gelöscht werden.

Eine schöne Sammlung solcher Onlinedienste haben die „Chatons“ zusammengestellt: entraide.chatons.org/de.



The screenshot shows the Chatons website interface. At the top, there is a logo for Chatons (a crown with eyes) and the text "FREIE SOFTWARE ONLINEDIENSTE". Below this, a paragraph describes the mission: "Freie Softwaredienste vom CHATONS Kollektiv, um das Web zu dezentralisieren und auf einem menschlichen Maß, vereint und respektvoll ihrer Privatsphäre zu entdecken." A link for "Mehr Informationen" is provided.

The main content area is divided into four service cards:

- KOLLABORATIVE TABELLENKALKULATION:** Features a green cat icon. Description: "Kollaborative Echtzeit-Tabellenkalkulation: Sie können gleichzeitig schreiben." It lists the instance "Etherecalc" by Nomaig and has an "ERSTELLEN" button.
- BILDER TEILEN:** Features a pink cat icon. Description: "Teilen Sie Bilder als Galerien. Schnell und ohne Anmeldung." It lists the instance "Lutim" by rofcopter.fr and has a "BILDER HOCHLADEN" button.
- POST-IT TAFEL:** Features a green cat icon with glasses. Description: "Sammeln und organisieren Sie Ideen, machen Sie die Orte der Beteiligung sichtbar." It lists the instance "Scrumbl" by Bastet Parinux.
- SICHERER TEXTSHARING:** Features a blue cat icon. Description: "End-to-End verschlüsseltes Werkzeug für das Teilen eines Textausschnittes." It lists the instance "Privatebin" by Chapril.

Each card includes a link to "Andere Instanzen und Dokumentation".

INSTANT MESSENGER

Viele wissen, dass es keine gute Idee ist, WhatsApp zu benutzen, denn WhatsApp wurde von Facebook aufgekauft. Andere Messenger [z. B. Telegram] sind noch bedenklicher.

Unser Wunschzettel für Messenger und Chat-Programme:

- ▶ **Offene Schnittstellen:** Das Kommunikationsprotokoll („wie kommt eine Nachricht von A nach B“) soll dokumentiert und öffentlich verfügbar sein. Wie bei E-Mails sollte die Kommunikation zwischen verschiedenen Anbietern funktionieren.
- ▶ **Freie Software:** Der Quellcode der Software soll verfügbar und unter einer freien Lizenz sein – sowohl bei App als auch Server-Software.
- ▶ **Ende-zu-Ende-Verschlüsselung:** Wenn Sie eine Nachricht senden, sollte diese auf Ihrem Gerät verschlüsselt und erst bei den Empfangenden wieder entschlüsselt werden.
- ▶ **Sicherheit [Kryptografie]:** Apps sollten nach aktuellem Stand sichere, nachvollziehbare Kryptografie verwenden.
- ▶ **Unabhängiges Audit:** Unabhängige Dritte sollten die Software regelmäßig auf Sicherheitslücken prüfen.
- ▶ **Betriebssysteme:** Wir möchten mindestens Android und iOS [iPhone/iPad] unterstützt sehen, da diese über 90% des Marktes ausmachen. Mehr Betriebssysteme wären wünschenswert.

- ▶ **Wenig Metadaten:** Unnötige Zugriffe auf Drittanbieter [z. B. zum Nachladen von Bildern, Schriftarten, CSS-Stilen oder Javascript-Bibliotheken] sollten vermieden werden. Dezentrale Dienste mit verschiedenen Instanzen erschweren die zentrale Sammlung von Metadaten.
- ▶ **Kein Adressbuch-Upload:** Die meisten Messaging-Apps benutzen Handy-Nummern zur Identifikation und bieten eine automatische Erkennung von Ihren Kontakten. Das ist ein Eingriff in Ihre Privatsphäre und die Ihrer Kontakte und darf nur mit expliziter Zustimmung erfolgen.
- ▶ **Nicknames:** Gelegentlich möchte man mit Leuten chatten, denen man keine Handynummer geben möchte. Es ist wünschenswert, sich über selbstgewählte Nicknames statt über die Telefonnummer zu verbinden.
- ▶ **Freie Verfügbarkeit:** Unter Android sollte der Messenger auch außerhalb des Google Play Store angeboten werden, so dass die App auch ohne Google-Account nutzbar ist. Das geht direkt oder per F-Droid, einem alternativen „Store“, in dem ausschließlich freie und quelloffene Software angeboten wird.
- ▶ **Kein Tracking:** Gerade Apps, die private Kommunikation versprechen, sollten keine Nutzungsdaten sammeln und übertragen.
- ▶ **Reproduzierbarkeit/„Reproducible Builds“:** S. Seite 5

Nicht vergessen:

Den perfekten Messenger gibt es nicht!

DATEN TEILEN UND AUSTAUSCHEN


Man kann zwischen zwei Arten, Dateien online zu teilen, unterscheiden. Zum einen in einer dauerhaften gemeinsamen Dateiablage mit Verzeichnisstruktur. Das ist die Kernfunktion einer Nextcloud [siehe Seite 8].

Wenn Sie keine Nextcloud haben und eine Datei verschieken wollen, die zu groß für einen E-Mail-Anhang ist, was tun Sie dann? Dafür gibt es Dienste, die eine zeitlich befristete Ablage von einzelnen Dateien ermöglichen. Diese lassen sich bequem als Downloadlink per E-Mail oder Messenger teilen.

MIT EINEM WEBBROWSER

Firefox bietet einen eigenen Datei-Austausch an. Eine unabhängige Firefox-Send-Instanz ist zum Beispiel:

 drop.chapril.org

Lufi ist ebenfalls ein Datei-Hosting-Server, der Ihre Daten verschlüsselt lagert und überträgt. Eine unabhängige Lufi-Instanz ist  drop.infini.fr





MIT THUNDERBIRD: PLIK STATT WETRANSFER

Thunderbird [ein E-Mail-Programm] fügt in Ihre Mail einen Link ein, wo sich jemand den Anhang herunterladen kann. Wir raten, dass sie Thunderbird so einrichten, dass dafür

der trackerfreie Dienst Plik genutzt wird statt das voreingestellte WeTransfer:

Im „Hamburger-Menü“ ☰ → Einstellungen → Verfassen → nach unten scrollen bis „Anhänge“ → weitere Anbieter finden → bei „FileLink für Plik“ auf [+ zu Thunderbird hinzufügen] klicken → Tab schließen → in den Einstellungen unter „Anhänge“ auf „Plik hinzufügen“ klicken und [Speichern] klicken. [Sollte der Speichern-Knopf ausgegraut ein: zweimal auf das Kästchen „Uploads nach dem ersten Download löschen“ klicken und speichern.]

Wenn das einmal eingerichtet ist, kann man beim Schreiben von E-Mails Anhänge über Plik teilen, indem man neben  Anhang auf das  klickt und Filelink → Plik auswählt.

ANONYM VIA TOR

Onionshare ist ein komfortables kleines Programm, das einen Onion-Dienst im Tor-Netz einrichtet, um Dateien bereitzustellen. Diese lassen sich dann per Tor Browser abrufen. Onionshare ist einfach zu installieren. Wer das spurenarmer Betriebssystem Tails benutzt, hat Onionshare schon dabei.

Tipp: Tor, Onion oder Tails sind wichtige Begriffe zum Sicheren Surfen im Internet. Falls Sie sich damit noch nicht auskennen, sind das gute Suchworte für eine Suchmaschine Ihrer Wahl.



DATEN UND E-MAILS VERSCHLÜSSELN

E-MAILS VERSCHLÜSSELN

Firmengeheimnisse und Kundendaten per Mail zu verschicken ist eine heikle Sache – geht aber manchmal nicht anders, wenn man im Homeoffice sitzt. Am besten wäre natürlich, wenn wir alle nur noch verschlüsselte E-Mails verschicken würden. Das ist leider immer noch nicht ganz so einfach. Wir empfehlen es trotzdem, weil der Aufwand sich lohnt.

Wenn Sie keine von der Firma gesicherte Mailadresse haben, sollten Sie als erstes Anbieter wie [web.de](#), [gmail.com](#) oder [yahoo.de](#) verlassen und zu sicheren Anbietern wie [posteo.de](#) oder [mailbox.org](#) wechseln. Dann ist schon viel Verschlüsselung inklusive. Mehr tun können Sie, wenn Sie PGP nutzen. [digitalcourage.de/pgp](#)

DATEN VERSCHLÜSSELN MIT VERACRYPT

Wer Daten vom Arbeits-PC auf den Privatrechner zieht, sollte bedenken, dass diese besonders geschützt werden müssen. Noch einmal mehr, wenn es sich um personen-beziehbare Daten von Kund:innen, Schüler:innen oder Klient:innen handelt. Legen Sie solche Daten am besten in einen VeraCrypt-Container. VeraCrypt ist relativ schnell zu erlernen und sehr flexibel, da es auf allen Plattformen und Datenträgern funktioniert. Sie können also auch Ihre

Sticks damit verschlüsseln, ganze Festplatten oder nur einfache Dateien oder Verzeichnisse.

PRIVACY CAPTCHA

Um kurze sensible Informationen wie eine Adresse oder eine Telefonnummer, die Sie per Mail verschicken müssen, wenigstens ein bisschen zu schützen, gibt es unsere Website [privacy-captcha.net](#).

Der Trick: Sie schreiben die Daten in ein Feld, und sie werden in eine Bild-Datei umgewandelt. Diese lässt sich dann nicht mehr so einfach wie ein Mail-Text automatisch mitlesen oder durchsuchen. Probieren Sie es einfach mal aus – es ist wirklich ganz einfach und es wirkt.





Wer hat dieses kurz&mündig-Heft erstellt?

▶ **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 BigBrother-Awards. Digitalcourage ist gemeinnützig, finanziert sich durch Spenden und lebt von viel freiwilliger Arbeit.

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

▶ Maintainer:innen dieser Broschüre: Sarah Bollmann, Hartmut Goebel, Christian Pietsch und das Team der AG Digitale Selbstverteidigung

Wer steckt hinter der AG "Digitale Selbstverteidigung"?

Die Mitglieder dieser AG kennen sich technisch gut aus, sie haben ihre Augen und Ohren überall, wo neue Entwicklungen präsentiert werden, und bohren nach, welche Einflüsse auf Privatsphäre und Überwachungsthemen im Anmarsch sind. Sie testen, probieren,

Dieses KURZ&MÜNDIG-Minibuch ist auch als komfortables interaktives PDF erhältlich. Es kostet nur 5,00 Euro und ist wie alle KURZ&MÜNDIG-Ausgaben [auch als Printversion] erhältlich unter: digitalcourage.de/kum

zweifeln und diskutieren im Team, welche Konsequenzen eine neue Entwicklung hat. Ihre Erkenntnisse geben sie in Texten oder bei Cryptoparties weiter.

Sie möchten mit uns tüfteln? Unser Team kann kundige – insbesondere weibliche – Verstärkung gebrauchen. Melden Sie sich gern!

Hinweis: Hundertprozentige Sicherheit gibt es nicht, auch nicht durch unsere Empfehlungen. Programme können unentdeckte Fehler haben, und Datenschnüffel-techniken entwickeln sich weiter. Bleiben Sie wachsam!



In der KURZ&MÜNDIG-Reihe sind bisher erschienen:

- | | |
|---|--|
| 01 Digitale Mündigkeit | 14 Überwachung in China |
| 02 Datenschutzrechte in Schulen durchsetzen | 15 Solidarität im Netz |
| 03 Faire Websites | 16 Fediverse. So geht Social Media |
| 04 Leitlinien für digitale Bildung in Schulen | 17 Einfach. Linux. |
| 05 Uploadfilter | 18 Smart Toys und Kinder-Tracking-Apps |
| 06 Stalking, Hass, Kontrolle | 19 Datenschutzbeschwerden richtig einreichen |
| 07 Homeoffice | 20 Datenschutz in Kirchengemeinden |
| 08 Digitale Bildungsangebote selbst erstellen | 21 Videoüberwachung an Schulen |
| 09 Digitale Angiffe im Büro | 22 Digitale Selbstverteidigung für Mädchen* |
| 10 Digitale Sicherheit für Frauenhäuser | 23 Workshops clever planen |
| 11 Versammlungsfreiheit | 24 Bodyshaming |
| 12 Nichts zu verbergen? | 25 Umgang mit Fotos |
| 13 Apps selbst prüfen und bewerten | 26 Künstliche Intelligenz |

HOMEOFFICE

Firmengeheimnisse wahren, Kundendaten schützen, Videokonferenzen starten, gemeinsam Verzeichnisse verwalten oder Texte schreiben – digitale Arbeit zu Hause wirft eine Menge Fragen auf.

Wir empfehlen Ihnen gute Alternativen zu den großen kommerziellen Diensten, alle mit hohen Datenschutzstandards und als freie Software-Angebote.

**GEBEN SIE FREIHEIT UND SICHERHEIT
NICHT AN DER GARDEROBE AB!
AUCH NICHT IM HOMEOFFICE.**

Digitalcourage e.V.

Marktstraße 18 | 33602 Bielefeld

mail@digitalcourage.de | digitalcourage.de

T: +49 521 1639 1639



9 783934 636354 >

5,00 Euro
4,00 SFR

ISBN 978-3934636-35-4

 **digitalcourage**

k&m007 Homeoffice