Infrastruktur

Eine (sorgfältig) zusammengestellte Auswahl an Diensten, die für unterschiedliche Anforderungen konzipiert sind. Von der Absicherung von Verbindungen in öffentlichen WLAN-Netzen bis hin zur Datenspeicherung und der Verwaltung von E-Mails. Ich habe eine Sammlung von Tools zusammengestellt, auf die ich sowohl privat als auch geschäftlich unterwegs zurückgreife.

Internet

Das Internet ist aus der heutigen Welt nicht mehr wegzudenken. Ohne Internet wären alltägliche Aufgaben wie Online-Banking, Geldüberweisungen, das Abrufen von Fahrplänen des öffentlichen Nahverkehrs, der Kauf von Tickets, die Überprüfung von Öffnungszeiten oder der Kontakt zu Familie und Freunden auf der ganzen Welt nur schwer möglich.

Selbst leichtere Aktivitäten, etwa das Konsumieren von Memes in sozialen Medien, sind auf einen Internetzugang angewiesen.

Um online zu bleiben, benötigt man in der Regel eine Mobilfunk-, WLAN- oder Festnetzverbindung.

Für zusätzliche Sicherheit und Flexibilität nutze ich bei den meisten Online-Aktivitäten NetBird, Tailscale oder Mullvad VPN.

Diese Lösungen bieten sichere Ende-zu-Ende-Verschlüsselung, vereinfachen den Zugriff auf private Netzwerke über Geräte hinweg, schützen die Privatsphäre in unsicheren Netzwerken und ermöglichen eine zuverlässige, ortsunabhängige Verbindung ohne komplexe Konfiguration.

SIM-Karten

Der Kauf einer SIM-Karte am aktuellen Aufenthaltsort ist in der Regel unkompliziert. Die meisten Läden und Shops bieten Prepaid-Optionen an, die den grundlegenden Datenbedarf für alltägliche Aufgaben abdecken.

Innerhalb der EU ist der Kauf einer SIM-Karte besonders komfortabel. Man kann problemlos eine SIM-Karte in einem günstigeren EU-Land erwerben und sie anschließend in der gesamten Region nutzen. Dank EU-weiter Regulierung ist Roaming innerhalb der Mitgliedsstaaten kostenfrei, sodass bei der Nutzung in teureren EU-Ländern keine zusätzlichen Gebühren anfallen.

- WiFi Map eSIM
- WorldSIM
- GigSky
- GoSIM
- Keepgo
- OneSimCard
- TravelSIM

Die meisten dieser SIM-Karten sind im Verhältnis zu ihrer Leistung relativ teuer. In etwa 99 % der Fälle ist man mit einer lokal gekauften SIM-Karte günstiger unterwegs und profitiert gleichzeitig von besserem Datenschutz.

Alternativ gibt es Online-Dienste, die den Aufwand vermeiden, vor Ort Geschäfte zu finden, die SIM-Karten ohne Know-Your-Customer-(KYC-)Anforderungen verkaufen. Je nach Land sowie benötigtem Daten- oder Telefonieumfang können diese Angebote jedoch kostenintensiv sein. Ein Beispiel hierfür ist silent.link.

Wer lediglich eine anonyme virtuelle Telefonnummer für Anrufe und SMS benötigt, kann einen Blick auf JMP, Crypton oder Hushed werfen, die keine KYC-Verifizierung erfordern.

WiFi

Kostenloses WLAN lässt sich über verschiedene Online-Ressourcen finden. Beispielsweise bietet WiFi Map Apps für iOS und Android an, die öffentlich zugängliche WLAN-Zugangspunkte übersichtlich auf einer Karte darstellen.

VPN

Ich nutze VPNs für einen Großteil meiner Online-Aktivitäten. Ein VPN ist dabei nur **eine von mehreren Maßnahmen**, um es der unternehmerischen Überwachung (Amazon, Facebook, Google, Twitter usw.) schwieriger zu machen.

Ein VPN kann außerdem hilfreich sein, wenn man Linux-ISOs über BitTorrent herunterlädt. Dabei sollte man sich jedoch bewusst sein, dass VPNs keine Allheilmittel für Privatsphäre sind und keinesfalls vor staatlicher Überwachung schützen.

Ich habe eine Zeit lang versucht, eine eigene VPN-Infrastruktur auf Basis von WireGuard zu betreiben. Die Idee war, ein kleines, selbstverwaltetes Setup zu haben, das mir volle Kontrolle über Konfiguration, Standorte und Zugangsmodelle gibt.

In der Praxis stellte sich jedoch heraus, dass der laufende Aufwand zu hoch war. Wartung, Updates, Monitoring, der regelmäßige Austausch von Servern sowie die Absicherung der gesamten Infrastruktur haben deutlich mehr Zeit und Aufmerksamkeit erfordert, als es für meinen Anwendungsfall sinnvoll war. Aus diesem Grund habe ich das Vorhaben schließlich aufgegeben und setze heute überwiegend auf kommerzielle VPN-Anbieter.

> **Hinweis:** Je weniger Nutzer ein VPN hat, desto einfacher wird es für andere Teilnehmer, einzelne Nutzer anhand von Nutzungsmustern zu identifizieren. Ein eigenes VPN zu betreiben ergibt nur für spezielle Zwecke Sinn, etwa zum Aufbau eines echten privaten Netzwerks für Datenaustausch oder sichere Kommunikation zwischen bekannten Parteien.
>
> Wenn es hingegen primär darum geht, zu verhindern, dass YouTube ein Schattenprofil über die eigene Vorliebe für Telenovelas erstellt, ist man mit

> einem kommerziellen VPN besser beraten – vorausgesetzt, der eingesetzte Browser ist möglichst resistent gegen Fingerprinting.

Für kommerzielle VPN-Dienste empfehle ich Anbieter zu wählen, die Barzahlung oder Monero (XMR) für eine bessere Anonymität akzeptieren. Hier sind einige Optionen:

- Mullvad VPN (Schweden; Hinweis: gewisse Vorsicht empfohlen. Akzeptiert Bitcoin (XBT) und Bargeld, zudem sind physische Geschenkkarten über Amazon erhältlich)
- NordVPN (Panama; akzeptiert Kryptowährungen)

Als allgemeine Faustregel gilt, den Einsatz von VPNs an die jeweilige Aufgabe und an die Art der zu übertragenden Inhalte anzupassen.

Dabei sollte man stets im Hinterkopf behalten, dass VPN-Anbieter – auch wenn sie eine No-Log-Policy versprechen – zu jedem Zeitpunkt die Quell-IP sehen können, von der aus die Verbindung aufgebaut wird.

Reisehinweis:

Die Nutzung von Tor und VPNs ist in vielen Ländern verboten, stark eingeschränkt oder an bestimmte Auflagen gebunden. Vor Reisen sollte man sich daher immer mit der lokalen Rechtslage und der tatsächlichen Durchsetzungspraxis vertraut machen.

In einigen Ländern sind VPNs und Anonymisierungsdienste weitgehend oder vollständig untersagt: In **Belarus**, **Nordkorea** und **Turkmenistan** sind VPNs faktisch verboten und ihre Nutzung kann zu ernsthaften Konsequenzen führen. In **Myanmar** ist die Verwendung nicht genehmigter VPNs strafbar.

Andere Staaten erlauben VPNs nur eingeschränkt oder ausschließlich in staatlich genehmigter Form: In **China** und **Russland** sind nur offiziell zugelassene VPN-Dienste erlaubt, während unabhängige Anbieter systematisch blockiert werden. In **Iran** und **Oman** ist die private Nutzung ohne behördliche Genehmigung illegal. In der **Türkei** werden VPNs regelmäßig blockiert, insbesondere während politischer Krisen oder sicherheitsrelevanter Ereignisse. In den **Vereinigten Arabischen Emiraten** ist VPN-Nutzung grundsätzlich erlaubt, kann jedoch strafbar sein, wenn sie zur Umgehung gesetzlicher Beschränkungen eingesetzt wird.

In weiteren Ländern existiert kein ausdrückliches Verbot, die Nutzung ist jedoch situationsabhängig oder riskant: In **Uganda** wurden VPNs zeitweise blockiert, ein generelles Verbot besteht jedoch nicht. In **Ägypten** sind VPNs formal legal, die Umgehung von Zensurmaßnahmen kann jedoch Sanktionen nach sich ziehen.

Dies bedeutet **nicht**, dass Tor oder VPNs grundsätzlich vermieden werden sollten. Vielmehr geht es darum, sich der rechtlichen Rahmenbedingungen bewusst zu sein und diese Werkzeuge informiert, situationsangepasst und verantwortungsvoll einzusetzen, um unnötige Risiken zu vermeiden.

Firewall

Auf meinem Windows PC Workstation sind standardmäßig alle Ports gesperrt und ausgehende Verbindungen müssen explizit erlaubt werden.

Für Linux-Desktops ist OpenSnitch generell einen Blick wert.

Unter macOS erfüllt Little Snitch im Alert-Modus seinen Zweck. Der kleine Bruder Little Snitch Mini ist eine gute Alternative für Nutzer, die keine detaillierte Kontrolle benötigen, aber dennoch ausgehende Verbindungen überwachen möchten. Dazu bieten die Blocklisten eine sinnvolle Ergänzung.

Allerdings scheinen Apples eigene Dienste Firewall-Regeln oder VPNs nicht immer zuverlässig zu respektieren. Daher ist es sinnvoll, die Kommunikation zusätzlich über eine dedizierte Firewall (z. B. auf Router-Ebene) zu unterb inden.

Browsing

Für mein tägliches Surfen im Internet nutze ich hauptsächlich Firefox mit einer Auswahl an Erweiterungen. Zusätzlich verwende ich ungoogled Chromium sowie Safari.

Safari setze ich vor allem für Homelab-Themen und für alles ein, was im Zusammenhang mit Apple-Diensten steht.

In Firefox verwende ich die folgenden Erweiterungen:

- uBlock Origin
- Decentraleyes

- ClearURLs
- Bitwarden Password Manager
- Surfingkeys
- LibRedirect
- Cookie AutoDelete
- User-Agent Switcher
- Firefox Translations (for cloud-free, in-browser translations of websites)

In Ungoogled Chromium verwende ich die folgenden Erweiterungen:

- uBlock Origin
- Decentraleyes
- ClearURLs
- Bitwarden Password Manager
- Surfingkeys
- LibRedirect
- Chromium Web Store

Ich halte JavaScript standardmäßig deaktiviert (über uBlock) und aktiviere es nur für mir bekannte und vertrauenswürdige Websites.

Natürlich existiert neben der JavaScript-Engine weitere Angriffsfläche. Durch die konsequente Reduzierung dieser Oberfläche wird das Kosten-/Nutzen-Verhältnis für Angriffe jedoch so unattraktiv, dass sich das theoretische Risiko in der Praxis möglicherweise nie realisiert.

Beachte, dass Browser-Erweiterungen deinen Browser eindeutiger identifizierbar machen können (Browser-Fingerprinting).

Teste regelmäßig den Fingerprint deines Browsers, um sicherzustellen, dass er nicht zu stark aus der Masse heraussticht. Werkzeuge wie Cover Your Tracks und Am I Unique helfen dabei, die Einzigartigkeit des eigenen Browsers einzuschätzen.

Zusätzlich dazu verwende ich in `about:config` bzw. in meiner `user.js` die folgenden Einstellungen für Firefox:

```
accessibility.typeaheadfind.flashBar = 0
app.shield.optoutstudies.enabled = false
beacon.enabled = false
browser.contentblocking.category = strict
browser.safebrowsing.downloads.remote.enabled = false
browser.safebrowsing.malware.enabled = false
browser.safebrowsing.phishing.enabled = false
browser.send_pings = false
browser.sessionstore.privacy_level = 2
browser.urlbar.speculativeConnect.enabled = false
browser.newtabpage.activity-stream.feeds.telemetry = false
browser.ping-centre.telemetry = false
browser.tabs.crashReporting.sendReport = false
browser.newtabpage.activity-stream.section.highlights.includePocket =
false
services.sync.prefs.sync.browser.newtabpage.activity-
stream.section.highlights.includePocket = false
extensions.pocket.enabled = false
toolkit.telemetry.enabled = false
toolkit.telemetry.server = ""
toolkit.telemetry.unified = false
datareporting.healthreport.uploadEnabled = false
media.gmp-widevinecdm.enabled = false
media.navigator.enabled = false
network.cookie.cookieBehavior = 5
network.dns.disablePrefetch = true
network.dns.disablePrefetchFromHTTPS = true
network.http.referer.XOriginPolicy = 2
network.http.referer.XOriginTrimmingPolicy = 2
network.http.sendRefererHeader = 0
network.IDN_show_punycode = true
network.predictor.enable-prefetch = false
network.predictor.enabled = false
network.prefetch-next = false
privacy.donottrackheader.enabled = true
privacy.firstparty.isolate = true
privacy.resistFingerprinting = true
privacy.resistFingerprinting.letterboxing = true
privacy.trackingprotection.cryptomining.enabled = true
privacy.trackingprotection.enabled = true
privacy.trackingprotection.fingerprinting.enabled = true
privacy.trackingprotection.socialtracking.enabled = true
webgl.disabled = true
pdfjs.enableScripting = false
security.ssl3.rsa_des_ede3_sha = false
security.ssl.require_safe_negotiation = true
geo.enabled = false
```

Auch wenn manche Firefox, Safari oder Chrome nicht mehr mögen, halte ich es weiterhin für sinnvoll, mehrere unterschiedliche Browser installiert zu haben – und zwar aus mehreren Gründen:

- **Getrennte Anwendungsfälle:** Unterschiedliche Browser für unterschiedliche Aufgaben zu nutzen – etwa einen für die Arbeit und einen anderen für private Zwecke – sorgt für bessere Struktur und reduziert Ablenkungen. Ebenso lassen sich sensible Bereiche wie Banking, Gaming oder Homelab-Themen sauber trennen.

- **Mehr Privatsphäre und Sicherheit:** Jeder Browser bringt eigene Datenschutz- und Sicherheitsmechanismen mit. Ungoogled Chromium minimiert Datensammlung, während Firefox über einen starken Tracking-Schutz verfügt. Die Nutzung mehrerer Browser erschwert Cross-Site-Tracking und erhöht die Trennung von Aktivitäten.

- **Unterschiedliche Stärken:** Jeder Browser hat seine eigenen Vorteile. Safari integriert sich nahtlos in das Apple-Ökosystem, Firefox bietet umfangreiche Anpassungsmöglichkeiten, und Ungoogled Chromium ist eine datenschutzfreundlichere Variante von Chrome.

- **Bessere Kompatibilität und Performance:** Manche Websites funktionieren in bestimmten Browsern zuverlässiger oder performanter. Mehrere installierte Browser stellen sicher, dass Inhalte unabhängig von Website oder Anwendung problemlos genutzt werden können.

Search Engines

Die folgenden Suchmaschinen werden von mir am meisten verwendet:

- SearXNG
- ~~Leta~~ (shutdown in Nov 2025)
- DuckDuckGo
- Brave

Möglicherweise werde ich wechseln, da DuckDuckGo angekündigt hat, Suchergebnisse zu zensieren – unter dem Vorwand, Nutzer vor Desinformation zu schützen.

Da ich aktiv weder Google noch Bing verwende, kann ich die folgenden Suchmaschinen empfehlen: Startpage, Qwant und Searx.

Maps

Für Adresssuchen und Navigation nutze ich überwiegend Apple Maps. Aber auch OpenStreetMap. Ich versuche aber, mehr und mehr Organic Maps und OsmAnd zu nutzen.

Wann immer möglich, versuche ich zudem GoMap! zu nutzen und empfehle ausdrücklich, dies ebenfalls zu tun. Wer mit Android unterwegs ist, dem empfehle ich ausserdem StreetComplete und NeoStumbler.

Kommunikation

Kommunikation macht einen großen Teil meines digitalen Lebens aus. Um mit Familie, Freunden und geschäftlichen Kontakten in Verbindung zu bleiben, nutze ich eine Vielzahl and Messenger, Videokonferenz-Tools, sozialen Netzwerken und weiteren Platformen.

E-Mail

Für E-Mail nutze ich hauptsächlich iCloud Mail mit einem kostenpflichtigen Account. Dieser ermöglicht es mir, eigene Domains einzubinden sowie Ad-hoc-Adressen nach Bedarf zu generieren.

Die Möglichkeit, für unterschiedliche Zwecke separate E-Mail-Adressen zu verwenden, hilft dabei, Kommunikation sauber zu trennen und die Weitergabe einer primären Adresse zu vermeiden. Gleichzeitig profitiere ich von der stabilen Zustellbarkeit und der guten Server-Reputation, die insbesondere im geschäftlichen Umfeldentscheidend ist.

Auch wenn iCloud Mail kein spezialisierter „Privacy-Mail“-Dienst ist, bietet es für meinen Anwendungsfall einen praktikablen Kompromiss aus Zuverlässigkeit, Integration ins Apple-Ökosystem und ausreichend Kontrolle über Domains und Adressverwaltung.

Vorsicht ist auch bei privaten E-Mail-Anbietern wie ProtonMail geboten, da sie Nutzer stark an ihre Plattform binden und einen späteren Wechsel erschweren – selbst dann, wenn dieser nicht freiwillig erfolgt.

Wer nach Alternativen sucht, findet hier eine nicht abschließende Liste möglicherweise interessanter Dienste. Für zusätzliche Anonymität empfiehlt sich die Nutzung über Tor.

- Mailbox.org
- Posteo
- Migadu
- Kolab Now
- Fastmail
- Mailfence
- StartMail
- Runbox
- Swisscows Mail
- OnionMail
- Disroot Mail

Messaging

Direkte und kleine Gruppenkommunikation

Ich nutze weiterhin **Messages** (ehemals iMessage) aber verstärkt mehr und mehr Signal, auch wenn ich beide Dienste inzwischen deutlich kritischer sehe als noch vor einigen Jahren. Apple schwächt den ohnehin begrenzten Datenschutz von Messages schrittweise weiter, und auch Signal ist trotz seiner technischen Stärken ein zentralisierter Dienst, der ein gewisses Maß an Vertrauen erfordert.

In der Praxis überwiegen jedoch pragmatische Gründe. Beide Messenger sind weit verbreitet, zuverlässig und tief im Alltag von Familie, Freunden und beruflichen Kontakten verankert. Auf **WhatsApp vollständig zu verzichten ist realistisch kaum möglich**, ohne soziale Beziehungen unnötig zu belasten oder ganz zu verlieren. So sehr mich das frustriert: **soziale Kontakte sind am Ende wichtiger als eine technisch saubere, aber isolierte Lösung.**

Positiv hervorzuheben ist, dass Signal inzwischen **Benutzernamen** eingeführt hat, sodass Gespräche auch ohne Weitergabe der eigenen Telefonnummer möglich sind (Ankündigung von Signal). Das ist eine sinnvolle Verbesserung, ändert jedoch nichts daran, dass Signal ein zentral betriebener Dienst bleibt.

Langfristig würde ich Messenger wie **Threema** oder **XMPP (Jabber)** bevorzugen, da sie ohne Telefonnummer auskommen und aus Datenschutzsicht robuster aufgestellt sind. In der Realität scheitert dies jedoch meist an fehlender Akzeptanz. Viele Menschen sind nicht bereit, für einen

Messenger zu bezahlen oder sich mit Alternativen auseinanderzusetzen. Versuche, das eigene Umfeld davon zu überzeugen, enden oft mit Unverständnis – oder mit der bekannten Frage, **warum man „immer alles anders machen muss“.**

Derzeit bleibt daher ein bewusster Kompromiss: **Ich nutze etablierte Messenger weiter, kenne ihre Einschränkungen und ziehe dort klare Grenzen, wo es möglich ist.** Parallel versuche ich, datenschutzfreundlichere Alternativen zu fördern und selbst zu nutzen, ohne dabei soziale Beziehungen aufs Spiel zu setzen.

Einen guten Überblick über viele Messenger bietet der **Kuketz-Blog – Messenger-Übersicht.**

Community- und Gruppenkommunikation

Früher habe ich viel Zeit im **IRC** verbracht. Über Jahre hinweg war es der Ort für offene, themengetriebene Diskussionen und spontane Gespräche. Nach dem Zusammenbruch von **Freenode** fiel es mir jedoch schwer, auf **Libera Chat** oder anderen Nachfolgenetzwerken wieder Anschluss zu finden. Zusätzlich empfand ich Teile der dortigen Moderations- und Betreiberkultur als problematisch, insbesondere im Umgang mit Fehlverhalten innerhalb des Netzwerks.

Auch mit Matrix habe ich mich eine Zeit lang intensiver beschäftigt, unter anderem mit Element. Das Netzwerk hat konzeptionell großes Potenzial, leidet jedoch aus meiner Sicht nach wie vor unter technischer Unzuverlässigkeit, schwacher Benutzererfahrung und teils sehr schlechter Performance. Viele Räume sind klein, abgeschottet oder inaktiv, wodurch **echte, lebendige Diskussionen selten geworden sind.**

XMPP möchte ich perspektivisch stärker nutzen, etwa mit **Conversations** auf dem Smartphone und **Profanity** am Rechner. Aktuell fehlt mir jedoch meist die Zeit, mich dort regelmäßig und aktiv einzubringen.

Inzwischen verbringe ich einen Großteil meiner Zeit auf **Discord**. Vor allem im Gaming-Umfeld ist es der zentrale Treffpunkt meines sozialen Umfelds. Inhalte lassen sich schnell teilen, Voice- und Video-Chats funktionieren zuverlässig, und spontane Interaktion ist ohne größere technische Hürden möglich.

Mir ist bewusst, dass Discord in puncto Datenschutz kaum Ansprüche erfüllt. Gleichzeitig finden dort keine sensiblen Gespräche statt, sondern soziale Interaktion, Unterhaltung und gemeinsames Spielen. Dieses Spannungsfeld – **zwischen funktionaler Nutzbarkeit und datenschutzrechtlichen Bauchschmerzen** – nehme ich bewusst in Kauf, ziehe aber klare

Grenzen, was Inhalte und Nutzungskontext betrifft.

Voice- und Video-Calling

Die meisten alltäglichen Videoanrufe finden bei mir über **FaceTime** statt, sofern alle Beteiligten im Apple-Ökosystem unterwegs sind. Das funktioniert zuverlässig, ist unkompliziert und erfüllt seinen Zweck.

Für Konferenz- oder Gruppenanrufe mit mehreren Räumen, Moderation oder Screen-Sharing bevorzuge ich Open-Source-Lösungen wie **Jitsi** oder **BigBlueButton**. In der Unternehmenswelt sind jedoch **Zoom** oder **Microsoft Teams** häufig alternativlos – sei es durch Vorgaben oder durch schlichte Gewohnheit.

In solchen Fällen versuche ich, den Schaden zu begrenzen: **Ich nutze diese Dienste möglichst isoliert**, etwa in einer virtuellen Maschine oder auf einem separaten Gerät, erlaube Mikrofonzugriff nur temporär und verweigere den Zugriff auf Kamera oder Bildschirm, sofern dies nicht zwingend erforderlich ist.

Telefonate im klassischen Sinne will ich in Zukunft eher vermeiden.. Zwar lassen sich viele Dinge im Gespräch schneller klären als über lange Textverläufe, dennoch versuche ich ungeplante Anrufe weitgehend zu vermeiden. **Unangekündigte Telefonate lehne ich in der Regel ab**, nicht zuletzt wegen der weiterhin hohen Anzahl an Spam- und Werbeanrufen. Wenn ich telefoniere, dann bevorzugt über **VoIP** – klassische GSM-Telefonie bietet aus meiner Sicht weder akzeptable Qualität noch nennenswerte Privatsphäre.

Social Networks

Abgesehen von gelegentlichen Beiträgen auf **Mastodon** nutze ich soziale Netzwerke nur noch sehr eingeschränkt bis gar nicht. **Reddit** habe ich nie aktiv genutzt, **Twitter/X** habe ich vor einiger Zeit völlig aufgegeben, und neuere Plattformen wie **Bluesky** oder **Lemmy** konnten mein Interesse bislang nicht nachhaltig wecken.

Nach der Übernahme von Twitter bin ich ins Fediverse zurückgekehrt und habe dort wieder einen Account eingerichtet. Auf **nrw.social** fühle ich mich gut aufgehoben – auch wenn ich die Plattform überwiegend passiv nutze. Es gibt einige Accounts mit sehr guten Inhalten, doch insgesamt habe ich den Eindruck, dass **auch Mastodon stark zu Echo-Kammern neigt.**

Vielleicht ist es weniger eine Plattform- als eine Nutzungsfrage: **weniger konsumieren, bewusster auswählen, gelegentlich die eigene Timeline neu sortieren** und offen für neue

Themen bleiben.

Darüber hinaus schaue ich gelegentlich auf **Hacker News** vorbei, um neue Open-Source-Projekte, Werkzeuge oder technische Entwicklungen zu entdecken – oder schlicht, um einen Eindruck davon zu bekommen, womit sich die Szene aktuell beschäftigt.

Kontakte, Kalender und Reminders

Früher habe ich einen eigenen **CardDAV- und CalDAV-Server mit Baikal** betrieben, um Kontakte und Kalender selbst zu hosten. Das mache ich inzwischen nicht mehr.

Meine E-Mail läuft über **iCloud**. Mit **"E-Mail-Adresse verbergen"** bietet Apple zudem einen Dienst zur automatischen Generierung von Wegwerf-Adressen an, der für mich **außerordentlich zuverlässig und unkompliziert** funktioniert. Da außerdem eine meiner Domains daran angebunden ist, war es für mich ein logischer Schritt, auch Kontakte und Kalender dort zu verwalten.

Oft wird argumentiert, dass iCloud nicht sicher genug sei. Apple setzt zwar auf starke Verschlüsselung und umfangreiche Sicherheitsmaßnahmen, allerdings sind Kalender und Kontakte aufgrund der verwendeten Standards (CardDAV / CalDAV) **nicht Ende-zu-Ende verschlüsselt**. Apple weist selbst transparent darauf hin (Apple: iCloud-Datensicherheit).

Für mich ist dieses Sicherheitsniveau derzeit **ausreichend**. Ich vertraue darauf, dass Apple meine Daten **nicht in der Weise monetarisiert**, wie es bei anderen großen Anbietern üblich ist, insbesondere nicht zur systematischen Profilbildung für Werbezwecke. Dieser Ansatz ist aus meiner Sicht auch Teil des Geschäftsmodells – inklusive des höheren Einstiegspreises der Plattform (Apple Privacy).

Sollte sich dieser Umgang mit Daten in Zukunft grundlegend ändern, würde ich mein Setup erneut überdenken. Bis dahin sind meine Kalender- und Kontaktdaten bei Apple für meinen Anwendungsfall gut aufgehoben.

Als Alternative zu den Apple Webwerf-Adresse, gibt es mailgw und im DuckDuckGo Browser die DuckDuckGo Email Protection welche auf deren Hilfe-Seiten ausfürlich erklärt wird.

Man muss nicht alles in die Cloud legen

> --

> **Man muss nicht alles jederzeit und überall in der Cloud verfügbar machen.** Dienste wie CardDAV, CalDAV oder Passwortmanager-Instanzen müssen nicht offen im Internet stehen. Wenn ein externer Zugriff notwendig ist, ist es sinnvoller, diese Dienste über sichere Tunnel wie **WireGuard** oder **Tailscale** erreichbar zu machen, statt sie direkt zu exponieren. Einen Dienst öffentlich bereitzustellen sollte immer die letzte Option sein.

Wer höhere Anforderungen an Kontrolle, Selbsthosting oder Abschottung hat, **hat dafür heute sehr gute Möglichkeiten** – vom lokalen Betrieb bis hin zu VPN-basiertem Zugriff. Für meinen Alltag überwiegen jedoch derzeit **Komfort, Integration und ein für mich akzeptables Maß an Sicherheit**, weshalb ich mich bewusst für iCloud entschieden habe.

Dokumente & Daten

Der Umgang mit Dokumenten und persönlichen Daten ist immer ein Abwägen zwischen Sicherheit und Alltagstauglichkeit. Nicht jeder Anwendungsfall erfordert maximale Absicherung oder komplexe Setups – entscheidend ist, **die eigenen Anforderungen realistisch einzuschätzen**.

In meinem Setup liegt der Fokus auf dem Schutz sensibler Daten im Ruhezustand, während unkritische Inhalte bewusst weniger streng behandelt werden. Ziel ist ein **pragmatischer, funktionaler Umgang mit Daten**, der Sicherheit bietet, ohne den Alltag unnötig zu verkomplizieren.

Wenn die Daten in irgendeiner Form vertraulich sind, verwende ich zusätzlich **Cryptomator**- oder **VeraCrypt**-Container, um die Inhalte vor unbefugtem Zugriff zu schützen.

Versionskontrolle

Ein großer Teil meiner sensiblen Daten steht unter Versionskontrolle, das heißt, ich verwalte sie in **Git-Repositories**. Wenn die Daten in irgendeiner Form vertraulich sind, verwende ich zusätzlich transcrypt um sie transparent zu ver- und entschlüsseln.

Je nach Art der Daten liegt das Git-Remote entweder in einem **öffentlichen oder privaten git**-Repository oder auf einem **privaten Git-Server**, den ich innerhalb meiner eigenen Infrastruktur betreibe.

Darüber hinaus nutze ich `git` auch zur Zusammenarbeit, da sich anderen Personen gezielt Zugriff auf einzelne Repositories gewähren lässt, ohne mehr Daten freizugeben als notwendig.

Dabei sollte man berücksichtigen, dass Versionskontrolle vor allem für **sich ändernde Daten** sinnvoll ist, bei denen eine nachvollziehbare Historie gewünscht ist. Für statische oder große Binärdateien kann Git hingegen schnell zu unnötigem Speicherverbrauch führen und ist dort nur eingeschränkt geeignet.

Synchronized Data (Datensynchronisation)

Daten, die keiner Versionskontrolle unterliegen müssen und unter Umständen nicht jederzeit verfügbar sein müssen, fallen für mich in diese Kategorie. Dazu zählen beispielsweise Dokumente, die aus organisatorischen oder rechtlichen Gründen aufbewahrt werden, sich aber nur selten ändern.

Für diese Art von Daten nutze ich **Syncthing**. Syncthing übernimmt die Synchronisation der benötigten Daten zwischen meinem **Computer**, meinem **NAS** und meinem **Smartphone**. Im Kern handelt es sich dabei um eine **dezentrale Alternative zu Diensten wie Dropbox**, ohne zentralen Anbieter und ohne Cloud-Zwang.

Da Syncthing mehrere Ordner unabhängig voneinander synchronisieren kann, habe ich zusätzlich einen **gemeinsamen „Shared"-Ordner** eingerichtet. Über diesen lassen sich innerhalb der Familie unkompliziert Dateien austauschen – etwa Fotos oder Dokumente – ohne sie per E-Mail versenden oder auf externe Cloud-Dienste hochladen zu müssen.

Office Suites & Dokumentenerstellung

Statt **Google Docs** oder **Microsoft Office 365** nutze ich überwiegend **reine Textformate**, die ich bei Bedarf in andere Ausgabeformate wie etwa PDF überführe. Dieser Ansatz erlaubt eine klare Trennung zwischen Inhalt und Darstellung und ist langfristig robust sowie gut automatisierbar.

Für das Schreiben von Texten verwende ich meist HedgeDoc oder VSCodium, in letzter Zeit auch zunehmend den Zed Editor. Zur Erzeugung von PDF-Dateien nehme ich entweder Pandoc oder eine **self-hosted** Instanz von Stirling PDF.

Für komplexere oder stärker layoutorientierte Texte, die ich nur selten erstelle, greife ich je nach Kontext auf macOS Pages oder LibreOffice zurück.

Kollaboratives Arbeiten findet entweder über **HedgeDoc** oder über CryptPad statt.

Diagramme

Für einfache Diagramme verwende ich diagrams.net (ehemals draw.io) oder eine **self-hosted** Instanz.

Mit **Monodraw** für macOS gibt es ein sehr gutes Werkzeug für ASCII-Diagramme, das allerdings leider nicht plattformübergreifend ist.

Wenn ich anspruchsvollere Diagramme für **Service- oder Systemarchitekturen** benötige, nutze ich Cloudcraft.

Backups

Da die meisten wichtigen Daten, mit denen ich arbeite, bereits in entfernte Git-Repositories gepusht oder über Syncthing synchronisiert werden, ist der Umfang klassischer Backups bei mir überschaubar. Für die Daten, die dennoch gesichert werden müssen, setze ich auf **rsync**, setze ich auf restic und rclone.

Security

Cloud

Infrastructure Providers

Domains

Git

Web

APIs & Services

Analytics

Push Notifications

Further Reading

Revision #1

Created 2026-02-26 15:07:14 UTC by Carsten

Updated 2026-02-26 15:08:30 UTC by Carsten