



❤ lich willkommen

Zum Webinar  :

„Sicher im Netz -

 Sich gut geschützt und selbstbestimmt im Internet bewegen, mit Smartphone, Tablet oder Computer. “



# Themenübersicht

- 1) Passwörter und Zugangsdaten
- 2) Mehrfaktor-Authentifizierung
- 3) Homebanking
- 4) Browser
- 5) Identitätsverschleierung
- 6) E-mail
- 7) Messenger
- 8) Social Media
- 9) Videokonferenzen
- 10) Betriebssysteme für Computer & Mobilgeräte

# Passwörter

Regel: sollte mindestens 8 Zeichen, Klein- und Großbuchstaben ,  
Zahlen und Sonderzeichen enthalten

Man kann sich auch sehr sichere Passwörter von Passwort-  
Generatoren erzeugen lassen

In einem Notizbuch festhalten mit einem kleinen Hinweis, nur für  
dich auch später noch verständlichem zur Zuordnung und oder einem  
externen Datenträger, beides zu Haus gut verstecken

Nur lokale OpenSource-Passwortmanager verwenden.: z.Bsp.  
KeyPassXC, interner Passwordmanger von Brave & Firefox, Lieber  
keine in einer fremden Cloud verwenden

# Mehrfaktor Authentifizierung (MFA) mit Einmalpasswörtern (OTP)

mit OTP-Authentifizierungs-Apps:

lieber OpenSource-Apps wie Aegis, Flauth, Open Passkey, Conceal Authenticator, Ente Auth  
oder Proton Authenticator  
anstatt GoogleAuthenticator

Mit einem physischen Gerät wie z.Bsp. RainerSCT-Authenticator

Am sichersten mit altem Smartphone ohne Internet-Anbindung und einer OTP-Auth-App

Die App verbindet sich jeweils einmal mittels QR-Code mit einer Plattform. Ab dann kann  
einfach zur Authentifizierung einfach der zugehörige gerade angezeigte (meist Zahlen-)Code  
eingegeben werden



# Homebanking



- Vollständig auf dem Smartphone würde ich es nicht empfehlen
- Möglichst in einem Sicheren Browser wie Brave oder abgesichertem Firefox
- Viele Banken erfordern heute aber die Authentifizierung mit ihrer Banking App
- Sicherer unter Linux in einer virtuellen Maschine oder von Live-USB-Stick

# Sichere Webbrowser

- Brave
- Vivaldi
- Firefox mit Sicherheitserweiterungen wie NoScript, uBlock,  $\mu$ Block u.ä.
- Torbrowser



# Verschleierung deiner Identität beim Nutzen des Internets

Normalerweise protokolliert dein Internet-Anbieter alle von dir aufgerufenen Webadressen. Doch das kannst Du verschleiern z.Bsp. mit folgenden Methoden:

- Proxy-Server
- Virtuelles privates Netzwerk (VPN)
- TOR-Netzwerk



# Proxy-Server

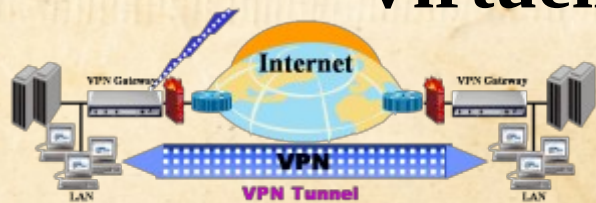
- Ein Dienst der stellvertretend für dich mit anderer IP-Adresse im Internet deine gewünschte Webquellen aufruft und zu dir weiterleitet

## Listen mit Proxies

- <https://www.experte.de/proxy-server>
- <https://www.netzwelt.de/proxy/index.html>
- <https://hide.mn/de/proxy-list>



# Virtuelles privates Netzwerk (VPN)



- Deine Webanfragen werden verschlüsselt an eine VPN-Stelle gesendet und von da weiter geleitet. Von außen ist nur die Verbindung zu dieser VPN-Stelle sichtbar aber nicht das eigentlich Ziel der Inhalt deiner Anfrage.
- Somit ist von außen ersichtlich welche Webseiten und Dienste Du darüber nutzt und welche Inhalte ausgetauscht werden, sondern lediglich das Du mit einer VPN-Stelle verbunden bist.
- Nachteil: manche, vor allem kostenfreie VPN-Anbieter haben zuweilen eine langsame Verbindung
  - Heute sehr übliche Anwendung:
    - Geschützter Zugriff auf bestimmte Bereiche im Firmen-Netzwerk aus dem Homeoffice
      - Zugriff auf Länder-beschränkte Webinhalte aus anderen Ländern
      - Verschleierung der eigenen Identität auf Webseiten

# VPN-Anbieter-Vergleiche



<https://www.heise.de/download/specials/Anonym-surfen-mit-VPN-Die-besten-VPN-Anbieter-im-Vergleich-3798036>

[https://www.chip.de/artikel/VPN-Test-Die-besten-Anbieter-im-Vergleich\\_182800063.html](https://www.chip.de/artikel/VPN-Test-Die-besten-Anbieter-im-Vergleich_182800063.html)

<https://www.pcwelt.de/article/1193534/die-besten-vpn-dienste-im-vergleich.html>

# The Onion Routing Project (TOR-Netzwerk)

- Leitet deine Aufrufe über mehrere zufällig ausgewählte Knotenpunkte des weltweiten TOR-Netzwerks an dein gewünschtes Ziel

## Vorteile:

- kostenfrei, braucht nur den TOR-Browser

## Nachteile:

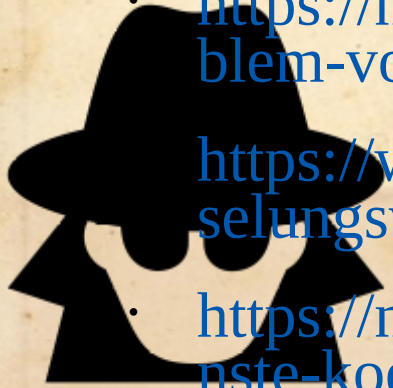
- einige Knotenpunkte könnten staatlich überwacht werden
- keine Verschlüsselung vom Browser zum Eintrittspunkt ins TOR-Netzwerk
- Nicht so einfach einzustellen, bis es reibungsfrei läuft



# Messenger

## begehrtes Angriffs- und Spionageziel

- <https://netzpolitik.org/2021/metadaten-wo-das-eigentliche-privacy-problem-von-whatsapp-liegt>
- <https://www.zeit.de/digital/2020-11/whatsapp-signal-eu-rat-verschlueselungsverbot-ueberwachung-messenger-dienste>
- <https://netzpolitik.org/2021/ohne-staatstrojaner-polizei-und-geheimdienste-koennen-whatsapp-mitlesen>
- <https://www.teltarif.de/app/whatsapp/datenschutz.html>
- <https://www.zeit.de/digital/datenschutz/2024-01/iphone-nsa-spionage-mikros-apple>
- <https://www.businessinsider.de/tech/whatsapp-keine-hintertuer-fuer-behoerden-2017-1>





# Messenger

mit Ende-zu-Ende-Verschlüsselung  
ohne Dienste-Hintertüren



Im Matrix-Netzwerk am besten mit Element oder FluffyChat ( <https://matrix.org/ecosystem/clients> ), selbst auf eigenem Server gehostet oder über einer von vielen kostenlosen Servern

Wire ( <https://wire.com/de> )

Session ( <https://getsession.org/de> )

Delta Chat ( <https://delta.chat/de> ) nur asynchron

Signal ( <https://signal.org/de> ) mit Vorbehalt

Telegram ( <https://telegram.org> ) E-E-Verschlüsselung nur in „geheimen Chats“ möglich

Yami ( <https://jami.net> ) dezentral aber nur zeitgleich: direkte Verbindung zwischen Gesprächspartnern oder Server dazwischen

# Sichere Email-Anbieter

- <https://posteo.de>
- <https://mailbox.org>
- <https://www.emailn.de>
- <https://firemail.de>
- <https://tuta.com/de>
- <https://mail.de/de>
- <https://proton.me/mail>





# Email-Verschlüsselung



Erzeuge ein mal ein Schlüsselpaar aus deinem öffentlichen Schlüssel und deinem privaten Schlüssel. Installiere diesen in Deinem Email-Programm. Sehr einfach geht das mit dem Emailprogramm „Thunderbird“ und dem Plugin „Enigmail“.

Wenn Du dich verschlüsselt mit wem austauschen willst, sende ihr/ihm vorher eine Email ohne sensiblen Inhalt mit deinem öffentlichen Schlüssel aus deinem Email-Programm. Die/der Empfangende kann deinen öffentlichen Schlüssel genehmigen und dann dir damit eine verschlüsselte Email senden, falls sie/er ebenfalls eine eigenes Schlüsselpaar in seinem Programm installiert hat. Diese kannst Du nur mit einem Programm öffnen in dem Du den zu dem vorher gesendeten öffentlichen Schlüssel, passenden privaten Schlüssel installiert hast.

# Videotreffen und Webinare



Mit Opensource-Software Jitsi-Meet oder BigBlueButton  
auch über Webbrowser nutzbar

Vielen kostenlos nutzbare Instanzen, wie

<https://www.infomaniak.com/de/ksuite/kmeet>

<https://meet.jit.si>

Weitere kostenfrei nutzbare JitsiMeet-Instanzen:

<https://scheible.it/liste-mit-oeffentlichen-jitsi-meet-instanzen>

JitsiMeet-App für PCs: <https://github.com/jitsi/jitsi-meet-electron/releases>

BigBlueButton-Instanz

<https://meeting.levigo.cloud>

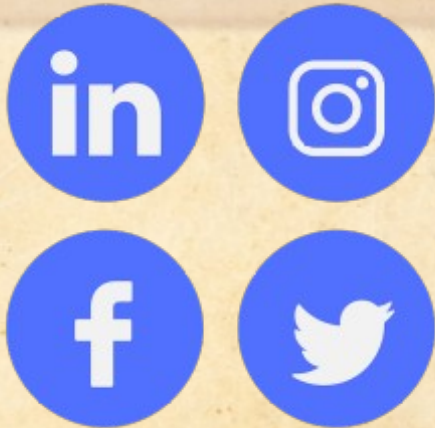
Oder über die zuvor genannten Messenger falls für alle beteiligten verfügbar



# Social Media

Hier habe ich mich mit einer gesonderten Email-Adresse angemeldet, die nur für diese Dienste genutzt wird aber nicht für eigenen Nachrichtenverkehr.

Wenn möglich würde ich mich außerdem mit einer extra Prepaid-Handynummer anmelden, falls die dafür verlangt wird, die ich nicht zum telefonieren nutze





# Merkmale von OpenSource-Software

Der Programmiercode der Software ist für alle einsehbar und  
veränderbar

Manche OpenSource-Lizenzen verpflichten dazu jede Änderung am  
Quellcode ebenfalls zu veröffentlichen

Menschen können von überall auf der Welt daran mitwirken und  
Änderungsvorschläge einreichen

Änderungsvorschläge werden von der Entwicklergemeinschaft geprüft.  
Das schützt vor dem Einschmuggeln von Schadcode.

Fehler und Sicherheitslücken können so schnell entdeckt und beseitigt  
werden

Neue Technologien können so ausprobiert werden. Was am besten  
nutzbar ist, verbreitet sich demokratisch am schnellsten

# Betriebssysteme

- Gnu-Linux: für ganz viele unterschiedlichste Geräte verfügbar
  - MS-Windows: nur für PCs u.ä.
- MacOS: nur für Apple<sup>TM</sup>-Mac-Geräte verfügbar
  - Android: für verschiedenste Mobilgeräte
    - iOS nur für Apple<sup>TM</sup>Mobilgeräte
    - CustomROMs wie Lineage, /E/
  - GrapheneOS nur für Google-Smartphone verfügbar
- Ubuntu-Touch: vollwertiges Gnu-Linux auf Mobilgeräten



Hier folgt meine persönliche Einschätzung zu Vor- und Nachteilen.:

# Vorteile von Windows

- Weit bekannt
- Auf den meisten PCs vorinstalliert
- Breite Unterstützung von den meisten Programmen
  - Unterstützt viele moderne Zusatzgeräte
  - Unzählige Anleitungen im Netz verfügbar
- sehr viel Erfahrung von Nutzenden ist darin eingeflossen



# Nachteile von Windows

- Wird gezwungen Hintertüren für Behörden und Geheimdienste einzubauen
  - Liest Emails mit
- Sehr hohe Leistungsanforderungen an Hardware, steigt mit neuen Versionen
- Sehr hohe Gefährdung durch Schadprogramme wie Trojaner, Viren, Spyware u.a.
  - Daten in der Microsoft-Cloud gespeichert
- Enthält meiner Erfahrung nach sehr viele Funktionsfehler und teilweise veraltete Technologien
- Neue Windowsversionen arbeiten nur schlecht mit älteren Geräte zusammen



# Vorteile von MacOS

- Sehr bekannt und beliebt
- Sehr leicht zu bedienen
- Sehr viele Funktionen
  - Sehr stabil
- Sehr gut abgestimmt, da Hard- und Software aus einem Haus
  - Unzählige Anleitungen im Netz verfügbar

# Nachteile von MacOS

- Wird gezwungen Hintertüren für Behörden und Geheimdienste einzubauen
  - Mittlerweile zunehmende Gefährdung durch Schadprogramme
  - Arbeit nur mit Geräten aus dem eigenen Haus gut zusammen
    - Daten in der AppleCloud gespeichert
  - Keine Selbstbestimmung über die eigenen Daten
    - Veraltetes Bedienkonzept
      - Kostet viel Geld

# Was ist Linux



- Linux-Kernel: Ursprünglich war mit Linux nur der Linux-Kernel, also der Betriebssystem Kern, gemeint, der direkt mit der Computer-internen Hardware spricht
  - Gnu-Linux = Linux-Kernel (Betriebssystemkern) + Gnu-Userland (textbefehlgesteuerte Werkzeuge ohne grafische Benutzeroberfläche zur Steuerung des Systems durch Admins)
- Linux-Distribution: ist eine Zusammenstellung aus Linux-Kern + Gnu-Userland + Grafischer Benutzeroberfläche + Anwender-Software), die bekanntesten Linux-Distributionen sind derzeit u.a. LinuxMint und UbuntuLinux
- Wenn heute von Linux gesprochen wird, ist meist eine ganze Linux-Distribution gemeint



# Vorteile von Linux 1/2

- OpenSource: wird von einer weltweiten Gemeinschaft und unzähligen Unternehmen offen stetig weiter entwickelt, darunter auch viele namhafte Unternehmen, wie Intel, AMD, Google, IBM, Redhat u.v.m
  - Kostenfrei nutzbar
- Sehr leicht und frei nach eigenen Vorlieben und Anforderungen anpassbar
  - Läuft auch noch auf älteren Geräten sehr gut
  - Für unterschiedlichste Geräte verfügbar
  - beliebtestes Betriebssystem für Server
- keine absichtlich eingebauten Hintertüren für Behörden und Geheimdienste

# Vorteile von Linux 2/2

- Geringere Gefährdung durch Schadprogramm
  - Wird nicht behördlich abgehört
- Baut auf viele Jahrzehnte Erfahrungen mit Sicherheit in Netzwerken
  - Daher sicherer für sensible Aufgaben wie Homebanking
  - Arbeitet gut mit vielen anderen Plattformen zusammen
  - Weltweites Experimentierfeld für verschiedenste Software-Technologien und -Ansätze durch die Vielfalt an Varianten (Distributionen)
- Alle Nutzenden entscheiden demokratisch mit, durch ihre Wahl der Nutzung einiger Varianten, welche dieser Ansätze sich davon durchsetzen.

# Nachteile von Linux

- Umgewöhnung in der Bedienung und bei Einstellungen
- Bei Endverbrauchern noch nicht so (aber stetig mehr) verbreitet
- Muss in der Regel selbst installiert werden ... heutzutage aber schon recht einfach, einige wenige Geräte werden mittlerweile mit vorinstalliertem Linux angeboten
- Nicht alle speziellen, insbesondere berufsspezifischen Programme laufen darauf.
  - tiefgreifendere Anpassungen brauchen tiefes Fachwissen und Erfahrung



# Vorteile von Android

- Weit bekannt
- Auf den meisten Smartphones vorinstalliert
- Breite Unterstützung von den meisten Apps
- Unzählige Anleitungen im Netz verfügbar
- Baut auf stabilem und sicherem Linux-Kern auf
- Jede App läuft eingekapselt in einer Sandbox

# Nachteile von Android

- Wird gezwungen Hintertüren für Behörden und Geheimdienste einzubauen
  - Viele Datensammel-Funktionen von Google
- Sehr hohe Gefährdung durch Schadprogramme wie Trojaner, Viren, Spyware u.a.
- Nicht von allen Geräte-Herstellern gut und sauber installiert und angepasst → das führt manchmal zu Fehlverhalten
  - Die oberen Schichten des Systems sind nicht OpenSource

# Vorteile von iOS

- Sehr bekannt und beliebt
- Sehr leicht zu bedienen
- Sehr gut abgestimmt, da Hard- und Software aus einem Haus
  - Unzählige Anleitungen im Netz verfügbar
- Gewisse Sicherheit vor Fremdeingriffen durch eingeschlossenes System



# Nachteile von iOS

- Wird gezwungen Hintertüren für Behörden und Geheimdienste einzubauen
- Mittlerweile zunehmende Gefährdung durch Schadprogramme
- Arbeit nur mit Geräten aus dem eigenen Haus gut zusammen
  - Lässt nur Apps aus dem eigenen AppStore zu
- Weitere gezielte Beschränkungen die Kunden an Apple binden sollen
  - Daten in der AppleCloud gespeichert
  - Keine Selbstbestimmung über die eigenen Daten
    - Kostet viel Geld

# Custom-Roms

- Nachgebautes Betriebssysteme für Android-Geräte auf Basis des Android-OpenSource-Projektes

## Vorteile:

- frei von Googles Überwachungsfunktionen
  - Sehr frei anpassbar
- Zusätzliche Sicherheitsfunktionen

## Nachteile

- Nicht so leicht zu installieren
- Läuft nur auf bestimmten Geräten gut
- Sicherheitsrisiko, wenn es nicht gut eingestellt ist



# Alternative Quellen für Android-Apps

- **Aurora-OSS**: Zugriff auf alle kostenfreien Apps auf dem Playstore auch ohne Google-Konto, kostenpflichtige brauchen auch Google-Konto
  - **F-Droid**: Zugriff auf ausschließlich OpenSource-Apps für Android und Nachbauten
- **MicroG**: Ersatz für Google-Dienste, die einige Apps verlangen ohne Google-Konto





# GrapheneOS

Ein Android-Nachbau der sehr stark auf Sicherheit ausgerichtet ist.

Gilt derzeit als das sicherste Betriebssystem für Mobilgeräte

- Vorteile:

- Völlig googlefreier Android-Nachbau
- Gilt als sicherstes mobil-Betriebssystem
  - Auch sehr sicher vor Überwachung

- Nachteile

- Soll sehr schwierig zu bedienen sein
- Nicht alle Funktionen funktionieren wie bei Android
- Läuft ironischerweise bislang nur auf Google-Pixel-Smartphones, Verhandlungen mit anderen Herstellern wie Fairphone laufen

# Ubuntu-touch

## Gnu-Linux auf mobil-Geräten

### Vorteile:

- Gleiche Freiheit wie bei Gnu-Linux auf dem Desktop

### Nachteile

- Nicht so viel auf Mobilgeräte angepasste Apps wie bei Android
- Bisläng nur für eine sehr geringe Anzahl von Geräte-Modellen verfügbar



UBports

# Geräte mit vorinstallierten alternativen Betriebssystemen

Smartphones:

- <https://murena.com/de/produkte/smartphones>
- <https://www.freifon.shop>

Laptops:

- <https://lapify.shop/linux-laptops-gebraucht>
- <https://www.tuxedocomputers.com/index.php>



# Weitere Fragen

Hast Du Fragen, Wünsche, Anregungen,  
Verbesserungsvorschläge oder wünschst Dir  
Unterstützung bei der Anwendung für deine Vorhaben?:

Richte sie gern an [tech@mitweltmacht.net](mailto:tech@mitweltmacht.net)

