CEC - Cyber Ethics Camp
Digitale Souveränitätt
Gesellschafts relevante Aspekte der Digitalisierung

Michael Georg Schmidt

ITS Explained
IT-Sicherheit einfach erklärt

E-Mail: info@its-explained.com
Mobil: +49 155 60 988 500

12. Mai 2026

Zusammenfassung

Das CEC - Cyber Ethics Camp ist eine feste Reihe von Veranstaltungen im Rahmen des #CSR-Camp - Corporate Social Responsibility Camp, einem jährlich stattfindenden Barcamp. Prof. Dr. Matthias Schmidt (BHT) und Michael Georg Schmidt (THL) (nicht verwandt und nicht verschwägert) führen diese mit freundlicher Unterstützung von Frank Feldmann und der Firma Eventbrite durch. Hierbei geht es darum, ein Bewusstsein für IT-Sicherheit und deren gesellschaftliche Zusammenhänge zu erzeugen. IT-Sicherheit beeinflusst unsere Gesellschaft und unser Zusammenleben. Die Digitalisierung der Gesellschaft birgt viele Möglichkeiten und Chancen, die wir nutzen sollten. Wichtig dabei ist es jedoch, eine möglichst hohe digitale Souveränität zu behalten. Darauf zu achten, dass wir nicht von großen Tech-Firmen oder anderen Staaten abhängig sind. Aktuell besteht eine hohe Abhängigkeit von einzelnen Tech-Riesen und vor allem den USA. Diesen Zustand sollten wir versuchen zu ändern. Das geht nicht von jetzt auf gleich, sondern in kleinen Schritten und Stück für Stück. Damit können wir beginnen, zu versuchen, ein digitales Gleichgewicht zwischen Europa, den USA und Asien herzustellen. Alle aufgeführten Programme sind im Quellennachweis verlinkt und können per Klick erreicht werden. Alle hier verlinkten Programme gibt es auch in einer kostenlosen Version, mit Ausnahme von Mullvad-VPN, NYM und Threema.

Alle hier erwähnten Maßnahmen gelten sowohl für Ihr Smartphone, als auch für Ihren Computer. Mit wenigen Ausnahmen, die in diesem Fall explizit gekennzeichnet sind. Dies sind Add-ons, die nur für Ihren Computer zur Verfügung stehen, das Life-Betriebssystem Tails, die Verschlüsselungssoftware VeraCrypt und SD-Karten, die Sie nur an einem Rechner nutzen können.

Dieser Text ist so aufgebaut, dass Sie im ersten Teil Kurzinformationen finden. Im zwetien Teil finden Sie ausführlichere Erläuterungen. Die Texte enthalten jeweils Sprungmarken, mit denen Sie zwischen beiden Teilen wechseln können.

Abschließend merke ich an, dass ich nur eine Geschlechtsform verwende, um diesen Text besser lesbar zu halten. Dennoch ist mir die Gleichberechtigung aller Geschlechter ausgesprochen wichtig.

Inhaltsverzeichnis

1 Kurzinformationen zu sicherer Kommunikation

1.1 E-Mails

E-Mails sollten

1. Ende-zu-Ende (E2EE) [**E2EE**] verschlüselt
2. bei einem europäischen/schweizer Anbieter
3. einfach zu bedienen

sein.

Ich nutze **ProtonMail** [**ProtonMail**]

Anmerkung: Mit der Einrichtung eines kostenlosen E-Mailkontos bei ProtnMail erhalten Sie gleichzeitig

- ProtonCalendar 1.14
- ProtonDrive 1.18
- ProtonVPN 2.4.1
- ProtonPass 1.3
- ProtonDocs [**ProtonDocs**]
- ProtonWallet [**ProtonWallet**]

Erläuterungen zu E-Mails: 2.1

1.2 Passwörter

Passwörter sollten folgende Kriterien erfüllen

- sie sollten laaaaaaang sein - mindestens 16 Zeichen
- sie sollten GROSSBUCHSTABEN
- sie sollten kleinbuchstaben
- sie sollten Ziffern 0...9
- sie sollten Sonderzeichen @! $-^{|}$ +

enthalten. Passwörter sollten nie geändert werden, es sei denn es tritt ein Notfall ein. Von Menschen ersonnene Passwörter sind leichter zu erraten, als kryptisch generierte. Daher gibt es Passwortgeneratoren.
Erläuterungen zu Passwörtern: 2.2

1.3 Passwortmanager und -generatoren

Passwortmanager, auch Passwort Tresor genannt, der unser Vertrauen genießt ist:

1. ProtonPass [**ProtonPass**] (online)

   Sehr beliebt ist ebenfalls

2. Bitwarden [**Bitwarden**] (online)

Alle hier genannten Passwortmanager generieren auf Wunsch auch sichere Passwörter.
Erläuterungen zu Passwortmanagern und -generatoren: 2.3

1.4 VPN - Virtual Private Network

1. ProtonVPN [**ProtonVPN**]
   Erläuterungen zu ProtonVPN: 2.4.1

2. Mullvad VPN [**MullvadVPN**]
   Erläuterungen zu Mullvad VPN: 2.4.2

3. NYM [**NYM**]
   Erläuterungen zu NYM: 2.4.3

1.5 DNS - Domain Name System

Wenn Sie im Internet surfen, rufen Sie Seiten in der Regel nach deren Namen auf wie „th-luebeck.de“. Da es viele verschiedene Alphabete und Schriften gibt, gäbe es schnell Probleme, wenn alle Nutzerinnen und Nutzer des Internets das machen würden. Daher werden diese Namen in so genannte **IP-Adressen** umgewandelt. Die th-luebeck.de ist dann 193.175.120.221.

Diese Wandlung führen so genannte **DNS-Server - Domain Name System Server** durch. Im Normalfall werden Ihre Anfragen unverschlüsselt übertragen. Damit können „Lauscher“ aus den von Ihnen getätigten Anfragen ein Profil von Ihnen erstellen.

Um das zu verhindern, ist es sinnvoll, Ihre Anfragen an DNS-Server zu verschlüsseln. Ich nutze dafür drei Anbieter

1. DNS4EU [**DNS4EU**, **DNS4EUAbout**] - ein von der EU gefördertes DNS-Server Projekt, das folgende Services anbietet:

   (a) verschlüsseltes DNS mit Kinderschutz [**KiSchu**]

   (b) verschlüsseltes DNS mit Werbeblocker [**AddBlock**]

   (c) verschlüsseltes DNS mit Kinderschutz und Werbeblocker [**ChildAddBlock**]

   (d) verschlüsseltes DNS ungefiltert [**Unfiltered**]

   Wie Sie diese DNS-Server auf Ihrem Smartphone einrichten, steht hier [**DNSSetup**].
   Erläuterungen zu DNS4EU: 2.5.1

2. Mullvad DNS [**MullvadDNS**, **MullvadÃIJberUns**]

   (a) verschlüsseltes DNS mit Blocker für Werbung und Tracker [**MullvadDNS**]

   (b) verschlüsseltes DNS mit Blocker für Werbung, Tracker und Malware (Schadsoftware) [**MullvadDNS**]

   (c) verschlüsseltes DNS mit Blocker für Werbung, Tracker, Malware (Schadsoftware) und Social Media [**MullvadDNS**]

   (d) verschlüsseltes DNS mit Blocker für Werbung, Tracker, Malware, Inhalte ab 18 Jahren und Online Casinos [**MullvadDNS**]

   (e) verschlüsseltes DNS mit Blocker für Werbung, Tracker, Malware (Schadsoftware), Inhalte ab 18 Jahren, Online Casinos und Social Media [**MullvadDNS**]

   Wie Sie Mullvad-DNS einrichten steht ebenfalls hier [**MullvadVPN**].
   Erläuterungen zu MullvadDNS: 2.5.2

3. quad9 [**quad9**, **quad9About**] - ein Open Source Projekt für verschlüsseltes DNS
   (a) verschlüsseltes DNS mit Blocker für Inhalte ab 18 Jahren [**quad9**]
   (b) verschlüsseltes DNS mit Blocker für Werbung [**quad9**]
   (c) verschlüsseltes DNS mit Bockern für Inhalte ab 18 Jahren und Werbung [**quad9**]
   (d) verschlüsseltes DNS ungefiltert [**quad9**]

Erläuterungen zu quad9: 2.5.3

1.6 Der „richtige“ Browser

1. Brave [**Brave**]
   Erläuterungen zu Brave: 2.6.1
2. DuckDuckGo [**DuckDuckGo**, **DuckDuckGoÃIJberUns**]
   Erläuterungen zu DuckDuckGo: 2.6.2
3. Firefox [**Firefox**]
   Erläuterungen zu Firefox: 2.6.3
4. Startpage [**Startpage**, **StartpageÃIJberUns**]
   Erläuterungen zu Startpage: 2.6.4

Erläuterungen zu Browser: 2.6

1.7 Add-Ons

Grundsätzlich sind Add-ons - Erweiterungen für Browser - zurückhaltend einzusetzen, denn sie können auch immer eine Angriffsfläche bieten. Es gibt allerdings Add-ons, die eine Hilfe sein können, um Ihre Privatsphäre zu schützen. Dazu gehören Firefox Multi-Account Containers [**MultiAccount**], Temporary Containers [**Temporary**] und User-Agent Switcher and Manager [**UserAgent**].
Erläuterungen zu Add-Ons: 2.7

1.8 TOR

TOR steht für Tor Onion Routing. Ihre Daten werden mehrfach gekapselt an ihr Ziel geschickt, so dass der Server über den Ihre Anfrage ins Internet gelangt, nicht „weiß“, wer die Anfrage gestellt hat. TOR ist ebenfalls das Tor zum Darknet. Darknet-Seiten haben die Endung .onion. Wenn Sie also Autos.onion im Browser suchen, ist die Wahrscheinlichkeit, dass Sie ein Darknet-Angebot für Autos erhalten groß. Sie können hier auch nach Suchmaschinen für spezielle Interessen suchen. Mit diesen finden Sie dann deutlich mehr Websites im Darknet als mit anderen Browsern. *Erläuterungen zu TOR: 2.11*

1.9 Tails

Tails [**Tails**] ist ein so genanntes Live Betriebssystem. Sie können es auf einem Datensträger installieren und damit auf fremden Rechnern im Internet surfen, ohne Spuren zu hinterlassen. Allerdings können sie mit Tails auch keine Daten speichern. *Erläuterungen zu Tails: 1.9*

1.10 Digitale Souveränität

Digitale Souveränität bedeutet die Unabhängigkeit von großen Tech-Konzernen, von Regierungen oder proprietärer Software. Nutzen Sie so viel wie möglich Open Source Software und freie Betriebssysteme, wie Linux. *Erläuterungen zu Digitaler Souveränität: 2.13*

1.11 Nutzung von KI/AI - künstlicher Intelligenz

Wenn Sie KI nutzen, müssen Sie davon ausgehen, dass von Ihnen ein Profil erstellt wird. Je mehr Sie mit KI arbeiten, desto genauer wird dieses Profil. Daher seien Sie vorsichtig damit oder befolgen die Erklärungen unter Punkt 2.7.
Erläuterungen zu KI/AI: 2.14

1.12 2FA - Second Factor Authentication

2FA [**2FA**] steht für „Second Factor Authentication“. Als zweiter Faktor zur Identifikation kommen mehrere Möglichkeiten in Betracht. Das können sein:

- E-Mails mit einer Nachricht
- SMS mit einer Nachricht
- per App generierte Codes
- Token [**Token**]
- Photo TANs [**photoTAN**]
- biometrische Merkmale [**Biometrie**]

Vermutlich gibt es noch weitere „zweite Faktoren“, jedoch wäre es unpassend, hier eine vollständige Aufzählung zu erzeugen.

Einfach, kostenlos und wirkungsvoll sind **Authenticator Apps**. Das sind Programme für 2FA. Man installiert sie auf dem Smartphone. Ich nutze dafür

1. OTP Auth - nur für iOS [**OTPAuth**]
2. FreeOTP [**FreeOTP**]
3. 2FAS [**2FAS**]

Eine noch sicherere Variante ist der Einsatz von **Token** [**Token**]. Das sind Geräte, die wie USB-Sticks aussehen. Man hält sie zur Freischaltung über das Smartphone. Sofern man also nicht über das Smartphone, das Passwort **und** den Token verfügt, kann keine Identifikation erfolgen.
Erläuterungen zu 2FA - Second Factor Authentication 2.15

1.13 Für jeden Account eine eigene E-Mailadresse

Oft müssen Sie eine E-Mailadresse angeben, wenn Sie irgendwo einen Zugang zu einem Dienst anlegen wollen. Wenn Sie immer die gleiche E-Mailadresse benutzen, bietet das Dritten die Möglichkeit, sie „zu verfolgen“ - zu tracken. Dem können Sie mit einem E-Mail Relay [**Relay**] aus dem Weg gehen.

Ich nutze dafür das kostenlose E-Mail Relay von DuckDuckGo [**DuckDuckGo**] oder alternativ das E-Mail-Relay von SimpleLogin [**SimpleLogin**]. In Kombination mit dem Browser Add-On von DuckDuckGo/SimpleLogin erstellt es mir für jeden neuen Account eine eigene E-Mailadresse (lesen Sie hierzu die

Erläuterungen unter Punkt *2.16*). Nachrichten an diese E-Mailadresse gehen in einem von mir vordefinierten E-Mailkonto ein. Das ist „mein E-Mailkonto“. Der Anbieter bei dem ich mich registriert habe, erfährt so meine private E-Mailadresse nicht.
Erläuterungen zu E-Mail Relays: 2.16

1.14 Kalender

Kalender enthalten sehr persönliche Informationen. Die meisten bereits vorinstallierten Kalender lesen alles mit. Ich nutze den **Proton Kalender** [**ProtonKalender**], um das zu verhindern. Er verschlüsselt meine Termine bereits auf dem Smartphone. Weil meine Termine nur mich etwas angehen.
Erläuterungen zu Kalender: 2.17

1.15 Speicher

Wenn Sie Daten lokal speichern, verlassen Sie sich nicht auf Verschlüsselungssysteme, die das Betriebssystem mitbringt, denn sobald Ihre Festplatte (SD) entschlüsselt ist, sind alle Daten zugänglich. Potentielle Angreifer hätten somit Vollzugriff auf alle Ihre Daten.

Daher sollten Sie wichtige Daten lieber separat mit dem Programm VeraCrypt [**VeraCrypt**] verschlüsseln. Dann müssen Sie immer nur die Datei entschlüsseln, die Sie gerade bearbeiten wollen.
Erläuterungen zu Speicher: 2.18

1.16 Speichermedien

Lassen Sie es nie zu, dass jemand USB-Geräte an Ihren Rechner oder Ihr Smartphone anschließt. Es könnten so genannte BadUSB [**BadUSB**] sein. Dann ist Ihr Rechner oder das Smartphone innerhalb von Mikrosekunden kompromittiert. SD-Karten hingegen sind sicher. *Erläuterungen zu Speichermedien: 2.19*

1.17 Anbieter für Technik die Ihre Kommunikation gefährden kann

Es gibt viele Anbieter, die Technik anbieten, die für Ihre Kommunikation gefährlich werdenkann. Völlig legal. *Erläuterungen zu Anbieter für Technik die Ihre Kommunikation gefährden kann:* **??**

1.18 Cloudspeicher

Es ist praktisch, seine Daten in der Cloud zu sichern, denn man kann von überall darauf zugreifen. Wichtig ist es aber, hierbei bestimmte Dinge zu beachten. Diese sind

1. Ende-zu-Ende Verschlüsselung (E2EE) [**E2EE**]
2. Speicherort innerhalb Europas oder der Schweiz

Ich nutze häufig den Speicher von **Proton Drive** [**ProtonDrive**], der per App [**ProtonDriveApp**] oder online [**ProtonLogin**] nutzbar ist.

Anmerkung: Wenn Sie die ProtonDrive App auf Ihrem PC nutzen, können Sie den Cloudspeicher in Ihren „Dateiexplorer“ integrieren. Dann sehen Sie ihn als „normales“ Laufwerk. Zusätzlich können Sie mit den genannten Apps eine **Echtzeit-Synchronisation** für von Ihnen vorher festgelegte Ordner und Dateien durchführen. Das ist ein Backup [**Datensicherung**] Ihrer Daten in Echtzeit. Möglicherweise ist diese Funktion jedoch kostenpflichtig.
Erläuterungen zu Cloudspeicher: 2.21

1.19 Backups

Backups Ihrer Daten sind notewendig, weil es immer passieren kann, dass ein Speichermedium beschädigt wird, oder Ihr Rechner gestohlen wird. Es empfiehlt sich mindestens zwei Backups an unterschiedlichen Orten zu benutzen. Ich nutze Cloudspeicher für Backups.

Empfehlenswert sind meiner Meinung nach:

- Borgbase [**Borgbase**]
- Hetzner [**Hetzner**]
- ProtonDrive [**ProtonDrive**]
- Tuta Speicher [**TutaSpeicher**]

Erläuterungen zu Backups: 2.22

1.20 Messenger

Als Messenger nutze ich

1. Signal [**Signal**] - als App und Desktopversion
   hier [**SignalDownload**] können Sie es herunterladen.

2. Threema [**Threema**] - als App und Desktopversion
   hier [**ThreemaDownload**] können Sie es herunterladen.

3. Simplex [**Simplex**]

Ein ***absolutes no go*** ist **Telegram**!
Weshalb das so ist wird hier [**Telegram**] anschaulich erklärt.
Erläuterungen zu Messengern 2.23

1.21 Unbelauscht telefonieren

Mobilfunktelefonate sind mit relativ geringem technischem Aufwand abhörbar. Wenn man unbelauscht telefonieren möchte. Kann man das mit den Apps **Signal** [**Signal**] oder **Threema** [**Threema**] machen. Allerdings müssen dann alle Beteiligten die jeweilige App installiert haben.
Erläuterungen zu Unbelauscht Telefonieren: 2.24

2 Erläuterungen zu den einzelnen Punkten

2.1 E-Mails

Das **wichtigste Kriterium** für E-Mails ist, dass sie **Ende-zu-Ende-Verschlüsselt** [**E2EE**] werden können. Viele Anbieter haben diese Möglichkeit nicht. E-Mails sind wie Postkarten, wenn man sie nicht verschlüsselt. Da oftmals personenbezogene Informationen in E-Mails versandt werden, beeinträchtigen diese die Rechte Dritter, ohne dass diese davon erfahren. Microsoft Outlook bietet keine E-Mailverschlüsselung an. Google & Co bezeichnen es als Service, dass sie E-Mails semantisch [**Semantik**] auswerten und die Inhalte zu Profilen verarbeiten.

Ein weiteres wichtiges Kriterium ist, dass die E-Mailanbieter in Europa oder der Schweiz ansässig sind, damit der Dienst deren strengen Datenschutzanforderungen unterliegt [**DSGVO**, **DatenschutzSchweiz**]. Bei amerikanischen Anbietern wie Microsoft, Google, Yahoo & Co. genießen „Ausländer“ keinen Datenschutz. Hier haben amerikanische Behörden auf Grund des USA Freedom Act of 2015 [**FreedomAct**] und des CLOUD Act [**CloudAct**, **CloudAct2**] das Recht von amerikanischen Unternehmen die Herausgabe von Daten derer Kunden und Geschäftspartner zu verlangen. Hierzu auch [**PatriotAct**, **PatriotActErklÃd'rt**, **FreedomActErklÃd'rt**].

Letztlich sollte die Bedienung einfach sein und am besten per App funktionieren. Wenn Sie eine App verwenden, werden bei einer Ende-zu-Ende-Verschlüsselung [**E2EE**] Ihre Daten bereits auf Ihrem Smartphone verschlüsselt. Verschlüsselt übertragen und erst die empfangsberechtigte Person kann die E-Mail wieder öffnen.

Ich setze **ProtonMail** [**ProtonMail**] ein, weil es Features bietet, die aus meiner Sicht Vorteile sind. Dies sind:

- einfache Ende-zu-Ende-Verschlüsselung, ohne Voraussetzungen auf der Gegenseite
- automatische Entfernung von E-Mail Trackern [**Nutzerverfolgung**]
- einfache Bedienung per App [**ProtonMailApp**] und Webmail
- selbst zerstörende E-Mails
- Einstellung möglich, dass Metadaten [**Metadaten**] angehängter Bilder automatisch gelöscht werden

- Funktion (in Webmail einstellbar), dass Newsletter automatisch gefiltert und angezeigt werden
  → erleichtert die Möglichkeit Newsletter zu lesen und abzubestellen
- Möglichkeit zur Strukturierung mit Ordnern
- automatische Überwachung, ob angezeigter Absender und dazugehörige Domain zusammenpassen
  → ich schreibe als Kanzler Merz ⇒ Fehlermeldung
- ein schweizer Unternehmen
  → hohes Datenschutzniveau [**DatenschutzSchweiz**]

Zurück zu E-Mails: 1.1

2.2 Passwörter

Passwörter müssen lang sein, da es Programme gibt, die Kombinationen aus Zeichen und Buchstaben automatisiert durchprobieren, bis die richtige Kombination gefunden ist. Wenn das Passwort lang genug ist - **mindestens 16 Zeichen** - Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen sind ebenfalls ein „Muss“, dann ist die Wahrscheinlichkeit, dass Ihr Passwort nicht geknackt werden kann groß.
Zurück zu Passwörter: 1.2

2.3 Passwortmanager und -generatoren

Passwortmanager nennt man auch Passworttresore, weil in ihnen Passwörter sicher verschlüsselt aufgehoben - gespeichert - werden.

Online Passwortmanager haben den Vorteil, dass man sie mit allen Geräten nutzen kann, mit denen man einen Online-Zugang hat. Ihr Nachteil ist, dass praktisch „jeder“ auf sie zu- und sie damit angreifen kann.

Die von uns erwähnten Passwortmanager sind:

- ProtonPass [**ProtonPass**] ist ein **online** Passwortmanager. Damit kann man ihn mit allen Geräten nutzen, die einen Onlinezugang haben. ProtonPass ist ebenfalls Open Source Software [**OpenSource**].

- Bitwarden [**Bitwarden**] ist ein **online** Passwortmanager, der von sich behauptet, derjenige zu sein, dem die meisten Nutzer vertrauen. Man kann ihn ebenfalls mit allen Geräten nutzen, die einen Onlinezugang haben.

  Anmerkung:
  Bitwarden ist ein amerikanisches Produkt. Auf Grund der aktuell schwierigen politischen Situation in den USA, sollte man sich genau überlegen, ob man für seine Passwörter ein amerikanisches Produkt nutzen will, denn „Ausländer“ genießen in den USA faktisch **keinen** Datenschutz.

Zurück zu Passwortmanagern: 1.3

2.4 VPN

Ein **VPN - Virtual Private Network [VPN]** sorgt für Ihre Privatsphäre beim Surfen. Wenn Sie eine Website ohne VPN aufrufen, passiert Ihre Anfrage sehr viele Zwischenstationen. Diese können alle mitlesen und vor allem -schreiben, wer da welche Seite aufruft. Somit kann ein Profil von Ihnen erstellt werden. Gleiches gilt für die Betreiber der Websites.

Wenn Sie ein VPN einsetzen, hat das mehrere Vorteile. Zum einen geht Ihre Anfrage direkt von Ihrem Smartphone **verschlüsselt** direkt an einen Server, der die Website aufruft. Dieser Server ist ein Server Ihres VPN-Anbieters. Da von diesem Server viele tausend Anfragen ins Internet gehen, ist nicht mehr nachvollziehbar, wer diese Website aufrufen will. Die Zwischenstationen und die Website sehen als „Aufrufer“ den Server des VPN-Anbieters.

In der Regel betreiben VPN-Anbieter weltweit viele Server. Sie können sich daher aussuchen, über welchen Server Sie ins Internet gehen wollen. Damit verbergen Sie Ihren tatsächlichen Aufenthaltsort. Sie könnten sich also in

Schleswig-Holstein, Lübeck, befinden, gehen aber über einen Server in Kroatien in das Internet. Dann sieht es so aus, als wenn ein kroatischer Nutzer eine Website aufruft. Wenn Sie das verwirrend finden, haben Sie in der Regel die Wahlmöglichkeit „den schnellsten“ oder einen „zufälligen“ Server zu verwenden. Wenn Sie diese Funktion im Laufe einer Zeitspanne öfter anklicken, sorgen Sie bei den Schnüfflern für noch mehr Verwirrung.

Damit haben Sie die Möglichkeit, regional beschränkte Angebote wahrzunehmen. Seien dies Filme, auf die der Zugriff regional beschränkt ist, Karten für Veranstaltungen, die regional begrenzt verkauft werden oder viele andere Dinge. Manchmal erkennen Websites, dass Sie über ein VPN surfen. Dann kann es helfen - bei ProtonVPN - den so genannten Stealth-Mode [**StealthMode**] zu verwenden, der versucht, zu verschleiern, dass Sie über ein VPN surfen. Alternativ könnten Sie gezielt einen Server des Landes Ihrer Wahl einsetzen, der eine möglichst geringe Auslastung hat. Dann könnte es sein, dass dieser noch nicht als VPN-Server bekannt ist.

Es ist jedoch wichtig, sich für einen vertrauenswürdigen Anbieter zu entscheiden, der Ihre Daten nicht mitschreibt, da sonst ein detailliertes Profil von Ihnen erstellt werden könnte. Ich vertraue den beiden nachfolgenden VPN-Anbietern.
Zurück zu VPN: 1.4

2.4.1 ProtonVPN

ProtonVPN [**ProtonVPN**] ist ein Angebot der **Proton Foundation** [**ProtonFoundation**]. Proton ist eine schweizerische Stiftung [**WerWirSind**]. Um ProtonVPN auf dem Smartphone nutzen zu können brauchen Sie die ProtonVPN-App [**ProtonVPNApp**]. ProtonVPN [**ProtonVPN**] gibt es in einer kostenlosen und einer bezahlten Version. Die kostenlose Version bietet nur wenige Länder an, über die Sie ins Internet gehen können. Außerdem ist die Datengeschwindigkeit etwas reduziert. Wenn Sie sich für die bezahlte Version entscheiden, haben Sie die Möglichkeit den Stealth Mode zu nutzen. Das kann bei einigen Websites notwendig sein, weil nicht alle Websites ihre Inhalte an ein VPN preisgeben. Das sind dann Seiten, die von ihren Nutzern möglichst viele und genaue Informationen sammeln möchten. Weitere Funktionen der bezahlten Version sind „NetShield“ [**NetShield**] und „Kill Switch“ [**KillSwitch**].

NetShield [**NetShield**] ist eine Funktion, die automatisch bekannte Malware blockiert, so dass sie gar nicht erst auf Ihrem Smartphone ankommt. Zusätzlich blockiert diese Funktion auch Werbung, was das Surfen nicht nur angenehmer, sondern auch schneller machen soll. Denn dann steht die Bandbreite für den Datenstrom den Daten zur Verfügung, die Sie sehen möchten.

Kill Switch [**KillSwitch**] ist ein Begriff der an dieser Stelle etwas großspurig erscheint. Eigentlich ist damit die „Notabschaltung“ des Internetzugangs ganzer Länder gemeint. Bei Proton [**WerWirSind**] bedeutet es, dass Ihre Internetverbindung unterbrochen wird, falls Ihr VPN-Zugang gestört ist. Damit vermeiden Sie, unbewusst ohne VPN zu surfen.
Zurück zu ProtonVPN: 1.4

2.4.2 Mullvad

Mullvad ist eine schwedische Firma [**MullvadWerWirSind**], die einen guten Ruf geniesst. Hier gibt es einen Tarif für alles [**MullvadPreise**]. Mullvad bietet Ihnen die Möglichkeit deren Services monatlich in Anspruch zu nehmen. Egal wie lange Sie Mullvad nutzen, sie zahlen immer 5 €/Monat (Stand: Juli 2025) [**MullvadPreise**]. Mullvad bietet einen Überblick über seine Server und deren aktuellen Zustand [**MullvadServer**]. Hier können Sie auch sehen, welche „Nachrichten“ Server aktuell haben. Das ist ein großes Maß an Transparenz für Nutzer.

Anmerkung: Für alle gängigen Betriebssysteme gibt es Mullvad auch als Browser. Für Firefox gibt es Mullvad als Add-on [**MullvadBrowser**].
Zurück zu Mullvad: 1.4

2.4.3 NYM

Das Besondere an **NYM** ist, dass die Nachrichten über Server (Nodes) geleitet werden, die Freiwillige zur Verfügung stellen. Der Datenverkehr ist vollständig verschlüsselt und niemand, außer den berechtigten Personen, kann darauf zugreifen, also auch nicht die Betreiber der Server. Das macht einen potentiellen Angriff erheblich schwerer als, wenn die Daten über zentrale Server fließen.

Zusätzlich bietet NYM ein **Mixnet** [**Mixnet**] an. Das Mixnet funktioniert wie hier im Vergleich zum TOR-Netzwerk [**TOR**] und einem „normalen“ VPN [**VPN**].

Das **NYM-Mixnet** arbeitet nach Maßgabe der Entwicklung von **David Chaum**, der die Architektur im Jahr 1981 entwickelt hat. Neben der IP-Adresse und dem Standort, die verborgen werden, verschleiert das NYM-Mixnet auch **Metadaten** [**Metadaten**]. Dafür nutzt es folgende drei Techniken

1. es fügt **Dummy-Pakete** zum Datenstrom hinzu - Pakete ohne Inhalt
2. es modifiziert die Übertragunszeiten

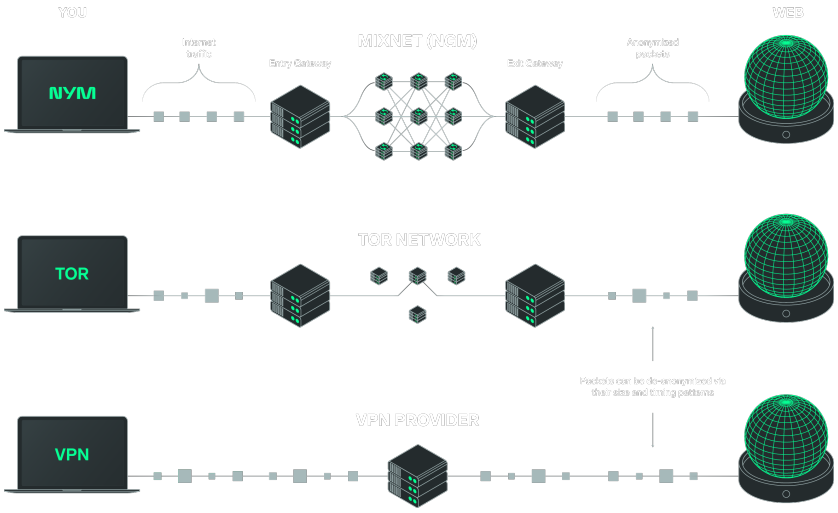

Abbildung 1: Das NYM-Mixnet im Vergleich zu TOR und VPN

3. es verändert die Größe der Pakete

Durch diese Maßnahmen erhöht das NYM-Mixnet den Schutz der Daten deutlich.
NYM ist anonym nutz- und bezahlbar. *Zurück zu NYM: 1.4*

2.5 DNS - Domain Name System

Das DNS - Domain Name System wandelt Namen von Websites wie *https://www.th-luebeck.de* in eine so genannte IP-Adresse um. Hier würde diese 193.175.120.221 lauten. Das ist notwendig, um sicher zu stellen, dass Nutzer möglichst immer dort landen, wo sie hinwollen. Unterschiedliche Alphabete, die es weltweit gibt, würden es sonst schwer machen, die gewünschten Websites zu erreichen. Diese Namensumwandlung sollte verschlüsselt geschehen, damit „Lauscher“ nicht mitbekommen, wer sich für welche Website interessiert, um mit diesen Informationen Profile der Nutzer zu erstellen.

Dabei kann es immer mal passieren, dass ein DNS-Server ausfällt. Für diesen möglichen Fall, sollte man einen zweiten, vielleicht auch dritten DNS-Server in seinen Einstellungen eingetragen haben, da sonst keine Namensauflösung durchgeführt werden kann und man dann nicht mehr im Internet surfen könnte, ohne großen Aufwand zu betreiben. In diesem Fall müsste man nämlich immer die IP-Adressen als Ziel im Browser eintragen.
Zurück zu DNS: 1.5

2.5.1 DNS4EU

DNS4EU [**DNS4EU**] ist ein von der EU gefördertes Projekt, das ebenfalls das Ziel hat, es Nutzern möglich zu machen, unbeobachtet Websites aufzurufen. Darüber hinaus bietet DNS4EU DNS-Server an, die Seiten blockieren, die

- für Kinder ungeeignet sind [**KiSchu**]
- Werbung blockieren [**AddBlock**]
- Kinderschutz und Werbeblocker [**ChildAddBlock**]
- ungefiltertes unbeobachtetes Surfen möglich machen [**Unfiltered**]

Wie diese Server eingerichtet werden erklärt DNS4EU hier [**DNSSetup**].
Zurück zu DNS: 1.5

2.5.2 MullvadDNS

Mullvad bietet einen so genannten Anycast [**Anycast**] an. Das heißt, dass eine ganze Gruppe von Servern die gleiche IP-Adresse nutzt und Anwender immer zu dem für sie am nächsten gelegenen Server geleitet werden. Wenn also bei Mullvad mal ein DNS-Server ausfällt, dürfte ein Nutzer dies kaum merken. Mullvad bietet die Möglichkeit unterschiedliche Webinhalte zu blockieren. Hierzu gehören

- Werbung [**MullvadDNS**]
- Tracker [**MullvadDNS**]
- Malware [**MullvadDNS**]
- Inhalte ab 18 Jahren [**MullvadDNS**]
- Online Casinos [**MullvadDNS**]
- Social Media [**MullvadDNS**]

Je nachdem welchen der angebotenen Server Sie wählen, erhalten Sie die aufgeführten Services, oder surfen gänzlich ungefiltert, aber mit verschlüsselter DNS-Auflösung. Als zusätzlichen Sicherheitsfaktor verkürzt Mullvad die übertragenen Anfragen so weit, wie es möglich ist, um einen Aufruf einer Website noch möglich zu machen. Damit wird nur ein Minimum an Daten von Ihnen weitergeleitet.
Zurück zu DNS: 1.5

2.5.3 quad9

quad9 [**quad9**] ist eine schweizer Stiftung, die das Ziel hat, unbeobachtete Aufrufe von Websites zu ermöglichen. Dabei werden angeforderte Seiten mit einer im Minutentakt aktualisierten Blacklist von Websites verglichen. So strebt quad9 an, Geräte vor Malware, Phishing und Werbung zu schützen. Bei der Gründung von quad9 im Jahr 2017 lag eine „Charta“ zum Schutz privater Daten zu Grunde [**quad9**]. Die Server von quad9 arbeiten nach eigenen Angaben DSGVO-konform.
Zurück zu DNS: 1.5

2.6 Der „richtige“ Browser

2.6.1 Brave

Brave [**Brave**] ist ebenfalls ein Open Source [**OpenSource**] Browser, der als besonders sicher gilt. Er bietet die Möglichkeit ein integriertes VPN - Virtual Private Network [**VPN**] zu nutzen. Zusätzlich hat Brave einen integrierten Zugang zum **Tor Netzwerk** [**TOR**].
Zurück zu Browser: 1.6

2.6.2 DuckDuckGo

DuckDuckGo ist am 25. September 2008 gegründet worden. Am 15. März 2010 haben sich die Entwickler dafür entschieden, eine Suchmaschine zu gestalten, die Privatsphäre an erste Stelle setzt. Seither hat sich diese Entwicklung kontinuierlich fortgesetzt. Den Verlauf der Geschichte von DuckDuckGo kann man auf deren Website [**DuckDuckGoÃIJberUns**] nachvollziehen.
Zurück zu Browser: 1.6

2.6.3 Firefox

Firefox ist ein Browser, der von der Mozilla Foundation [**MozillaFoundation**] bereitgestellt wird. Er ist ein Open Source Programm [**OpenSource**]. Allgemein gilt Firefox als vertrauenswürdig.
Zurück zu Browser: 1.6

2.6.4 Startpage

Startpage ist ein Unternehmen, das seinen Sitz in den Niederlanden hat. Deshalb unterliegt es den strengen Regeln der DSGVO. Im 2006 hat Startpage die erste anonyme Suchmaschine überhaupt entwickelt. Ziel des Unternehmens ist der Schutz der Privatsphäre von Menschen. Startpage bietet drei Produkte an

1. Startpage Privatsphäre Schutz - legt Startpage als Standardsuchmaschine fest und blockiert Cookies und Tracker.

2. Anonyme Suchmaschine Startpage - sorgt für eine Suche ohne Tracking und profilierten Suchverlauf.

3. Anonyme Ansicht - dieses Produkt verspricht, dass man Websites betrachten kann, ohne Spuren zu hinterlassen und ohne von Trackern verfolgt zu werden.

Zurück zu Browser: 1.6

2.7 Add-Ons

2.8 Firefox MultiAccount-Containers

Das Add-On Firefox MultiAccount-Containers [**MultiAccount**] öffnet Websites in „Containern“. Es gibt vorgegebene Container, aber Sie können auch beliebig viele selbst benannte Container erstellen. Um die Erkennung zu erleichtern stehen Ihnen Pictogramme und Farben zur Verfügung.

Der Vorteil der Container ist, dass Websites außerhalb des von Ihnen definierten Containers keinen Zugriff auf die Daten der Websites innerhalb des Containers haben. Wenn Sie eine Website zum ersten Mal nach der Installation dieses Add-ons öffnen, weisen Sie die Site einem von Ihnen bestimmten Container zu. Ab diesem Zeitpunkt wird die betreffende URL immer in dem von Ihnen festgelegten Container geöffnet.
Zurück zu Add-Ons: 1.7

2.9 Temporary Containers

Das Add-On Temporary Containers [**Temporary**] öffnet jede Website die Sie aufrufen in einem eigenen „Container“. Somit hat keine Website Zugriff auf die Daten einer anderen von Ihnen geöffneten Website. Allerdings löscht Temporary Containers alle Websitedaten nach 15 Minuten Inaktivität. Daher ist es sinnvoll, Seiten, die Sie länger benutzen wollen, in einen Container von Firefox Multi-Account Containers [**MultiAccount**] zu legen.
Zurück zu Add-Ons: 1.7

2.10 User-Agent Switcher and Manager

Das Add-On User-Agent Switcher and Manager [**UserAgent**] macht es Ihnen möglich, nach außen hin mit veränderten Angaben zu Ihrem Betriebssystem, Browser und Ähnlichem zu erscheinen. Damit verfälschen Sie Ihren „Browser Fingerprint“. Überprüfen können Sie das mit Hilfe der Websites Am I Unique [**AmIUnique**] der EFF (Electronic Frontier Foundation und der Website Browser Leaks [**BrowserLeaks**].
Zurück zu Add-Ons: 1.7

2.11 TOR

Wenn Sie TOR nutzen sollten Sie einiges beachten.

- Nutzen Sie es nicht zu oft, damit Sie nicht über die „Exit-Nodes“ - die Ausgangsserver - zu genau beobachtet werden können. Es könnte sein, dass Sie sonst deanonymisiert werden könnten.
- Nutzen Sie TOR nur mit einem VPN, da man sonst Ihren Datenverkehr von Ihrem Rechner zum Eingang in das TOR-Netzwerk abhören könnte.
- Nehmen Sie im TOR Browser keine Anpassungen vor, da Sie sonst ein individuelles Bild nach außen abgeben, das Sie leichter identifizierbar macht. Nutzen Sie TOR, wie er ausgeliefert wird.

Zurück zu TOR: 1.8

2.12 Tails

Tails [**Tails**] ist ein so genanntes Live Betriebssystem. Sie installieren es auf einem Datenträger (USB-Stick, SD-Karte, externe HD/SD). Wenn Sie es an einen Ihnen fremden Rechner anschließen und von diesem Speichermedium starten, können Sie ohne Spuren zu hinterlassen, im Internet surfen. Tails verwendet TOR als Browser und bietet **keine** Möglichkeit, Daten zu speichern. So haben Sie die Möglichkeit, auch auf fremden Rechnern sicher zu surfen. *Zurück zu Tails: 1.9*

2.13 Digitale Souveränität

Digitale Souveränität beinhaltet sehr viel. Unabhängigkeit von Techriesen, Unabhängigkeit von Regierungen oder Einrichtungen. Am besten können Sie diese umsetzen, indem Sie Opern Sourc Software verwenden. Statt Outlook Thunderbird [**Thunderbird**]. Statt Windows ein Linux Betriebssystem. Hier bieten sich an Ubuntu [**Ubuntu**], Debian [**Debian**] oder Linux Mint [**LinuxMint**]. Debian enthält kaum proprietäre Software, im Gegensatz zu Ubuntu, dafür ist Ubuntu gerade für Einsteiger leichter zu bedienen. Linux Mint benötigt nur sehr knappe Ressourcen.

Versuchen Sie digital so souverän wie möglich zu sein. Am besten mit so viel wie möglich Open Source Software. *Zurück zu Digitale Souveränität 1.10*

2.14 Nutzung von KI/AI - künstlicher Intelligenz

Wenn Sie künstliche Intelligenz nutzen, werden Ihre persönlichen Daten, Suchanfragen und viele technische Informationen protokolliert, profiliert und zum Training der verwendeten KI eingesetzt. Dem sollten Sie in den Einstellungen der jeweiligen KI widersprechen, bevor Sie anfangen zu suchen, oder Sie sollten anonyme KI verwenden, die Ihre Privatsphäre schützen. Die beiden folgenden Anbieter versprechen glaubwürdig, Ihre KI-Suchen anonym zu halten

- DuckDuckGo mit Duck.ai [**DuckAI**]
- Lumo (KI von Proton) [**Lumo**]

Weitere Unternehmen, die anonyme KI anbieten sind

- Anonchatgpt [**Deepgram**]
- Venice [**Venice**]

Beide Unternehmen sind amerikanische Unternehmen, was in jedem Fall Vorsicht gebietet, da Sie als Ausländer in den USA **keinen** Datenschutz genießen. Die Website Venice [**Venice**, **VeniceTermsOfService**] verspricht ebenfalls anonymes und uneingeschränktes Wissen. Es handelt sich hierbei jedoch um ein amerikanisches Unternehmen, weshalb äußerste Vorsicht und eher Zurückhaltung geboten ist. Der Name soll Kultur und europäische Verbundenheit suggerieren, was durch lateinische Sprüche unterstrichen wird. Dennoch ist die tatsächliche Intention nicht ohne weiteres klar.
Zurück zu Nutzung von KI/AI - künstlicher Intelligenz: 1.11

2.15 2FA - Second Factor Authentication

Im englischen ist es einfach die Funktion zu beschreiben - authentication. Im Deutschen ist dies etwas schwieriger, denn eine **Authentifikation** bedeutet, dass sich eine Person als solche „ausweisen“ kann. Wenn **innerhalb des Systems** geprüft werden muss, ob genau diese Person Zugriff berechtigt ist, spricht man von **Authentisieren**.

Ich behandele hier zwei Möglichkeiten der Authentisierung, denn genau das findet hier statt. Es ist „egal“ ob die Person die Zugriff auf ein digitales Konto haben will, eine bestimmte Person ist. Entscheidend ist, ob diese Person berechtigt ist, auf das Konto (Account) zuzugreifen. Das wird mit Hilfe zweier Faktoren (2FA) [**2FA**] überprüft:

1. Passwort
2. (in diesem Fall) Code oder Token

Eine einfache und mit der richtigen App sichere Methode ist der Einsatz einer Authenticator App. Um eine Authenticator App nutzen zu können, muss man einmalig bei dem Konto, bei dem man sich anmelden möchte, in den Einstellungen festlegen, dass man diese Methode nutzen will. Anschließend scannt man mit dem Smartphone - aus der Authenticator App heraus - einen QR-Code [**QR-Code**], den das betreffende Konto anzeigt. Über diesen Code findet eine Synchronisation zwischen der App auf dem Smartphone und dem Anbieter des Kontos, zu dem der Zugang gehört, statt.

App und Anbieter des Kontos erzeugen zeitgleich Zahlencodes, die in der App angezeigt werden. Zur Authentisierung muss man den Zahlencode eintragen. Wenn es der richtige ist, findet die Freischaltung statt. So ein Zahlencode gilt in der Regel bis zu einer Minute. Das reicht für einen Eintrag aus.

Alle von uns genannten Authenticator Apps sind Open Source [**OpenSource**] und gelten als sicher und zuverlässig. Einige Authenticator Apps übertragen die Zugangscodes unverschlüsselt oder senden diese sogar an Tracker, so dass die Authentisierung unsicher wird.

Noch sicherer ist die Authentisierung mit einem **Token** [**Token**], weil man in diesem Fall über ein „Stück Hardware“ verfügen muss. Dies muss ein Token sein, der **NFC - Near Field Communication** [**NFC**] beherrscht, eine Form des „Kurzstrecken Funks“. Hier geht es um wenige Zentimeter Reichweite. Diese Option spielt vor allem für den Zugang zu Passwortmanagern eine Rolle.

Um die Authentisierung mit einem Token nutzen zu können, muss der Passwortmanager, oder das Konto um das es geht, sie anbieten und es muss eine Synchronisation mit dem Token stattgefunden haben. Ist das der Fall, reicht es aus, dass man nach Eingabe des Passworts den Token über das Display des Smartphones führt. Anschließend wird der Passwortmanager oder das Konto freigeschaltet. Voraussetzung ist ein Smartphone, das NFC beherrscht. Bei modernen Smartphones sollte das jedoch keine Frage sein.

Ich setze Token von:

- Nitrokey (deutsches Produkt) [**NitroKey**]
- Yubikey (amerikanisches Produkt) [**YubiKey**]

ein. Mehr über die Produkte und Firmen erfahren Sie hier [**NitroKey**, **NitroKeyÃIJberUns**, **NitroKeyNFC**, **NitroKeyToken**, **YubiKey**, **YubiKeyÃIJberUns**, **YubiKeyToken**, **YubiKeyProdukte**]
Zurück zu 2FA - Second Factor Authentication: 1.12

2.16 Für jeden Account eine eigene E-Mailadresse

E-Mailrelays [**DuckDuckGoRelayErklÃd'rt**] empfangen E-Mails und leiten diese weiter. In diesem Fall an eine von Ihnen vorgegebene E-Mailadresse. Das kann gern Ihre private E-Mailadresse sein, denn es erfährt niemand, wohin die E-Mail weitergeleitet wird.

Die Anbieter die ich dafür nutze sind DuckDuckGo [**DuckDuckGo**] und SimpleLogin [**SimpleLogin**]. DuckDuckGo ist eine amerikanische Stiftung, die sich der Wahrung der Privatsphäre verschrieben hat. Um dieses E-Mailrelay [**DuckDuckGoRelayErklÃd'rt**] nutzen zu können, müssen Sie sich online bei DuckDuckGo [**DuckDuckGoEmailProtection**] hierfür registrieren. Anschließend laden Sie sich für Ihr Smartphone die passende App herunter - Android [**DuckDuckGoExtensionAndroid**] - oder für iOS [**DuckDuckGoExtensioniOS**]. Sobald Sie diese Schritte erledigt haben, erscheint in Ihrem Browser bei der Registrierung für ein neues Konto im Feld für die E-Maileingabe am rechten Rand das Logo von DuckDuckGo - eine Ente im roten Kreis. Wenn Sie darauf klicken, schlägt DuckDuckGo Ihnen eine E-Mailadresse vor. Sie können diese sofort annehmen, denn es spielt keine Rolle, wie diese lautet. Die Nachrichten dorthin gelangen immer auf das von Ihnen vordefinierte Konto. Erhalten Sie hierüber eine E-Mail, können Sie automatisch mit diesem Absender auch antworten. So kann niemand sehen, dass hinter verschiedenen Anmeldungen ein und die selbe Person steckt. Es erfährt also niemand, dass Sie sich für Schuhe, Uhren und Kosmetik interessieren, sondern immer nur, dass Sie sich für eines dieser Dinge interessieren.

Auf die gleiche Art und Weise funktioniert SimpleLogin [**SimpleLogin**]. Auch für SimpleLogin gibt es ein Firefox Add-on [**SimpleLoginAddOn**], eine Android-App [**SimpleLoginAndroid**] und eine iOS-App [**SimpleLoginiOS**]. Im Gegensatz zu DuckDuckGo ist SimpleLogin ein Schweizer Unternehmen, das zu Proton [**ProtonLogin**] gehört. Mit SimpleLogin haben Sie umfangreiche Möglichkeiten ihre Alias-E-Mailadressen zu konfigurieren. Es gibt eine kostenlose Version und eine Bezahlversion [**SimpleLoginPreise**]. Ein Blick darauf lohnt sich.
Zurück zu Für jeden Account eine eigene E-Mailadresse: 1.13

2.17 Kalender

Kalender enthalten oftmals eine Fülle an persönlichen Informationen, die niemanden etwas angehen. Daher sollten die Einträge dort auch Ende-zu-Ende-verschlüsselt [**E2EE**] sein. Die standardmäßig auf Smartphones vorinstallierten Kalender bieten Ihnen oft den - eher zweifelhaften - Service an, dass Ihnen Empfehlungen für Orte, die Sie in Ihre Kalender eingetragen haben, gemacht werden. Das bedeutet, dass Ihre Einträge von Dritten mitgelesen werden. Das ist nicht gut, denn aus diesen Informationen können präzise Profile von Ihnen erstellt werden.

Ich nutze den Kalender von Proton [**ProtonKalender**], den es auch als App [**ProtonKalenderApp**] gibt. Er ist auch als Webkalender aufrufbar [**ProtonLogin**].
Erläuterungen zu Kalender: 1.14

2.18 Speicher

Wenn Sie die Dateiverschlüsselung Ihres Betriebssystems verwenden, verschlüsselt diese Ihre gesamte Festplatte (SD). Sobald Sie sich an ihrem Rechner anmelden, wird der gesamte Inhalt der Festplatte entschlüsselt. Das birgt die Gefahr, dass ein potentieller „Eindringling“ Zugriff auf alle Ihre Daten erhält. Um dieses Risiko zu minimieren, ist es sinnvoll, vertrauliche Daten mit dem Programm VeraCrypt [**VeraCrypt**] zu verschlüsseln. Dafür erstellen Sie mit VeraCrypt „Container“, in denen Sie die vertraulichen Daten speichern. Die Container öffnen Sie nur bei Bedarf. Am besten legen Sie jede vertrauliche Datei in einen einzelnen Container, damit bei einem potentiellen Angriff so wenig wie möglich Daten kompromittiert werden. Die VeraCrypt Container können Sie wie „normale“ Dateien kopieren und „transportieren“. VeraCrypt ist kostenlose Open Source Software. *Zurück zu Speicher:1.15*

2.19 Speichermedien

USB-Speicher enthält eigene Mikroprozessoren. Das macht es möglich, dass aus einem einfachen Speichermedium eine „USB-Tastatur“ wird. Das, was die Tastatur eingeben soll, programmiert der Angreifer vorher an seinem Rechner. Anschließend reicht es aus, dass ein entsprechender BadUSB an Ihren Rechner angeschlossen wird, damit innerhalb von Mikrosekunden Schadcode auf Ihren Rechner gelangt.

SD-Karten hingegen haben „nur“ Speicherfunktionen. Daher sollten Sie **nie** zulassen, dass jemand ein USB-Gerät an Ihren Rechner anschließt. Selbstverständlich dürfen Sie das selbst mit unbekannten Geräten auch nicht machen.

Wenn Sie sich ein Bild davon machen möchten, wie ein BadUSB funktioniert, können Sie das selbst ausprobieren. Das „Quasi-Synonym“ für BadUSB ist der RubberDucky [**RubberDucky**]. Den Rubber Ducky bietet die amerikanische Firma HAK5 [**HAK5**] an. Um ihn zu programmieren, muss man einen online Compiler von HAK5 benutzen. Man sollte sich überlegen, ob man dem Compiler einer Firma vertraut, die ausschließlich Werkzeug für Spionage anbietet.

Eine sehr viel kostengünstigere Alternative zum Rubber Ducky (169,- € Stand Mai 2026) ist der PicoUSB [**BerryBase**] den Sie für 8,90 € (Stand Mai 2026) bei Berry Base [**BerryBase**] erhalten. Der Installationsaufwand ist geringfügig größer, aber Sie können Ihre Programme dafür lokal nutzen und müssen nichts online kompilieren. *Zurück zu Speichermedien:1.16*

2.20 Anbieter für Technik die Ihre Kommunikation gefährden kann

Einige der vielen Anbieter für Technik die Ihre Kommunikation gefährden kann sind

- ATG Kriminaltechnik [**ATGKriminaltechnik**]
- BerryBase [**BerryBase**]
- Hacker Warehouse [**hackerWarehouse**]
- HAK 5 [**HAK5**]
- Lab404 [**lab404**]

2.21 Cloudspeicher

Cloudspeicher bietet die Möglichkeit, von überall und unterschiedlichen Geräten auf Daten zuzugreifen. Gleichzeitig, stellt er die Gefahr dar, dass Unbefugte auf Ihre Daten zugreifen könnten, weil sie die Server des Speicheranbieters kompromittieren.

Daher ist es wichtig, dass auch hier Ihre Daten Ende-zu-Ende-verschlüsselt [**E2EE**] sind, denn mit sicher verschlüsselten Daten kann kein Angreifer etwas anfangen. Wichtig ist auch, dass Sie sich nicht auf einen einzigen Anbieter verlassen, denn es kann immer vorkommen, dass Server kaputt gehen, oder Ihre Daten „einfach“ beschädigt werden. Deshalb sollten Sie Ihre Daten immer bei zwei unterschiedlichen Anbietern speichern.

Ebenso wichtig ist es, dass Sie Ihre Daten **nicht** bei M365 speichern, denn Microsoft indexiert alle dort gespeicherten Daten. Das heißt, dass Ihre Daten dort **nicht mehr** vertraulich sind. Erst ab Mai 2026 soll es die Möglichkeit geben, dass Nutzer einstellen können, dass ihre Daten nicht indexiert werden. Das heißt aber nicht, dass Microsoft nicht dennoch darauf zugreift.

Ich nutze die folgenden Anbieter, um meine Daten zu sichern:

1. ProtonDrive [**ProtonDrive**] mit der ProtonDrive App [**ProtonDriveApp**]
2. Tresorit [**TresorIT**] mit der TresorIT App [**TresorITApp**]

Anmerkung:
Beide Anbieter stellen auch Desktop Apps zur Verfügung, die den Cloudspeicher in Ihren „Dateiexplorer“ integrieren, so dass Sie darauf wie auf ein „normales“ Laufwerk zugreifen können. In den Apps dieser Anbieter können Sie auch eine automatische Echtzeitsicherung einstellen. Dabei legen Sie fest, welche Dateien oder Ordner Sie sichern möchten. Sobald an diesen eine Änderung stattfindet, werden diese Änderungen in Echtzeit an die Cloudspeicher übertragen. Da nur die Änderungen übertragen werden, spart man einiges an Cloudspeicher, denn so vermeidet das System Doppelungen. Man nennt dieses Vorgehen inkrementell [**Inkrement**].
Zurück zu Cloudspeicher: 1.18

2.22 Backups

Unentbehrlich sind Backups Ihrer Daten, denn ein Rechner kann gestohlen werden, kaputt gehen, eine Software kann kompromittiert werden.

Empfehlenswert sind inkrementelle Backups in Echtzeit. Verlassen Sie sich nie auf nur eine Backup-Quelle, sondern richten Sie immer mindestens zwei von einander vollständig unabhängige Backup-Orte ein. Wichtig ist es, dass Ihre Backups vor der Sicherung verschlüsselt werden und erst dann das Sicherungsmedium erreichen. Eine inkrementelle Sicherung spart Speicherplatz und Zeit, denn inkrementell bedeutet, dass nur Änderungen, aber nicht der gesamte Datenbestand gesichert werden.

Ich nutze für Backups ProtonDrive [**ProtonDrive**] mit der entsprechenden App. In der ProtonDrive App können Sie einstellen, welche Dateien oder Ordner automatisch in Echtzeit gesichert werden sollen. Die Daten werden Ende-zu-Ende verschlüsselt in die Schweiz übertragen, wo Sie ein hohes Maß an Datenschutz genießen. Zur Sicherheit sollten Sie mehr als ein Backup vorhalten. Alternative Anbieter für Echtzeitsicherungen sind TresorIT [**TresorIT**] und der deutsche Anbieter Tuta [**TutaSpeicher**], die auch verschlüsselten Cloudspeicher anbieten. Wenn Sie Linux als Betriebssystem nutzen, empfiehlt sich eine zusätzliche Sicherung mit dem Programm borgbackup [**BorgBackup**]. Wenn Sie es vorziehen, statt auf der Konsole graphisch zu arbeiten, können Sie dies im Zusammenhang mit dem Programm Borgmatic [**Borgmatic**] machen. Noch bequemer haben Sie es, wenn Sie Vorta [**Vorta**] nutzen. Als Speicheranbieter setze ich sowohl Hetzner [**Hetzner**] als auch BorgBase [**Borgbase**] ein. Eine Anleitung zur Installation und Konfiguration finden Sie bei Hetzner ebenfalls [**BorgBackupHowTo**]. *Zurück zu Backups: 1.19*

2.23 Messenger

Messenger gibt es viele. Die meisten von Ihnen sind aus Sicht des Datenschutzes zumindest kritisch zu betrachten. ich beschränke mich hier darauf, Messenger zu empfehlen, die ich selber nutze, weil ich sie für sicher und empfehlenswert halte. **Signal** [**Signal**] und **Threema** [**Threema**].

Eine ausdrückliche **Warnung** gilt dem Messenger **Telegram** [**Telegram**]. Telegram überträgt alle Daten die Sie dort eintippen in Echtzeit an die Firmen eigenen Server und speichert die Daten dort. Wo „dort“ ist, weiß niemand so genau. Privatsphäre gibt es bei Telegram nicht [**Telegram**], daher sollte man lieber Abstand davon nehmen diesen Messenger zu benutzen.

Signal [**Signal**] ist ein Messenger, der von einer amerikanischen Stiftung angeboten wird. Grundsätzlich ist es nicht zu empfehlen, amerikanische Pro-

dukte zu verwenden, aber Signal versichert glaubwürdig, dass es nur das Datum speichert, an dem jemand Signal installiert hat und das Datum der letzten Nachricht. Somit stehen keine kompromittierenden Informationen zur Verfügung, die amerikanische Behörden erlangen könnten.

Vorteil von Signal ist weiterhin, dass bereits viele Menschen es nutzen. Wenn Sie es auf Ihrem Smartphone installieren und zulassen, dass Signal auf Ihre Kontakte zugreift, werden Sie sich wundern, wieviele Ihrer Kontakte bereits Signal verwenden.

Threema [**Threema**] ist mindestens genauso sicher wie Signal, hat zusätzlich den Vorteil, dass es von einem schweizer Unternehmen angeboten wird. Damit unterliegt es strengen Datenschutzvorschriften [**DatenschutzSchweiz**].

Simplex [**Simplex**] ist ein Messenger der noch neu auf dem Markt ist. Er arbeitet dezentral, dass heisst, dass er kein Serverzentrum hat, sondern seine Server weit verteilt sind. Das macht es Angreifern schwerer, die Kommunikation zu belauschen.
Eine Besonderheit bei Simplex ist, dass Simplex eine Kommunikation nie bidirektional führt, Wenn Alice also eine Nachricht an Bob schickt, geht die Nachricht über Kanal Alpha. Die Antwort von Bob an Alice läuft jedoch über Kanal Beta. So kann im schlimmsten Fall nur ein Teil der Kommunikation mitgeschnitten werden. Die Nutzer haben die Möglichkeit selbst zu bestimmen, welche Kanäle sie nutzen, so dass unterschiedliche Kommunikationen über unterschiedliche Kanäle ablaufen. Die gesamte Kommunikation ist bei Simplex Ende-zu-Ende-Verschlüsselt. Die Verschlüsselung ist Quantensicher.
Eine wetiere Besonderheit von Simplex ist, dass ein Nutzer seinen Namen jederzeit wechseln kann. Wenn Alice mit Bob kommuniziert erscheint sie für Bob als Alice. Möchte Alice mit Charly kommunizieren, kann sie für Charly als Gemma erscheinen.
Einen Blick auf Simplex hat der renommierte Sicherheitsforscher Mike Kuketz geworfen. Um sich selbst ein Bild von Simplex zu machen, ist es hilfreich seinen Artikel dazu zu lesen [**Simplex_Kuketz**].

Allen gemeinsam ist, dass sie die Möglichkeit anbieten für

- Gruppenchats
- Telefonkonferenzen
- Kontaktaufnahme ohne Telefonnummer
  der Autor dieses Handouts ist zu erreichen unter
  - Signal - ITS_Nerd.01

  - Threema - WYH86UFA

- alle drei sind immer Ende-zu-Ende (E2EE - End-to-End-Encryption) [**E2EE**] verschlüsselt. Simplex ist sogar quantensicher (Post Quantum Cryptography - PQC [**BSI_PQC**] verschlüsselt.

- mit allen dreien kann man unbelauscht telefonieren

Zurück zu Messenger: 1.20

2.24 Unbelauscht telefonieren

Mit dem neuen Mobilfunkstandard 5G [**5G**] wird es schwieriger Telefonate zu belauschen. Aber viele Smartphones beherrschen diesen Standard noch nicht. Viele Verträge bieten ihn nicht an und es gibt noch viele Mobilfunkzellen, die nicht mit 5G funken. Daher ist es sinnvoll, so viele Telefonate wie möglich mit den Messenger Apps Signal [**Signal**], Simplex [**Simplex**] und Threema [**Threema**] zu führen, weil diese auch Telefonate Ende-zu-Ende-verschlüsseln [**E2EE**]. Dafür müssen beide Seiten die App installiert haben.
Zurück zu Unbelauscht Telefonieren: 1.21