Digitale Selbstverteidigung

Ein Kurz-Workshop

2023

Sicher kommunizieren

https://epicenter.academy/sicher-kommunizieren

E-Mail und SMS sind unsicher

E-Mails / SMS :

- **An allen Stationen, an denen Mails vorbeikommen, können deren Inhalt gelesen werden**
- **Ähnlich „geheim“ wie eine Postkarte**

Vergleich von E-Mail-Anbietern

Unterschiede :

- **Benutzen Mail-Anbieter die Inhalte der E-Mails dazu um Werbung anzuzeigen (Werbeprofile werden erstellt) ?**

Outlook, Gmail, Yahoo Mail, … :

Diese Mail-Anbieter

- **sind aus Datenschutz-Perspektive eher unsicher**
- **scannen oft die Inhalte der E-Mails, um damit Datenprofile anzulegen**
- **sitzen in den USA und sind damit in Reichweite amerikanischer Geheimdienste**

datenschutzfokussierte E-Mail-Anbietern:innen:

- haben ihren Sitz in der EU
- sind zwar nicht kostenlos, aber sie gehen sorgsam mit Informationen von und über ihre NutzerInnen um.

Denk daran:
Ist ein Dienst kostenlos, bezahlst du mit deinen Daten!

Sichere Kommunikation ?

- Unverschlüsselte Kommunikation
- Transportverschlüsselte Kommunikation
- Ende-zu-Ende-verschlüsselte Kommunikation

E-Mail mit Transportverschlüsselung

Transportverschlüsselung:

- **E-Mails werden über eine verschlüsselte Verbindung von einem Ort zum anderen transportiert**

Problem:

- **Die Inhalte sind zwar „unterwegs“ geschützt, aber nicht auf dem Server der Anbieter:in.**

Asymmetrische Verschlüsselung

Vorteil:

- **zwei Menschen können verschlüsselt kommunizieren, obwohl sie sich z.B. auf zwei unterschiedlichen Kontinenten befinden und einander noch nie gesehen haben**

- **Bei asymmetrischer Verschlüsselung besitzen die Kommunikationspartner:innen zwei Schlüssel:**
  - **Privater Schlüssel**
  - **Öffentlicher Schlüssel**


öffentlicher Schlüssel
Schlüsselpaar
privater Schlüssel
A$&03jö$ &fjs24sX 48Fg?jdfi93 a§“00 hfd- j93&/=
Klartext
verschlüsselter Text
Klartext

Tools und Dienste um verschlüsselt zu kommunizieren

- Sicher E-Mails schreiben: PGP im Mailprogramm nutzen
- Sichere Nachrichten schreiben: Messenger verwenden

Sicher im Internet surfen

Wie kann man sicher
im WorldWideWeb unterwegs sein ?

- **Browser**
- **Alternative Suchmaschinen**
- **Sichere Datenübertragung**
- **Anonym im Netz – kleiner Ausflug ins Darknet**

privatsphärefreundlicher Browser :

1. darf keine Nutzungsdaten an den Hersteller „verraten“
2. muss den/die Nutzer:in unterstützen, Werbetracker zu deaktivieren
3. Quellcode des Programms muss verfügbar sein ("Open Source")

Google Chrome

- **Google Chrome sammelt sehr viele Daten über Nutzer:innen**

→ deshalb wird von Google Chrome abgeraten

Mozilla Firefox

- **Firefox ist ein privatsphäre-freundlicher Browser.**
- **Geschäftsziel der NGO Mozilla Foundation ist der Browser selbst und nicht Werbeeinnahmen, die durch Daten und Tracking erwirtschaftet werden.**

Schutz vor Verfolgung

- **Browserverlauf**
- **Cookies**
- **Fingerprinting**

Schutz vor Verfolgung: Browserverlauf

- Der Browserverlauf enthält eine Liste aller Internetseiten, die besucht wurden
- Kann vom Benutzer gelöscht werden

Schutz vor Verfolgung: Cookies

Cookies sind bei manchen Webseiten nötig, da sie einige Spezial-Funktionen ermöglichen.

- **Beispiel:**
  Warenkorb beim Online-Shopping enthält Artikel

Schutz vor Verfolgung: Cookies

Cookies verfolgen Aktivitäten im Netz
→ Services sind plötzlich nicht mehr kostenfrei

- **Beispiel:**
  - **Online-Zeitungen z.B. erkennen Leser:innen am Cookie wieder und wollen beim zweiten Besuch plötzlich Geld für das Lesen eines Artikels.**

Schutz vor Verfolgung: Fingerprinting

**Anhand einzigartiger Merkmale des Web-Browsers und einiger anderer Einstellungen,
(wie etwa Sprache, Schriften, Bildschirmauflösung)
kann man wiedererkannt werden**

Browser-Erweiterungen gegen Tracking und Werbung:

- Privacy Badger, um Werbetracker auszuschalten und
- uBlock Origin, um Werbung zu blockieren

Alternative Suchmaschinen

Suchmaschine:

- **ist nie absolut,**
- **die angezeigten Ergebnisse enthalten stets eine Bewertung, was der eigenen Firmenpolitik nach wichtig und was weniger wichtig ist.**

Google

- **Google ist aktuell die mit Abstand meistgenutzte Suchmaschine der Welt.**

- **Die Suchergebnisse basieren auf einer Annahme:**
  - **was deine *Absicht* bei der Suche ist**
  - **oder wovon man möchte, dass du es findest**

Startpage

- **Startpage leitet die eingegebenen Suchanfragen anonymisiert an Googles Suchmaschine weiter und gibt deren Ergebnisse aus.**

DuckDuckGo

DuckDuckGo ist eine Suchmaschine, die ebenfalls keine persönlichen Informationen sammelt.

- **Anders als Startpage nutzt DuckDuckGo nicht Google als Quelle, sondern vor allem Microsofts Suchmaschine Bing und weitere Quellen wie Wikipedia sowie die Suchmaschinen Yahoo oder Yandex.**

Anonym im Netz mit Tor?

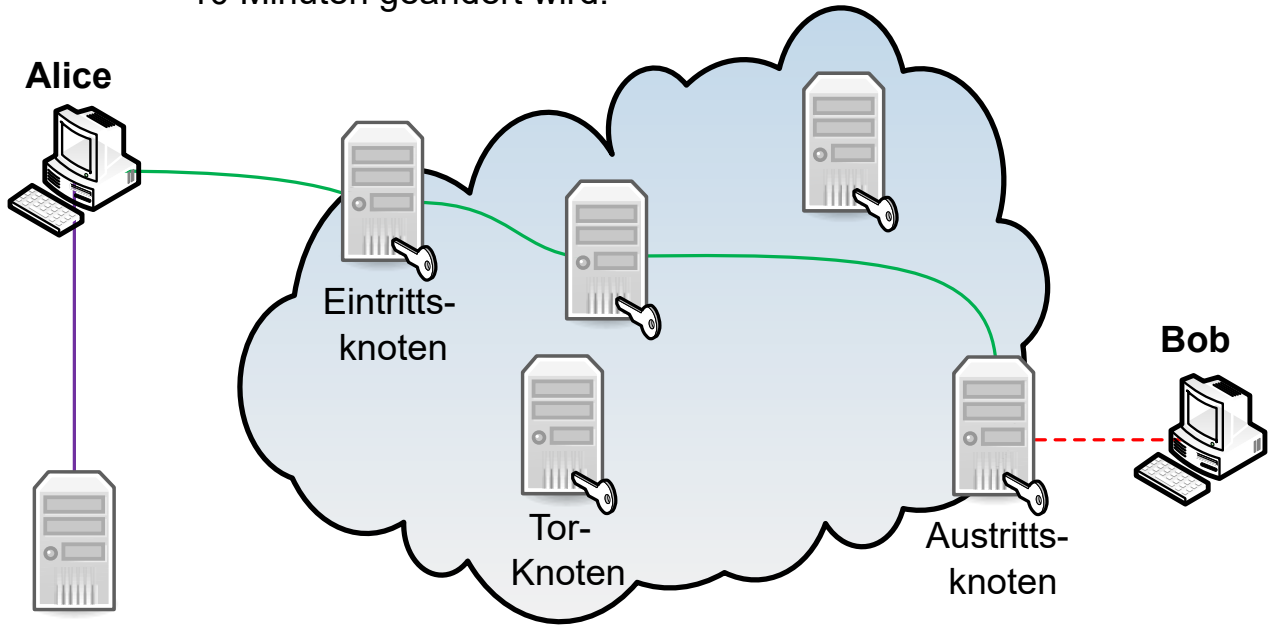
Tor = "The Onion Router"

- **wird in Ländern mit vollständiger Internetüberwachung häufig genutzt, um anonym und verschlüsselt kommunizieren zu können.**

Arbeitsweise von TOR

2. Der Client baut zum Ziel eine zufällige Route über drei Tor-Knoten auf, die alle 10 Minuten geändert wird.

1. Der Client lädt von einem Verzeichnisserver eine Liste aller nutzbaren Tor-Knoten herunter.

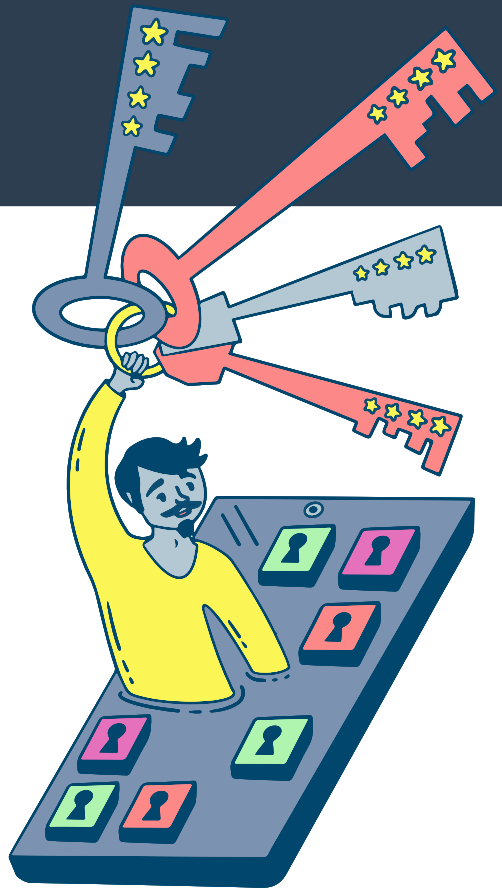


Nötig für das Tor-Netzwerk:

- **Tor-Browser oder**
- **Brave-Browser oder**
- **Tails-Betriebsystem**

Passwörter

https://epicenter.academy/passwoerter



Passwörter sind wichtig

Drei Arten der Authentifizierung:

- etwas, das man weiß – **Wissen**
- etwas, das man hat – **Besitz**
- und etwas, das man ist – **Biometrische Merkmale**

Die gängigste Methode der Authentifizierung ist das Passwort

Was macht ein sicheres Passwort aus?

Drei Arten der Authentifizierung

- etwas, das man weiß – **Wissen**
  - **Der Wissensfaktor kann jeder Authentifizierungsfaktor sein, der aus Informationen besteht, die der/die Nutzer*in kennt.**
  - **Beispiele:**
    - **eine persönliche Nummer (PIN),**
    - **ein Benutzername,**
    - **ein Passwort oder**
    - **eine Antwort auf eine geheime Frage.**
- etwas, das man hat – **Besitz**
- und etwas, das man ist – **Biometrische Merkmale**

Drei Arten der Authentifizierung

- etwas, das man weiß – **Wissen**
- etwas, das man hat **– Besitz**
  - **Ein Berechtigungsnachweis, der auf Gegenständen basiert, die man besitzen und bei sich tragen kann.**
  - **Beispiele:**
    - **Mobiltelefon (SMS oder Authentifizierungs-App)**
    - **RFID-Chip**
    - **Bankomatkarte**
- und etwas, das man ist – **Biometrische Merkmale**

Drei Arten der Authentifizierung

- etwas, das man weiß – **Wissen**
- etwas, das man hat – **Besitz**
- und etwas, das man ist **– Biometrische Merkmale**
  - **Man kann sich auch authentifizieren, indem ein eindeutiges Merkmal („Biometrie“) der zu authentifizierenden Person überprüft wird.**
  - **Beispiele:**
    - **Fingerabdruck,**
    - **Scans der Iris,**
    - **Form der Ohren oder**
    - **Verlaufsmuster der Venen in den Händen**
  - **Biometrische Merkmale sind NICHT veränderbar. Ein Nachweis für eine Zugriffsberechtigung sollte aber immer veränderbar sein, um auch sicher zu bleiben.**

Zwei Faktor Authentifizierung – 2FA

- Sicherheit erhöhen:
  unterschiedliche Arten der Authentifizierung kombinieren
  - z.B. Bankomatkarte (Besitz) und PIN (Wissen)

Zeit, die ein Hacker braucht, um ein Passwort zu erzwingen

ANZAHL DER ZEICHEN	NUR ZAHLEN	KLEINBUCHSTABEN	GROSS- & KLEINBUCHSTABEN	ZAHLEN, GROSS- & KLEINBUCHSTABEN	ZAHLEN, GROSS- & KLEINBUCHSTABEN, SYMBOLE
4	Sofort	Sofort	Sofort	Sofort	Sofort
5	Sofort	Sofort	Sofort	Sofort	Sofort
6	Sofort	Sofort	Sofort	1 sek	5 sek
7	Sofort	Sofort	25 sek	1 min	6 min
8	Sofort	5 sek	22 min	1 Stunde	8 Stunden
9	Sofort	2 min	19 Stunden	3 Tage	3 Wochen
10	Sofort	58 min	1 Monat	7 Monate	5 Jahre
11	2 sek	1 Tag	5 Jahre	41 Jahre	400 Jahre
12	25 sek	3 Wochen	300 Jahre	2 Tsd. Jahre	34 Tsd. Jahre
13	4 min	1 Jahre	16 Tsd. Jahre	100 Tsd. Jahre	2 Mio. Jahre
14	41 min	51 Jahre	800 Tsd. Jahre	9 Mio. Jahre	200 Mio. Jahre
15	6 Stunden	1 Tsd. Jahre	43 Mio. Jahre	600 Mio. Jahre	15 Mrd. Jahre
16	2 Tage	34 Tsd. Jahre	2 Mrd. Jahre	37 Mrd. Jahre	1 Bill. Jahre
17	4 Wochen	800 Tsd. Jahre	100 Mrd. Jahre	2 Bill. Jahre	93 Bill. Jahre
18	9 Monate	23 Mio. Jahre	6 Bill. Jahre	100 Bill. Jahre	7 Brd. Jahre

Passwort stehlen („Phishing“)

- es werden fingierte E-Mails mit vertrauenserweckender Aufmachung an die potentiellen Opfer versendet.
- Inhalt dieser Nachrichten kann z.B. sein, dass ein bestimmter Dienst, den man nutzt einen auffordert einem Link zu folgen und sich einzuloggen.

Datenbank stehlen

- Auch ganze Datenbanken von massenweise genutzten Diensten werden gestohlen.
- Oft sind Datenbanken durch einen Fehler der Betreiber:innen nicht ausreichend geschützt und deshalb leichte Beute.
- Diese Daten können weiterverkauft und/oder für weitere Angriffe genutzt werden.

Problem: Mehrfach verwendetes Passwort

- Mehrfach verwendete Passwörter erhöhen das Risiko massiv, da, wenn ein Passwort einmal in fremde Hände gelangt ist, auch mehrere Accounts betroffen sind.
- Manchmal werden Webseiten von Angreifern manipuliert, um an Passwörter zu gelangen oder Passwortdatenbanken zu stehlen.
- Wenn du ein Passwort mehrfach verwendest und dieses bei einer Datenpanne oder auf andere Weise in fremde Hände gelangt ist, kann es für den Zugriff auf deine anderen Konten verwendet werden.

Gute Passwörter verwenden

Top Ten der deutschen Passwörter (2021)

1) 123456
2) passwort
3) 12345
4) hallo
5) 123456789
6) qwertz
7) schatz
8) basteln
9) berlin
10) 12345678

Gute Passwörter verwenden

Schlechte Passwörter

- kurz < 12 Zeichen
- Einfach, nur Nummern, nur Kleinbuchstaben
- Wiederverwendet bei anderen Diensten

Gute Passwörter

- Lang > 32 Zeichen
- Komplex, alphanumerisch und Sonderzeichen
- Einzigartig für diesen Dienst

Digitale Selbstverteidigung

Eine Zusammenfassung von Gunter Bauer
Basierend auf dem Digitalen Lernmaterial https://epicenter.academy/e-learning

Grafik auf Folie 28 : Arbeitsweise von TOR von Saman Vosoghi, Quelle:
https://de.wikipedia.org/wiki/Tor_(Netzwerk)#/media/Datei:TOR_Arbeitsweise.svg
Lizenz: CC 0