

# Schütze deine digitale Identität!

## Zweifaktor-Authentifizierung

Sylvia

Chaos Communication Camp, August 2023

# Fragen?

- Es gibt keine dummen Fragen!
- Verständnisfragen bitte direkt.
- Alle anderen Fragen im Anschluss an den Vortrag.
- Folien: `https://raw.githubusercontent.com/sylvialange/vortraege/main/2fa.pdf`



# Sylvia

- Lehrerin in Süddeutschland
- Beschäftigung mit Datenschutzthemen in der Freizeit, z.B. Mitwirkung bei Cryptoparties

# Gliederung

## 1 Motivation

- Die digitale Identität und Schadenspotential
- Ein Faktor reicht nicht
- Exkurs: Hashwerte
- Generalschlüssel zur digitalen Identität

## 2 Multi-Faktor-Authentifizierung

- Arten von Faktoren
- Wissen: Passwörter
- Haben: TOTP und FIDO

## 3 Anmerkungen

## 4 Praktische Umsetzung

- Entscheidung für Key
- Wo beginnen?



- ## Die digitale Identität und Schadenspotential

# Was man mit einer gestohlenen Identität tun kann

- Auf Kosten anderer einkaufen, z.B. Amazon, Ebay.
- Im Namen anderer posten. → Rufschädigung.
- Stalken, z.B. wenn Zugriff auf Apple-ID, Standortbestimmung möglich.
- Daten stehlen und **veröffentlichen!**

- Auf Kosten anderer einkaufen, z.B. Amazon, Ebay.
- Im Namen anderer posten. → Rufschädigung.
- Stalken, z.B. wenn Zugriff auf Apple-ID, Standortbestimmung möglich.
- Daten stehlen und **veröffentlichen!**



- Auf Kosten anderer einkaufen, z.B. Amazon, Ebay.
- Im Namen anderer posten. → Rufschädigung.
- Stalken, z.B. wenn Zugriff auf Apple-ID, Standortbestimmung möglich.
- Daten stehlen und **veröffentlichen!**

- Auf Kosten anderer einkaufen, z.B. Amazon, Ebay.
- Im Namen anderer posten. → Rufschädigung.
- Stalken, z.B. wenn Zugriff auf Apple-ID, Standortbestimmung möglich.
- Daten stehlen und **veröffentlichen!**

# Passwörter reichten nicht: Doxingskandal 2018

- Weihnachten 2018: Jugendlicher „Hacker“ **ohne besondere Hacker-Künste** gelangte an Daten von Politikern.
- Nutzt Passwort-Zurücksetzen-Funktion.
- Veröffentlicht intime Chatverläufe von Politikern.

Ein Faktor reicht nicht

# Warum 1 Faktor nicht reicht

- Passwort auf kompromittiertem Rechner benutzt (Trojaner, Keylogger)
- Phishing
- Shoulder-Surfing / beim Tippen gefilmt
- Gerät mit gespeicherten Passwörtern geht verloren / wird gestohlen

Ein Faktor reicht nicht

# Warum 1 Faktor nicht reicht

- Passwort auf kompromittiertem Rechner benutzt (Trojaner, Keylogger)
- Phishing
- Shoulder-Surfing / beim Tippen gefilmt
- Gerät mit gespeicherten Passwörtern geht verloren / wird gestohlen

Ein Faktor reicht nicht

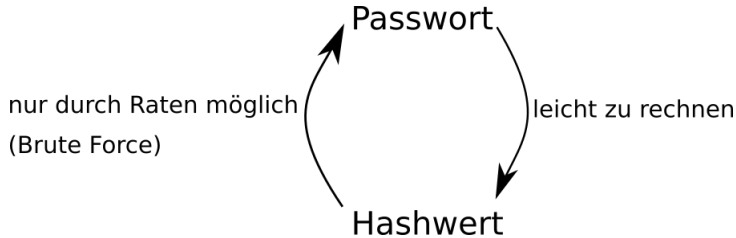
# Warum 1 Faktor nicht reicht

- Passwort auf kompromittiertem Rechner benutzt (Trojaner, Keylogger)
- Phishing
- Shoulder-Surfing / beim Tippen gefilmt
- Gerät mit gespeicherten Passwörtern geht verloren / wird gestohlen
- Datenpanne beim Dienst. Datenbank mit Useraccounts gestohlen. `https://sec.hpi.uni-potsdam.de/ilc/search?lang=de`

# Warum 1 Faktor nicht reicht

- Passwort auf kompromittiertem Rechner benutzt (Trojaner, Keylogger)
- Phishing
- Shoulder-Surfing / beim Tippen gefilmt
- Gerät mit gespeicherten Passwörtern geht verloren / wird gestohlen
- Datenpanne beim Dienst. Datenbank mit Useraccounts gestohlen. `https://sec.hpi.uni-potsdam.de/ilc/search?lang=de`

# Exkurs: Hashfunktion

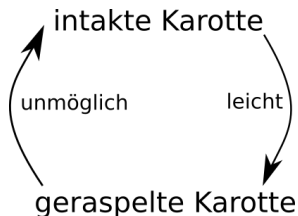


Wie eine Falltür:

- Eine Richtung leicht, ...
- die andere schwer ...



# Ein anschaulicher Vergleich



- Genau wie mit einer Karotte:
  - raspeln leicht,
  - wieder zusammen setzen unmöglich.
- Sicher ist aber, ob das Geraspelte von einer Karotte kommt.

# Hashwerte in Datenbanken

userrr	name	password
100	Annika	072b030ba126b2f4b2374f342be9ed44
101	Denise	d82c8d1619ad8176d665453cfb2e55f0
102	Kathrin	7f39f8317fbdb1988ef4c628eba02591
103	Sarah	9a1158154dfa42caddbd0694a4e9bdc8
104	Jana	b53b3a3d6ab90ce0268229151c9bde11

- In einer Datenbank werden i.d.R. Hashwerte statt des Passwortes im Klartext gespeichert.
- Gibt Nutzer sein Passwort ein, wird dieses gehasht und mit Hashwert in der Datenbank verglichen.
- Bei Übereinstimmung Zugang zur Webseite.

# Brute-Force-Angriff

- Hat ein Angreifer eine Datenbank mit Hashwerten, kann er Milliarden von Passwörtern ausprobieren (=Brute Force).
- Ohne eine Zeitverzögerung durch den Dienst. - Denn dieser ist nicht mehr zwischengeschaltet.
- Millionen Versuche pro Sekunde möglich.

# Der Generalschlüssel zur digitalen Identität

- Angreifer\*In hat Zugriff auf xyz@posteo.de
- Opfer hat bei Amazon xyz@posteo.de angegeben.
- Passwort-vergessen-Code auf diese Adresse schicken lassen.
- Angreifer\*In hat Zugriff.
- Angreifer\*In ändert auch noch Mail-Passwort. →Eigentümer\*In des Accounts bekommt keinen Zugriff mehr ...



## Passworthilfe

Geben Sie die E-Mail-Adresse oder Mobiltelefonnummer ein, die mit Ihrem Amazon-Konto verbunden ist.

E-Mail-Adresse oder Mobiltelefonnummer

xyz@posteo.de

Weiter

# Multifaktor-Authentifizierung

Authentifizierung = „Ich beweise, dass ich es bin.“

**Multi-Faktor** = Ich zeige es auf **mehrere** Arten

- |           |  |
|-----------|--|
| 1. Wissen | Passwörter   |
| 2. Haben  | Security-Token, z.B. Nitrokey, Yubikey; One-Time-Passwort (OTP); Passkey, Fido |
| 3. Sein   | Biometrische Daten wie Iris, Fingerabdruck, Venenmuster                        |



# Arten von Faktoren

1. Wissen      Passwörter üblich  $\Rightarrow$  weiter verwenden!
  2. Haben      Verbreitet sich zunehmend, z.B. Chipkarten, Security Token
  3. Sein      Wird kritisch gesehen:  
Revoke (=Ungültig- Erklären) und Wechsel nicht möglich
- Übliche Kombination: **sicheres** Passwort (Wissen) + Security Token oder OTP (Haben)
  - Denkfehler vermeiden: „Das Passwort ist nicht mehr so wichtig ...“



# Passwörter

- Sollen nach wie vor stark sein!
- Inzwischen gilt Faustformel:  
„Länge schlägt Komplexität.“
- Studien zeigen: Sonderzeichen und Zahlen ohnehin sehr vorhersehbar benutzt: 4ufw4ch3n!
- Empfehlung: Dice-Methode

## Zweifaktor-Authentifizierung





# Haben: Time Based One Time Passwort (TOTP)

- 6-stelliges Passwort
- von einer App aus aktueller Uhrzeit und einem geheimen Schlüssel generiert
- nur 30 Sekunden lang gültig



Haben: TOTP und FIDO

# TOTP: Berechnung

## Server (z.B. posteo.de):

geheimer Schlüssel:

facaeb6e8da2d3dcce16cf8245ed982b

Uhrzeit:

2020-02-15 14:40:30



Hashwert von Uhrzeit + Schlüssel

d2891823134078945ca1db3d53b

## Client / Token:

geheimer Schlüssel:

facaeb6e8da2d3dcce16cf8245ed982b

Uhrzeit:

2020-02-15 14:40:30



Hashwert von Uhrzeit + Schlüssel

d2891823134078945ca1db3d53b



Haben: TOTP und FIDO

# TOTP: Token versus App

Yubikey und Nitrokey:

- geheimer Schlüssel auf Key gespeichert
- dort nicht auslesbar, Key spuckt nur TOTP aus, niemals den geheimen Schlüssel

Authenticator Apps:

- Geheimnis auf Gerät gespeichert
- somit unsicherer als Security-Token



# Kritik an TOTP

- symmetrische Verschlüsselung (Server arbeitet mit gleichem Schlüssel wie Client)
- Verschleierung durch Hashen wie bei Passwörtern **nicht** möglich
- Somit **KEIN** Schutz gegen Angriff auf Server (wenn Angreifer\*In die Datenbank stiehlt)
- Hier hätte TOTP nicht geholfen:  
<https://monitor.firefox.com/breaches>
- ABER: Gerät das Passwort durch den Nutzer in falsche Hände (z.B. Phishing), ist Account durch zweiten Faktor geschützt.



Haben: TOTP und FIDO

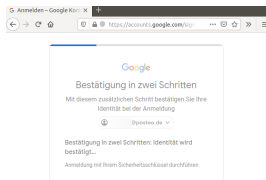
# Wo TOTP schützt ..

- Trojaner, Keylogger
- Phishing
- Shoulder-Surfing
- Geräte-Verlust (zumindest, wenn Token nicht auch verloren oder durch PIN gesichert)
- **Nicht bei** Datenpanne beim Dienst.



# Haben: FIDO, Passkey

- FIDO-Standard
- z.B. bei Google, Tutanota möglich, sonst bisher wenige Anbieter
- Easy: einfach Stick bei Anmeldung einstecken
- keine zusätzliche Software nötig
- Sicherer als TOTP, denn basierend auf **asymmetrischer** Verschlüsselung,
- Bei Diensten nachfragen, wann FIDO kommt



Haben: TOTP und FIDO

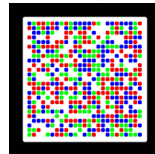
# U2F - FIDO: Praxis

- z.B. Login in Google-Konto oder <https://passkey.org> zeigen, Nutzernamen + Passwort, dann verlangt Browser den Stick, einstecken, antippen, fertig.



# Faktor Haben beim Online-Banking

- 2. Faktor laut Gesetz vorgeschrieben
- SMS, TOTP-App, chipTAN, Sm@rt-TAN
- empfohlen: Sm@rt-TAN
- geheimer Schlüssel auf Chipkarte + Daten der Transaktion → TAN
- Gerät nicht mit Internet verbunden



# Risiken mit dem Faktor „Haben“

- TOTP könnte durch Phishing gestohlen werden (dann allerdings nur 1 Login möglich)
- Security Token könnte gestohlen werden / verloren gehen
- PIN des Security-Tokens 3 mal falsch eingegeben / vergessen
- Man kann sich aus dem Account aussperren, z.B. Security Token defekt
- Deshalb **Ausweichmethoden** einrichten!

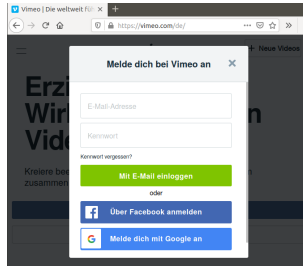
Haben: TOTP und FIDO

# Ausweichmethoden installieren!

- zweiten Key einrichten und sicher verwahren
- RecoveryCodes
- Oder geheimen Schlüssel notieren und sicher aufbewahren

# Föderierte Authentifizierung

- z.B. mit Google / Facebook einloggen
- Nachteil: Datenfluss zum Identity-Provider
- eventueller Vorteil: Der Identity-Provider ist besser gesichert als ein kleines Start-up



# Was zum Nachdenken ...

- Digitaler Nachlass?
- Sollen meine Erben Zugang zu bestimmten Accounts haben?
- Wie bekommen sie diesen Zugang?

## Praktische Umsetzung: Entscheidung für einen Key

## Nitrokey

## offene Software, offene Hardware

teurer (29€ + 99€)

## Berliner Firma

saubere Webseite ohne Dritt-Domains

nur bei <https://shop.nitrokey.com> verfügbar

## Yubikey

proprietäre Software

59€

US-amerikanische Firma

verwandte Webseite mit vielen  
Dritt-Domains (hat mit Key an sich nichts zu  
tun, zeigt aber etwas über die Firma)

zwar nicht im Elektromarkt aber  
immerhin bei Amazon verfügbar.

# Yubikey

- Blaues Modell für 25€ bietet nur FIDO, z.B. Absichern des Posteo-Postfaches nicht möglich.
- Yubikeys der 5er-Serie für ca. 59€ haben alle Funktionen, die man braucht: FIDO, TOTP, statisches Passwort, OpenPGP
- TOTP auch am Handy möglich

# Nitrokey



## Nitrokey FIDO2

- Kinderleichter Schutz Ihrer Benutzerkonten
- Passwortloses Login (FIDO2)
- Zwei-Faktor-Authentisierung (2FA, FIDO U2F)

29,00 €



## Nitrokey Pro 2

- Sicheres Login mit Einmalpasswörtern
- E-Mail-Verschlüsselung
- Festplatten- und Dateiverschlüsselung
- Manipulationssichere Chipkarte
- Open Source & Open Hardware

99,00 €

- FIDO-Stick kann nur FIDO
- Nitrokey Pro 2 für ca. 99€ kann: TOTP, statisches Passwort, OpenPGP, KEIN FIDO
- 69€ mehr Invest als bei Yubikey, TOTP am Handy nicht möglich



# NFC = Near Field Contact

- Yubikey hat NFC
- Komfortable Benutzung am Handy möglich
- unnötige Sicherheitslücke?
- Statt NFC auch USB OTG („on the go“) möglich.



Nitrokey über USB OTG verbunden

# Wo beginnen?

- Recovery-Mail-Adressen
- überall, wo Geld fließt
- Mit Passwortmanager Überblick behalten
- Tipp: Alle Einträge auf ungültig und erst auf gültig stellen, wenn 2FA eingerichtet
- Für normale Foren nicht nötig

## Wie sehr das Mail-Postfach abdichten?

## Gratwanderung zwischen Sicherheit und Komfort ...

## Komfort

Webmailer mit TOTP gesichert,  
**IMAP aktiviert** (nur Passwort)

## Angriffe per IMAP ohne zweiten Faktor möglich

Mails per Thunderbird,  
Handy-App abrufbar

## Sicherheit

## Webmailer per TOTP gesichert, **IMAP** deaktiviert

## Niemand kommt ohne zweiten Faktor an Mails ran

Komfortabler Abruf per App /  
Thunderbird nicht möglich

## Meine Lösung:

## 1. Mailadresse

für Kontakt mit Freunden, Kollegen u.ä.

IMAP-Abruf aktiviert, 2FA im Webmailer

## 2. Mailadresse

Kontakt mit Diensten (Google, Amazon, Ebay ...)

2FA im Webmailer und **Eingangsverschlüsselung**  
Angreifer kann nichts mit erbeuteten Mails anfangen

Falls zu kompliziert: IMAP-Zugriff sperren



## Zusammenfassung

- hoher zusätzlicher Schutz durch 2. Faktor
- erster Faktor immer noch wichtig!
- Ausweichmethoden
- Recovery-Mail-Adressen und Accounts mit Kontodaten besonders schützenswert

Download der Folien: <https://raw.githubusercontent.com/sylvialange/vortraege/main/2fa.pdf>

# Quellen

- **Kuketz-Blog** <https://www.kuketz-blog.de/gnupg-e-mail-verschluesselung-unter-android-nitrokey-teil4/>
- [https://shop.nitrokey.com/de\\_DE/shop](https://shop.nitrokey.com/de_DE/shop)
- <https://posteo.de/hilfe?tag=passwort-und-sicherheit>
- <https://www.security-insider.de/fido2-bringt-den-passwortfreien-login-a-753106/>  
zum Datenschutz bei FIDO
- **Deutsche Dice-Wortliste:** [http://world.std.com/~reinhold/diceware\\_german.txt](http://world.std.com/~reinhold/diceware_german.txt)

## Download der Folien:

- <https://raw.githubusercontent.com/sylvialange/vortraege/main/2fa.pdf>

# Praktischer Teil

- Eigenes Sicherheitskonzept entwickeln und hinterfragen
- Programme für Yubikey / Nitrokey installieren
- ... andere Anliegen?



# Mein eigenes Sicherheitskonzept

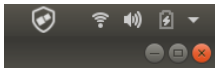
- Welches sind Ihre wichtigsten Accounts?
- Notieren Sie tabellarisch die Accounts und wie diese derzeit geschützt sind, welche Recovery-Möglichkeiten es gibt u.ä.
- Bei Bedarf erstellen Sie eine weitere Tabelle, wie Sie diese Accounts aus der ersten Tabelle künftig schützen wollen. Z.B. Recovery-Mailadresse ändern, zweiten Faktor hinzufügen, stärkeres Passwort usw.
- Beispiel einer solchen Tabelle:  
<https://walz-lange.de/auth.pdf>

# Sicherheitskonzept hinterfragen

- Sind die Passwörter von wichtigen Konten unique?
- Wie oft gibt es „Passwort auswendig, Passwort unique“? Realistisch?
- Wie gut sind die Konten gegen Aussperren geschützt?
- Sind Konten leicht über Recovery-Möglichkeiten zu übernehmen?
- ...

# Nitrokey mit Linux

- `https://www.nitrokey.com/documentation/installation`
- Dort verwendetes Modell und Betriebssystem wählen.
- In der Regel genügt: `sudo apt-get update && sudo apt-get install libccid nitrokey-app`
- Im Dash nach Nitrokey-App suchen und starten.
- Oben rechts neben Akkusymbol erscheint das Nitrokey-App-Symbol.



# Nitrokey mit Windows

- `https://www.nitrokey.com/download/windows`
- Dort gibt es einen Link auf Github: `https://github.com/Nitrokey/nitrokey-app/releases/tag/v1.4`
- In der Rubrik Assets die exe-Datei herunterladen und als Administrator ausführen.

# Yubikey mit Linux

- Terminal: `sudo apt-add-repository ppa:yubico/stable`
- `sudo apt update && sudo apt install yubioath-desktop yubikey-personalization-gui`
- Im Dash nach Yubico Authenticator suchen und starten
- Erklärvideo:  
<https://www.invidio.us/watch?v=mdQzbnbng4B7o>

# Yubikey mit Windows

- auf `https://yubico.com` → Support → Downloads
- die Authenticator-App herunterladen
- Erklärvideo:  
`https://www.invidio.us/watch?v=mdQzbng4B7o`

# Yubikey mit Android

- Im Playstore Yubico Authenticator herunterladen oder
- auf `https://github.com/Yubico/yubioath-android/releases` **APK** herunterladen und installieren