

>>> Workshop: Hands-On Digitale Selbstverteidigung  
>>> ein Workshop der AG-Link

Nikita & Peter

23. Oktober 2024

Vorstellung

## >>> Vorstellung

- \* AG Link - AG für kritische Informatik
- \* seit 2018
- \* Website: [ag-link.xyz](https://ag-link.xyz) (+ Folien)
- \* Email: [ag-link@riseup.net](mailto:ag-link@riseup.net)
- \* Instagram: [@ag.link\\_le](https://www.instagram.com/ag.link_le)
- \* Mastodon:  
<https://systemli.social/@link>



## >>> Warum Daten schützen?

Wer hat Interesse an meinen Daten?

- \* ich + Freunde, Familie, Bekannte
- \* Hacker, Erpresser, etc.
- \* Firmen
- \* Behörden

## >>> Gefahr durch unverschlüsselte Daten

Daten werden immer noch oft unverschlüsselt gespeichert.

- \* login Passwort schützt nicht ohne weiteres Daten
- \* Daten *vollständig* zu löschen ist nicht einfach

>>> Welche Daten sind potentiell unverschlüsselt?

Device	Mount Point/ RAID/Volume	Type	Format	Size (MB)	Start	End
<b>LINUX FILE SYSTEM</b>						
Hard Drives						
/dev/sda						
/dev/sda1	/	ext3	✓	1027	1	131
/dev/sda2	/usr	ext3	✓	8001	132	1151
/dev/sda3		swap	✓	3498	1152	1597
/dev/sda4						
		Extended		7946	1598	2610
/dev/sda5	/disk3	ext3	✓	2000	1598	1852
/dev/sda6	/disk2	ext3	✓	2000	1853	2107
/dev/sda7	/disk1	ext3	✓	2000	2108	2362
/dev/sda8	/var	ext3	✓	996	2363	2489
/dev/sda9	/flash	ext3	✓	949	2490	2610
<input type="checkbox"/> Hide RAID device/LVM Volume Group members						
<b>WINDOWS FILE SYSTEM</b>						
OS (C:) 231.77 GB NTFS Healthy (Boot, Page File, Crash)		New Volume (D:) 64.03 GB NTFS Healthy (Logical Drive)		New Volume (J:) 80.00 GB NTFS Healthy (Logical Drive)		
<input type="checkbox"/> Primary partition <input type="checkbox"/> Extended partition <input type="checkbox"/> Free space <input type="checkbox"/> Logical drive						

Abbildung: Wo werden Daten gespeichert?

## >>> Gefahr durch unverschlüsselte Daten

Angenommen du verlierst deinen Laptop.

Bist du dir sicher, dass niemand auf deine persönlichen Daten zugreifen kann?

## >>> Vorteile von Verschlüsselung

Kümmert euch aktiv um die Verschlüsselung eurer Daten!

- \* Speicherort spielt dann keine Rolle mehr
- \* Keine Gefährdung bei Verlust
- \* Verschlüsselung ist sehr schwer bis gar nicht zu knacken

>>> Verschlüsselung - der einfache Fall



Abbildung: Symmetrische Verschlüsselung

# >>> Verschlüsselung - der einfache Fall

## AES Online Encryption

Enter text to be Encrypted

123

OR

No file chosen

Select Mode

CBC

Key Size in Bits

128

Enter IV (Optional)

1234567898765432

Enter Secret Key

1234123456789878

Output Text Format: Base64 Hex

AES Encrypted Output:

4573BF2C65009DF18FAF9421B5D0E789

## AES Online Decryption

Enter text to be Decrypted

4573BF2C65009DF18FAF9421B5D0E789

Input Text Format: Base64 Hex

Select Mode

CBC

Enter IV Used During Encryption(Optional)

1234567898765432

Key Size in Bits

128

Enter Secret Key

1234123456789878

AES Decrypted Output (Base64):

MTIz

123

## >>> Verschlüsselung - Sicherheit?

- \* AES 256-Bit Verschlüsselung
- >  $2^{256}$  mögliche Kombinationen
- > Dauer Entschlüsselung ohne Wissen des Passwort = ca.  $3,3 \times 10^{56}$  Jahre
  - \* vgl. Alter des Universums:  $13,8 \times 10^9$

## >>> Verschlüsselung - Auswirkungen von Quantencomputing

### \* Grover's Algorithmus:

- \* reduziert die effektive Sicherheit auf etwa die Hälfte
- > AES-256 wird zu AES-128 äquivalent gegen Quantenangriffe
- > Geschätzte Entschlüsselungszeit: ca.  $1,08 \times 10^{22}$  Jahre
  - \* vgl. Alter des Universums:  $13,8 \times 10^9$

### \* Geschätzte Sicherheit gegen Quantenangriffe: 50 bis 100+ Jahre



>>> Welche Daten sind bereits verschlüsselt?

Standardmäßig nicht zwangsläufig verschlüsselt:

- \* Windows
- \* macOS
- \* Linux
- \* Festplatten
- \* USB-Sticks
- \* Cloud-Speicher

Standardmäßig verschlüsselt:

- \* Android, iOS, spezielle Speichermedien (Self-Encrypting Drives)
  - \* Achtung! Was ist mit zusätzlicher SD-Karte?

## >>> Verschlüsselungsprogramme

*Wie verschlüssele ich meine Daten?*

Universell:

- \* VeraCrypt

- \* Container, Laufwerke, Partitionen
- \* zum Beispiel voll- oder teilweise Verschlüsselung von:  
Laptop-/Desktopsspeicher, USB-Sticks, externe Festplatten, ...

Windows:

- \* BitLocker (closed Source)

macOs:

- \* FileVault (closed Source)

Linux:

- \* LUKS (Linux Unified Key Setup)

Cloud-Speicher:

- \* cryptomator

>>> **Vorgehen**

Was folgt:

Was erstmal offen bleibt:

## >>> Vorgehen

Was folgt:

- \* „Safe Place“ auf eigenem Computer einrichten, mittels verschlüsselten Containern

Was erstmal offen bleibt:

## >>> Vorgehen

Was folgt:

- \* „Safe Place“ auf eigenem Computer einrichten, mittels verschlüsselten Containern

Was erstmal offen bleibt:

- \* Daten verschlüsselt mit Cloud-Speicher synchronisieren
- \* Prozess-, Marketing- und Nutzer\*innen-Daten von Webdiensten
- \* Datensicherung (z.B. Backups)

## >>> Let's Encrypt

### Warum VeraCrypt?

- \* Open Source (keine backdoors, prüfbar, fortführbar auch nach Entwicklungsstopp)
- \* weite Verbreitung und Anerkennung
- \* unabhängige Audits, unter anderem vom Bundesamt für Sicherheit<sup>1</sup>
- \* einfach anzuwenden

### Zum Projekt:

- \* Vom Unternehmen IDRIX betreut<sup>2</sup>
- \* Nachfolge vom TrueCrypt Projekt

---

<sup>1</sup><https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Veracrypt/Veracrypt.html>

<sup>2</sup><https://www.idrix.fr/Root/>

## >>> Arten der Verschlüsselung in VeraCrypt

In VeraCrypt gibt es zwei Arten der Verschlüsselung:

- \* 1. File als Container

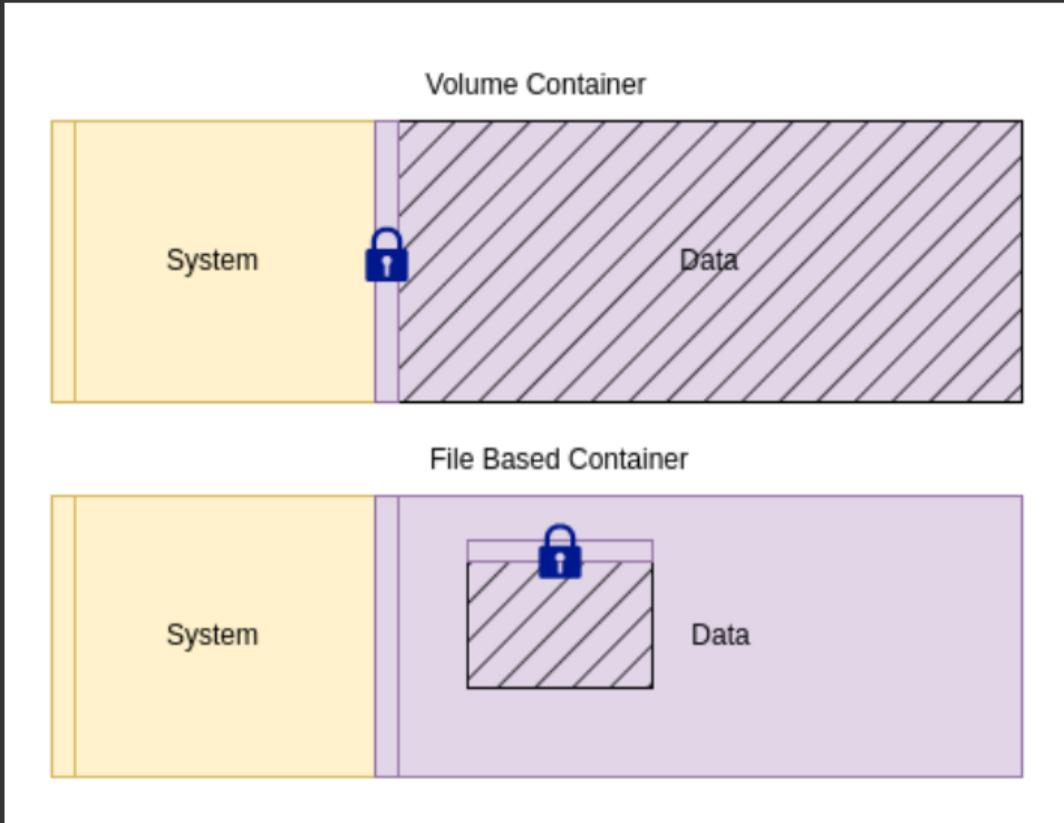
- \* können wie normale Files behandelt werden (verschoben, gelöscht, unbenannt)
- \* Liegt auf der Festplatte, Metadaten fallen an
- \* Kann während der Laufzeit verschlüsselt bleiben, was Zugriff erschwert

- \* 2. (Gesamte) Partition als Container

- \* Möglichkeit der Vollverschlüsselung
- \* keine unverschlüsselten Reste auf der Festplatte

Problem von Containerbasierter Verschlüsselung: Container können verschlüsselt nur als ganzes übertragen werden.

# >>> File vs. Volume basierte Verschlüsselung



**Abbildung:** VeraCrypt Verschlüsselungsmöglichkeiten (Eigene Grafik)

## >>> Weitere Anwendungsmöglichkeiten

- \* Versteckte verschlüsselte Partitionen (mit plausible deniability)

# Workshop - VeraCrypt