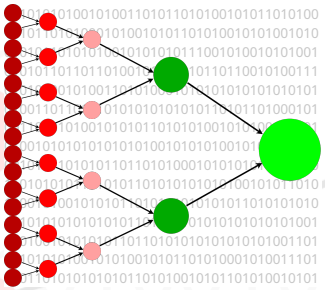
# „End of 10“

## Keine Angst vor Linux!

Hendrik Griesche,
IT-Sicherheit und Datenschutz,
Linux-Administrator und Webprogrammierung
hendrik@griesche.org

Ladencafé Klönsnack
des Vereins „Christliche Initiative für eine soziale Welt e.V.“



# Heutige Themen

1. Linux Mint Live-System
2. Exkurs: Partitionierung
3. Digitale Souveränität
4. Ist Linux sicher
5. Identische Anwendungsprogramme
6. Sicherheit
   - Phishing
   - Ransomware
   - Verschlüsselte Datenübertragung
   - Netzwerkaspekte
   - Sichere Passwörter
7. Ladencafé Klönsnack

lewing@isc.tamu.edu Larry Ewing and The GIMP

# Live-System vom USB-Stick starten

Normalerweise bootet (das Betriebssystem laden) ein Computer autmatisch vom eingebauten Blockspeicher. Um von einem anderen Datenträger oder über das Netzwerk zu booten, muss man gleich nach dem Einschalten des Rechners eine Taste drücken. Diese Taste ist rechnerspezifisch, z. B.:

- F8
- F11
- F12
- F1 oder F2 oder <entf>, um ins BIOS/EFI zu gelangen → dort die Bootreihenfolge ändern

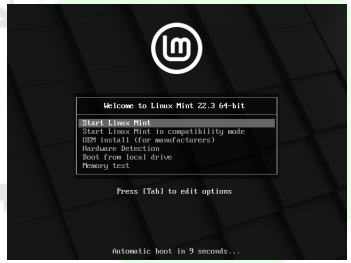

www.thomann.de/de/the_t_pc_usb_3.0_

Anschließend wählt man den USB-Stick aus bzw. setzt ihn an die oberste Stelle.

→ Der Rechner startet Linux Mint (dauert einen Moment).

# Boot-Loader

Gleich zu Beginn des Bootvorgangs vm USB-Stift sieht man das Auswahlmenü des Boot-Loaders. Der Boot-Loader startet vor dem Betriebssystem und bietet z. B. die Möglichkeit, aus mehreren Betriebssystemen auszuwählen. So kann man ein sog. „Dual-Boot“ (Linux oder Windows starten) realisieren.
Ein Boot-Loader ist bei Linux Standard.



# Live-System ausprobieren

Nun kann man das Live-System ausprobieren. Man kann wirklich **alles** ausprobieren: Software installieren und deinstallieren, Konfigurationen ändern usw. Alles dauert etwas, da die Daten auf dem USB-Stick gepackt sind und immer zuerst entpackt werden müssen. Die dafür erforderliche Zeit ist abhängig von der Rechenleistung und dem Interface des USB-Sticks (2.0 oder 3.0).

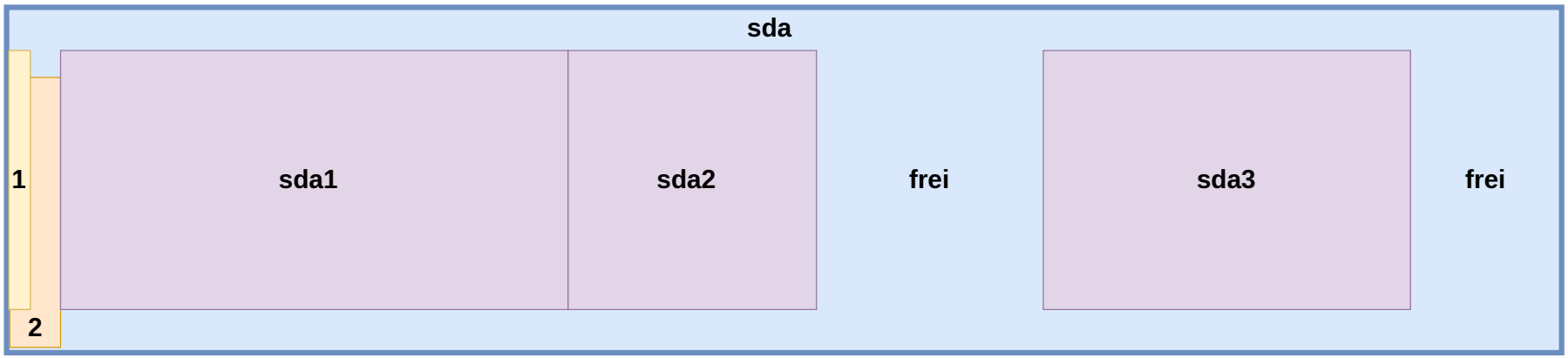
**Alle** Änderungen sind flüchtig – beim Neustart sind alle Änderungen weg.
→ Falls man etwas verbogen hat – kein Problem: Neustart genügt.

# Vom Live-System aus Linux Mint auf den eigenen Blockspeicher installieren

# Exkurs: Partitionierung – MBR (Master Boot Record)



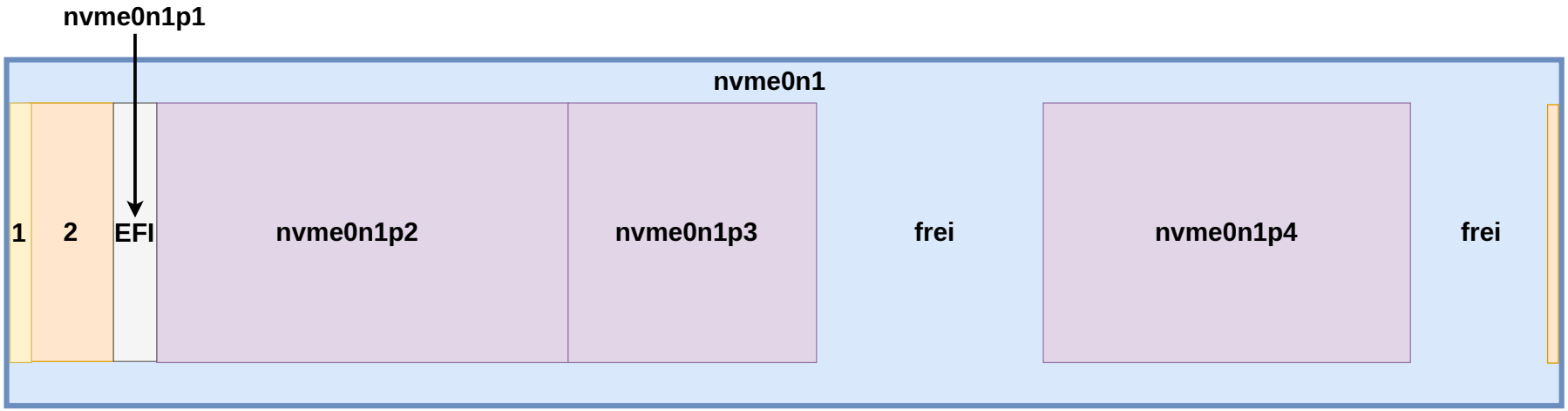

Um auf den Blockspeicher (Festplatte) zuzugreifen, muss er partitioniert werden.




**1 - Master Boot Record (512 Byte (0. Sektor))**
**2 - Partition Table (4 x 16 Byte) innerhalb des MBR**

# Exkurs: Partitionierung – GPT (Grand Partition Table)

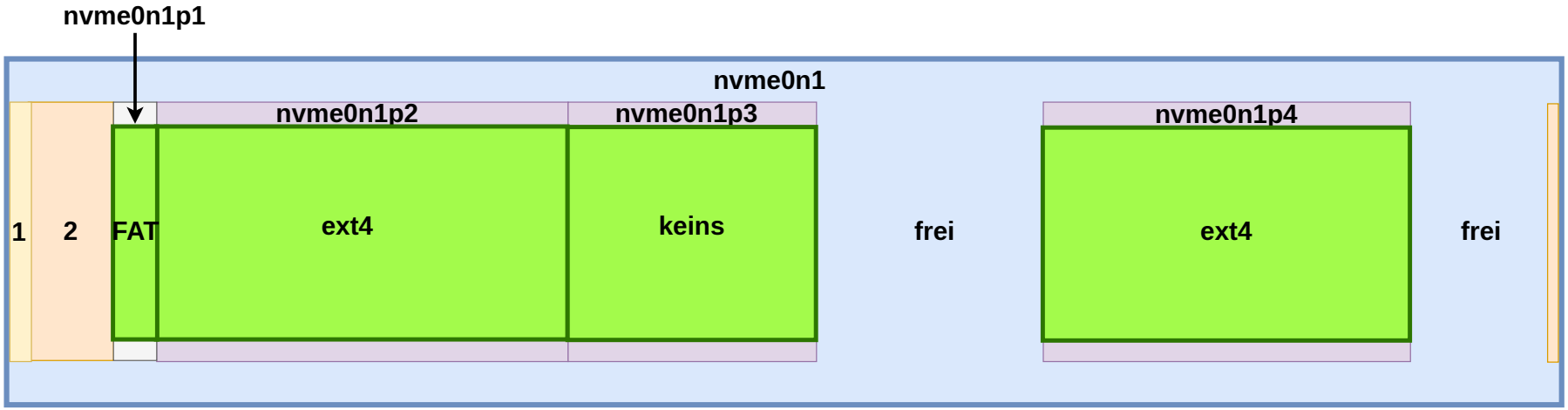

Um auf den Blockspeicher (Festplatte) zuzugreifen, muss er partitioniert werden.




**1 - Master Boot Record (512 Byte (0. Sektor))**
**2 - Grand Partition Table nach dem MBR (mehrere Blöcke)**

# Exkurs: Partitionierung – GPT (Grand Partition Table)

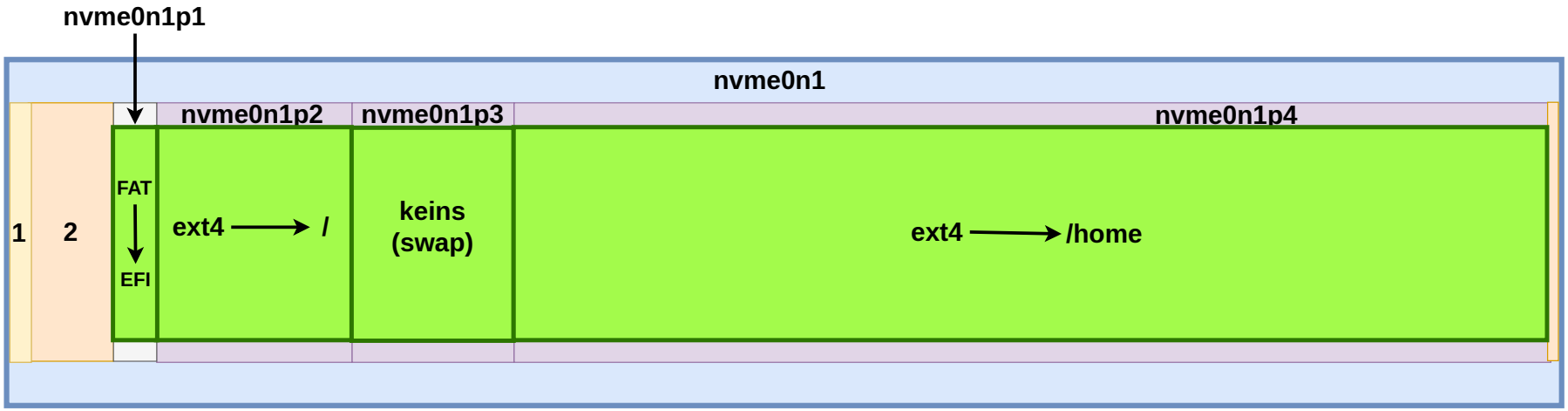

Um auf eine Partition zugreifen zu können, muss auf ihr ein Dateisystem angelegt werden („Formatieren“)




**1 - Master Boot Record (512 Byte (0. Sektor))**
**2 - Grand Partition Table nach dem MBR (mehrere Blöcke)**

# Exkurs: Partitionierung – Linux-typisch


Um auf ein Dateisystem zugreifen zu können (nur lesend oder lesend/schreibend), muss es an beliebiger Stelle in den Verzeichnisbaum des lokalen Betriebssystems (/, „root“) eingebunden werden „Mounten“)




**1 - Master Boot Record (512 Byte (0. Sektor))**
**2 - Grand Partition Table nach dem MBR (mehrere Blöcke)**

# Einige Einstellungen vornehmen

# Digitale Souveränität

- (Nur) Man selbst ist Eigentümer und Besitzer seiner eigenen Daten
- Man kann alle eigene Daten uneingeschränkt lesen und schreiben (ändern) – auch noch in 100 Jahren
- Das ist ausschließlich mit Open Source Software gewährleistet, da sämtliche Spezifikationen (z. B. zu Speicherformaten) öffentlich zugänglich sind
- bei proprietären Programmen (und Speicherformaten) ist man komplett vom Hersteller abhängig und kann typischerweise nach einer gewissen Zeit seine eigenen Daten nicht mehr schreiben (ändern) und noch später auch nicht mehr lesen

norbert-pohlmann.com/glossar-cyber-sicherheit/technologische-souveraenitaet-im-cyber-raum/

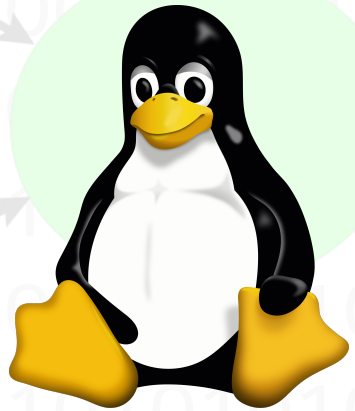
# Ist Linux sicher?

- Ist Linux sicher? JA!
- Ist Linux sicherer als Windows?JA?
- Ist Linux sicherer als Apple (iOS)? Die eigenen Daten JA!
- Wie sieht es mit digitaler Souveränität aus?
- Weshalb? $\rightarrow$

# Ist Linux sicher?

Linux:

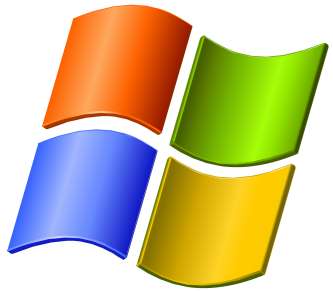
- „Open Source“ (quelloffen) – von Nutzern für Nutzer
  → der **einzige** Weg zu digitaler Souveränität und Datenhoheit
- nutzt modernste Technologien und Konzepte
- ist modular aufgebaut
  → Komponenten, die eine bestimmte Zeit nicht genutzt wurden, werden automatisch aus Kernel und Arbeitsspeicher entfernt und bei Bedarf automatisch wieder eingeladen
- an Linux entwickeln weltweit tausende Programmierer: Profis, Amateure und sogar Firmen
  → dies ist ein Vielfaches des geistigen Potentials der (wenigen) angestellten Windows-Entwickler



# Ist Linux sicherer als Windows? JA!

Windows:

- ist ein proprietäres Produkt – zum Geldverdienen (Nutzer zahlen, Firmen kassieren)
- ist konzeptionell aus den 1990er Jahren
- neue Technologien wurden nur „angebaut“, jedoch nicht integriert
- ist monolithisch aufgebaut
- ist an zahlreichen Stellen verwundbar
- an Windows entwickeln einige (wenige) angestellte Entwickler
- kann zahlreiche aktuelle Technologien nicht, nur rudimentär oder nur auf Umwegen nutzen (Virtualisierung, Dateisysteme, ...)



www.linux-community.de/ausgaben/easylinux/2009/0zur-windows-emulation/

# Ist Linux sicherer als Apple? Die eigenen Daten? JA!

Apple (iOS):

- ist ein proprietäres Produkt – zum Geldverdienen (Nutzer zahlen, Firmen kassieren)
- an iOS entwickeln einige (wenige) angestellte Entwickler
- Steve Jobs (DER Visionär Apples) ist seit 2011 tot – seitdem gab es keine einzige Innovationen mehr, man lebt nur noch von der Substanz und schottet sich immer massiver ab

wiki.reactivemicro.com/

images/e/e3/Apple_Spectrum

_Colors_1993.pdf

# Ist Linux sicherer als Apple? Die eigenen Daten? JA!

Apple (iOS):

- der Nutzer ist nicht Besitzer seiner Daten, das ist Apple
- Apple macht mit den persönlichen Daten der Benutzer, was Apple will
- Datenschutz ist nicht ansatzweise gewährleistet: Verpflichtender Apple-Account, Überprüfung der eigenen Identität, Apple sammelt, kombiniert, trackt, klassifiziert personenbezogene Daten und gibt sie an Dritte uneingeschränkt weiter
- Es ist schwierig, Daten in Apple-Geräte hineinzubekommen und noch schwieriger, Daten wieder herauszubekommen

wiki.reactivemicro.com/

images/e/e3/Apple_Spectrum

_Colors_1993.pdf

# Ist Linux sicherer als Apple? Die eigenen Daten? JA!

Apple (iOS):

- www.apple.com/legal/internet-services/itunes/chde/terms.html
- www.apple.com/legal/privacy/de-ww/
- www.apple.com/legal/sla/docs/iOS18_iPadOS18.pdf
- www.bundeskartellamt.de/DE/DigitalWirtschaft/VerfahrenGegenGrosse-Digitalkonzerne/Apple/Apple.html

wiki.reactivemicro.com/images/e/e3/Apple_Spectrum_Colors_1993.pdf

# Identische Anwendungsprogramme

Zahlreiche Anwendungsprogramme, die Sie von Windows bzw. iOS kennen, sind identisch mit denen von Linux.

- LibreOffice The Document Foundation LibreOffice
- Firefox (in Firefox für ist sogar die Downloadfunktion gesperrt)
- Thunderbird
- Online-Banking: Über Webbrowser wie gewohnt
- Webmail: Über Webbrowser wie gewohnt
- VLC
- GIMP

lewing@isc.tamu.edu Larry Ewing and

The GIMP

upload.wikimedia.org/wikipedia/commons/thumb/0/02/LibreOffice_Logo_Flat.svg/3840px-LibreOffice_Logo_Flat.svg.png; de.wikipedia.org

/wiki/Datei:Mozilla_Firefox_Logo.png; upload.wikimedia.org/wikipedia/commons/thumb/e/e1/Thunderbird_Logo%2C_2018.svg/3840px-

Thunderbird_Logo%2C_2018.svg.png; de.wikipedia.org/wiki/Datei:VLC_Icon.svg; upload.wikimedia.org/wikipedia/commons/thumb/6/67

/The_GIMP_icon_-_v3.0.svg/3840px-The_GIMP_icon_-_v3.0.svg.png

# Phishing = Abgreifen sensibler Daten

Phishing = Abgreifen sensibler Daten (meist Zugangsdaten) durch mehr oder weniger geschicktes Täuschen argloser Anwender, z. B. durch E-Mails mit einem Link, den der arglose Anwender klickt. Dadurch wird er auf eine Webseite gelenkt, auf der er zur Eingabe sensibler Daten aufgefordert wird.


www.malwarebytes.com/de/phishing

**Sind sie drin, sind sie weg!**

# Phishing: Abhilfe

**Klicke keinen Link, den du nicht selbst bestellt hast**

# Phishing: Abhilfe

**Prüfe den URI**

URI = Uniform Resource Identifier
(einheitlicher Bezeichner für Ressourcen)

# Phishing: Abhilfe

**Gib personenbezogene Daten (Name, Adresse, Telefon, Mailadresse, Bankverbindung) nur dann ein, wenn du ganz genau weißt:**

- **Wer erhält die Daten?**
- **Was macht er damit?**
- **Ist er absolut vertrauenswürdig?**

# Ransomware

- Die eigenen Daten auf dem eigenen Rechner werden durch Kriminelle verschlüsselt – man selbst kann nicht mehr auf sie zugreifen
- Anschließend erpressen die Kriminellen Geld (meist Bitcoins)
- Es wird behauptet, dass nach Zahlung der Schlüssel zum Entschlüsseln der eigenen Daten preisgegeben würde
- Die eigentliche Gefahr: Der eigene Rechner führt unbekannte Programme aus, von denen nicht bekannt ist, was sie noch alles anstellen
  z. B. kann der eigene Rechner am eigenen Kommunikationsanschluss (Telefon) Teil eines Bot-Netzes werden → strafrechtlich relevant

www.btc-echo.de/academy/bibliothek/was-ist-bitcoin/

# Ransomware: Abhilfe

**Führe ausschließlich Software auf deinen Geräten und in deinem Netzwerk aus, von denen du (oder andere) genau wissen, was sie macht (und insbesondere, was sie nicht macht: Nach Hause telefonieren, Rechner ausschnüffeln und manipulieren, Backdoors installieren und öffnen, an Bot-Netzen teilnehmen, deine eigenen Daten verschlüsseln, ...)**

# Verschlüsselte Datenübertragung

- Kommunikation über unsichere Kanäle (Internet) **muss** (ausreichend stark) verschlüsselt erfolgen! → Niemand anderes als der Berechtigte darf die Daten lesen können
- Es **muss** gewährleistet sein, dass man mit dem „richtigen“ Server kommuniziert (und kein Man-in-the-middle die Daten abgreift, liest und dem eigentlichen Empfänger manipulierte Daten sendet)
- Hierfür werden Zertifikate genutzt
- Schlosssymbol im Webbrowser informiert meist über die verschlüsselte Übertragung zum „richtigen“ Server mittels TLS

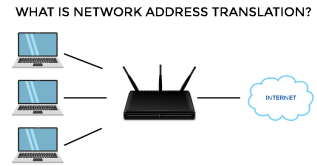
downloadscdn5.freepik.com/d/
138642991/52683/158/157920/
hand-drawn-robber-cartoon-
illustration.zip?token=exp=
1773784328 hmac=acfc638f2
ca77d996becdfba102e17c0

# Verschlüsselte Datenübertragung

## Demonstration

# NAT – Fritzbox, Speedport und andere

- drahtgebundene Rechner im eigenen Netzwerk relativ gut gegen Angriffe von außerhalb geschützt
- dynamische Firewall (blocken Verbindungsversuche vn außen nach innen)
- Vorsicht: In Fritzboxen, Speedports usw. integriertes WLAN: WLAN ist im gleichen Netzwerk wie LAN
  → sicher verschlüsseln (WPA2/WPA3)




https://www.rtautomation.com/rtas-blog/what-is-network-address-translation/

# WLAN

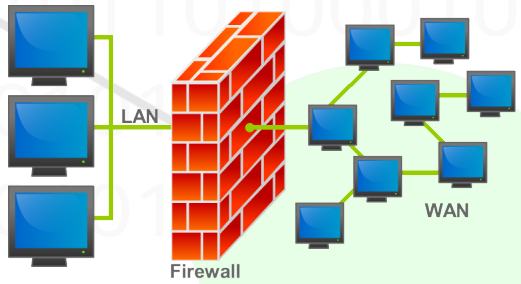
- → sicher verschlüsseln (WPA2/WPA3)
- dennoch: Firewall aktivieren, die mindestens Verbindungsversuche von außen blockiert


https://www.seton.de/symbol-piktogramm-schilder-wlan.html#CPS%20CPS2261970+1175409101

# Firewall

Aufgaben:

- Netzwerkverkehr blockieren → zahlreiche Filterregeln
  - eingehend / ausgehend
  - TCP / UDP
  - IPv4 / IPv6
  - nur Datenpakete bereits bestehender Verbindungen oder auch andere
  - externe Netzwerk-Scans



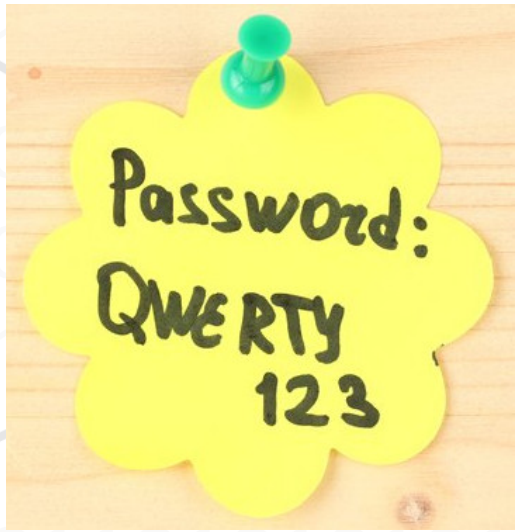
# Sichere Passwörter

Sichere Passwörter

- Länge: Mindestens 20 Zeichen aus Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen
- KEINE Umlaute oder ß
- Passwortmanager benutzen

Zusätzlich, falls möglich

- Zwei-Faktor-Authentifizierung (2FA)
- Schlüssel nutzen (eher weniger wahrscheinlich)




www.dr-datenschutz.de/das-perfekte-passwort/

# Berechnungsbeispiel zum Knacken von Passwörtern

Zeit eines normalen Bürorechners zum Knacken eines 10-stelligen Passwortes aus einem Vorrat von 108 Zeichen)

- $108^{10}$ Kombinationen
- $\rightarrow$ 5 Tage
- also 2,5 Millionen Kombinationen pro Sekunde

ist Ausgangswert

pixabay.com/de/photos/einbrecher-kriminell-dieb-r%c3%a4uber-4925202/

# Berechnungsbeispiel zum Knacken von Passwörtern

mit schnellem Rechner (ca. 10-fache Rechenleistung)

- $108^{10}$ Kombinationen
- $\rightarrow$ 0,5 Tage

pixabay.com/de/photos/einbrecher-kriminell-dieb-r%c3%a4uber-4925202/

# Berechnungsbeispiel zum Knacken von Passwörtern

unter Nutzung einer Grafikkarte (ca. 1000-fache Rechenleistung)

- $108^{10}$ Kombinationen
- $\rightarrow$ 0,0025 Tage $=$ 3,6 Minuten

pixabay.com/de/photos/einbrecher-kriminell-dieb-r%c3%a4uber-4925202/

# Berechnungsbeispiel zum Knacken von Passwörtern

mit der geschätzten Rechenleistung eines Geheimdienstes (ca. $10^{10}$)-fach

- $108^{10}$ Kombinationen
- $\rightarrow$ 0,02 Millisekunden
- $\rightarrow 54 \cdot 10^{15}$ Kombinationen pro Sekunde

pixabay.com/de/photos/einbrecher-kriminell-dieb-r%c3%a4uber-4925202/

# Berechnungsbeispiel zum Knacken von Passwörtern

20-stelliges Passwort aus einem Vorrat von 108 Zeichen
mit der geschätzten Rechenleistung eines Geheimdienstes (ca. $10^{10}$)-fach

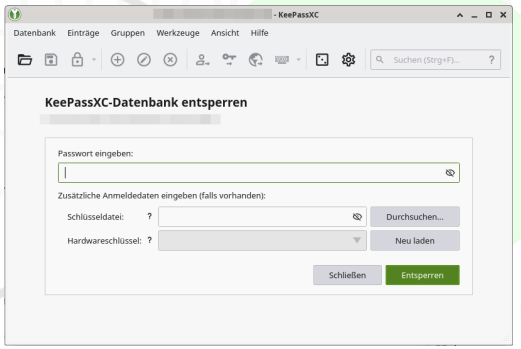
- $\frac{108^{20}\,Kombinationen}{54 \cdot 10^{15}\,\frac{Kombinationen}{Sekunde}}$
- $\approx$ 11 Millionen Sekunden $\approx$ 125 Jahre

pixabay.com/de/photos/einbrecher-kriminell-dieb-r%c3%a4uber-4925202/

Wie wird das mit Quantencomputing aussehen?

# Passwort-Manager

- automatische Erzeugung sicherer Passwörter
- Passwörter werden verschlüsselt gespeichert
- Passwort-Datei niemals aus der Hand geben!
- Masterpasswort zum Entsperren des Passwort-Managers mittels eines einprägsamen Satzes (Anfangsbuchstaben nutzen)
- KEINE Umlaute oder ß
- Passwort-Manager mit plattform-unabhängigem Speicherformat wählen, z. B. *Keepass*



# (Endlich) Geschafft

# Viel Erfolg

www.spreadshirt.de/shop/design/akku+leer+sticker-D5b5ccb1ce4474262bcf51b91

# Ladencafé Klönsnack

Öffnungszeiten

www.spreadshirt.de/shop/design/akku+leer+sticker-

D5b5ccb1ce4474262bcf51b91

# Ladencafé Klönsnack

Angebot

www.spreadshirt.de/shop/design/akku+leer+sticker-

D5b5ccb1ce4474262bcf51b91