Computersicherheit für Aktive

© Franz Gratzer, CC-BY-SA

Warum rede ausgerechnet ich über Computersicherheit?

- Kein Techniker
- Engagiert für Freie Software
- Erfahrungen als Aktivist
- Tierschutzprozess miterlebt

© Franz Gratzer, CC-BY-SA

Was ist „Computersicherheit“?

A) Schutz vor Viren und Trojanern

B) Abwesenheit von Datenlecks

C) Schutz vorm Verlust wichtiger Daten

D) uneingeschränkte Selbstbestimmung

E) Schutz vor physischen Verletzungen

© Franz Gratzer, CC-BY-SA

Was meine ich mit „Computersicherheit“?

Privatsphäre und Selbstbestimmung: Ein System, das ausschließlich tut, was ich möchte. Es sammelt/sendet weder unerwünscht Daten noch beschränkt es mich.

© Franz Gratzer, CC-BY-SA

Verstandlose Automaten

Computer haben keine eigenen Impulse. Sie führen alle Anweisungen aus, die sie erhalten. Egal woher oder von wem sie kommen. Unwichtig, ob diese Anweisungen unsinnig oder gar nachteilig für uns sind.

© Franz Gratzer, CC-BY-SA

Was kann ich von einem neu gekauftem Computer erwarten?

A) aktuelle Software

B) Schutz vor Fremdzugriff

C) harmonierende Komponenten

D) Hilfe im Fall von Problemen

© Franz Gratzer, CC-BY-SA

Weshalb sind handelsübliche Computer meist ein Problem?

Bei „proprietären“ (= unfreien) Systemen können und dürfen wir die internen Abläufe weder untersuchen noch abändern. Wir können sie nur beschränkt anpassen.

© Franz Gratzer, CC-BY-SA

Wer bestimmt also?

A) Händler:innen

B) Hersteller:innen

C) Regierung

D) potenzielle Eindringlinge

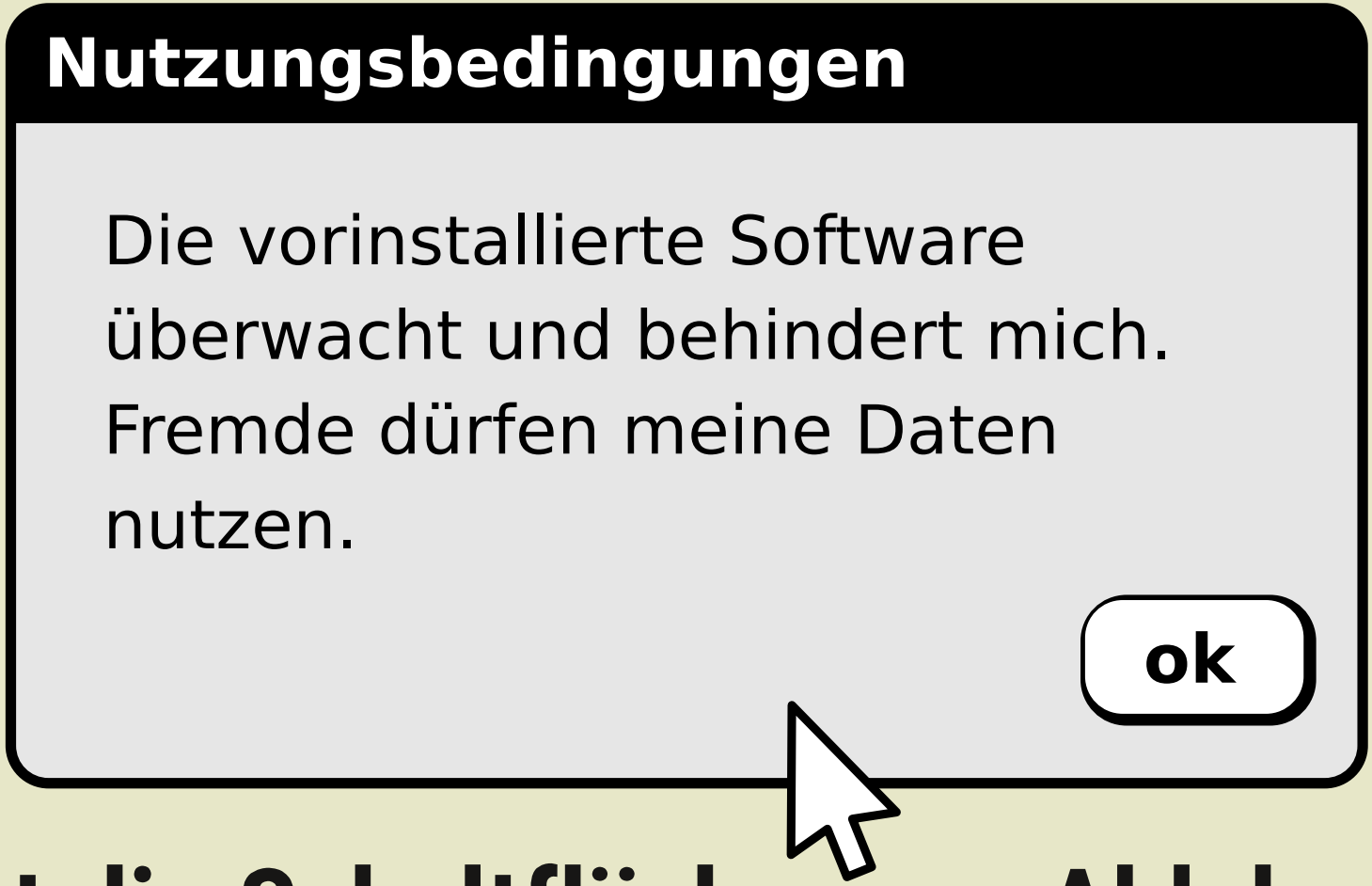
E) Ich selbst

© Franz Gratzer, CC-BY-SA

Wer ist in Kontrolle?

Computer und Mobilgeräte werden als fertig vorkonfigurierte Systeme verkauft. Wir können meist kaum wissen und beeinflussen, wer ihnen Anweisungen gibt und was genau in ihnen passiert.

© Franz Gratzer, CC-BY-SA



Wo ist die Schaltfläche zum Ablehnen?

 © Franz Gratzer, CC-BY-SA

Die 4 Freiheiten Freier Software

1) Verwenden

Wir dürfen sie ohne Nutzungs-beschränkungen beliebig einsetzen.

© Franz Gratzer, CC-BY-SA

Die 4 Freiheiten Freier Software

2) Verstehen

Wir dürfen sie untersuchen und an unsere Bedürfnisse anpassen (lassen).

 © Franz Gratzer, CC-BY-SA

Die 4 Freiheiten Freier Software

3) Verbreiten

Wir dürfen anderen helfen und Kopien der Software an sie weitergeben.

© Franz Gratzer, CC-BY-SA

Die 4 Freiheiten Freier Software

4) Verbessern

Wir dürfen unsere verbesserten Versionen veröffentlichen, sodass alle davon profitieren können.

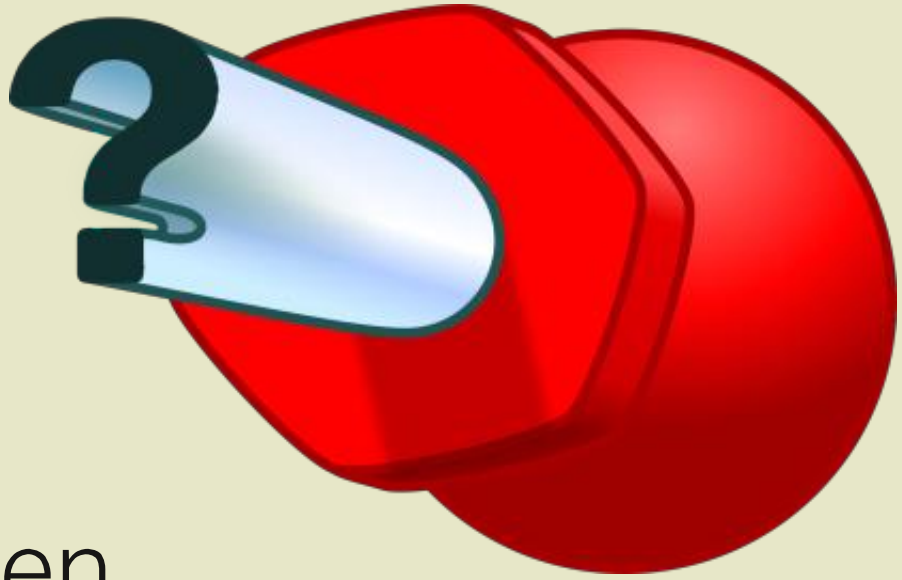
© Franz Gratzer, CC-BY-SA

VGT.at
VEREIN GEGEN TIERFABRIKEN

Nur wenn wir alle vier Freiheiten tatsächlich nutzen können, kann ein Programm Freie Software genannt werden.

© Franz Gratzer, CC-BY-SA

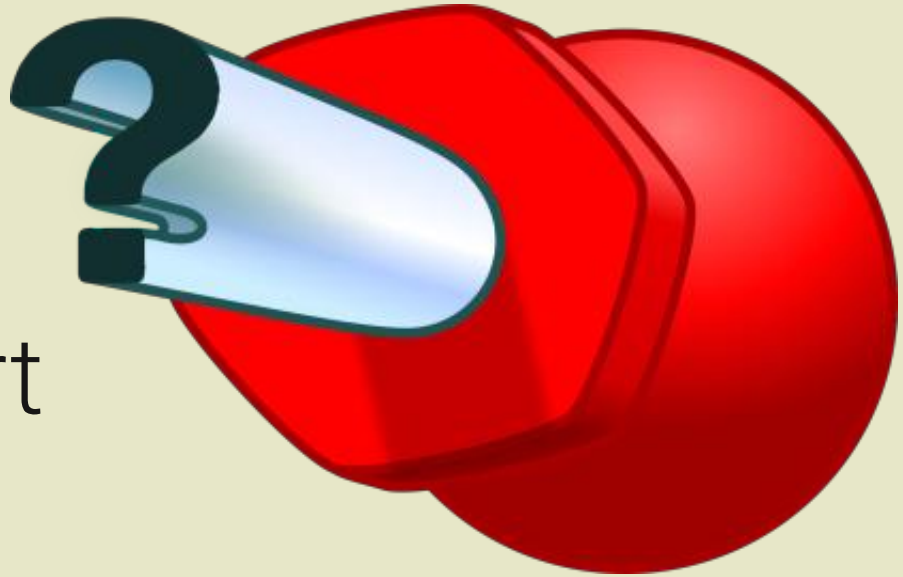
Ein entlarvender Vergleich:



Was würde es bei einem Schraubenzieher bedeuten, ähnlich beschränkt wie Computer zu sein?

 © Franz Gratzer, CC-BY-SA

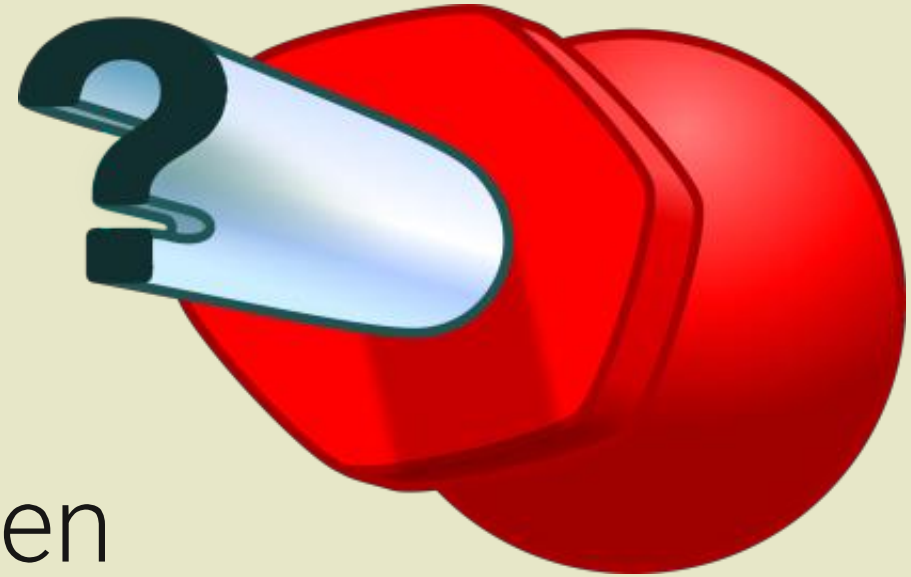
Konsequenz 1:



Schraubenzieher wären nicht mehr standardisiert und würden nur noch zu Schrauben derselben Firma passen.

© Franz Gratzer, CC-BY-SA

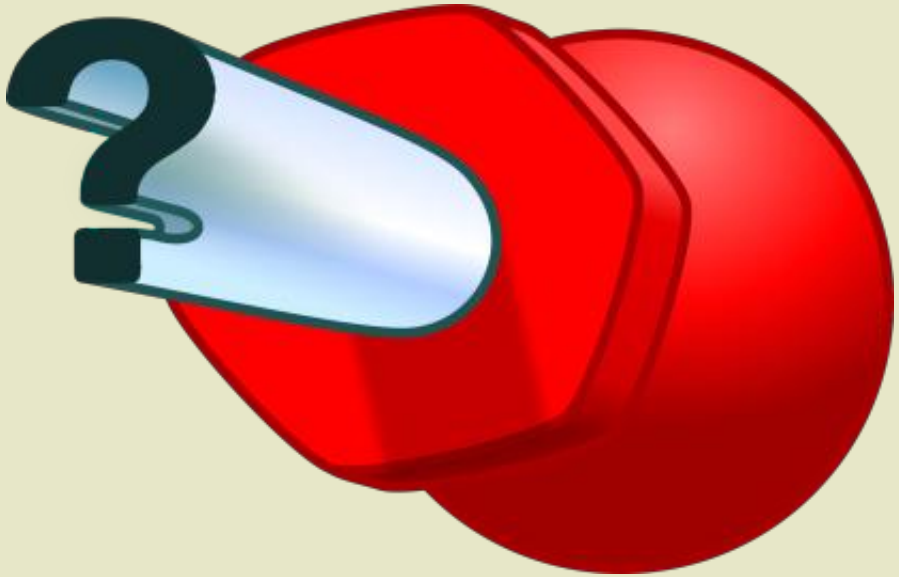
Konsequenz 2:



Schraubenzieher-Lizenzen würden nur das Öffnen von Schrauben erlauben. Zum Festschrauben müssten wir teurere Schraubenzieher dieser Firma kaufen.

© Franz Gratzer, CC-BY-SA

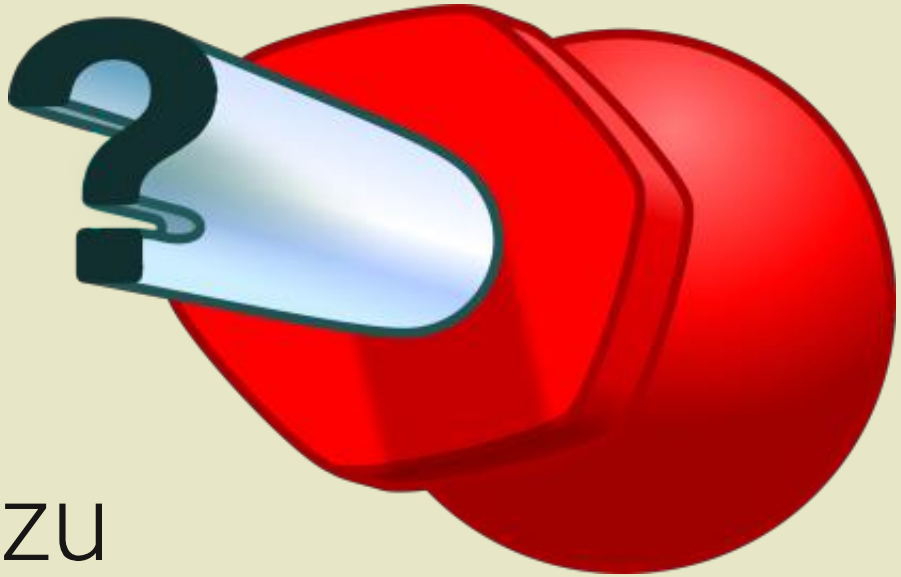
Konsequenz 3:



Nur ein Unternehmen dürfte Schraubenzieher bauen, weil diese Idee patentiert wäre. Das allgemeine Recht Schrauben zum Beispiel auch mit Zangen zu benutzen, müsste erst erkämpft werden.

© Franz Gratzer, CC-BY-SA

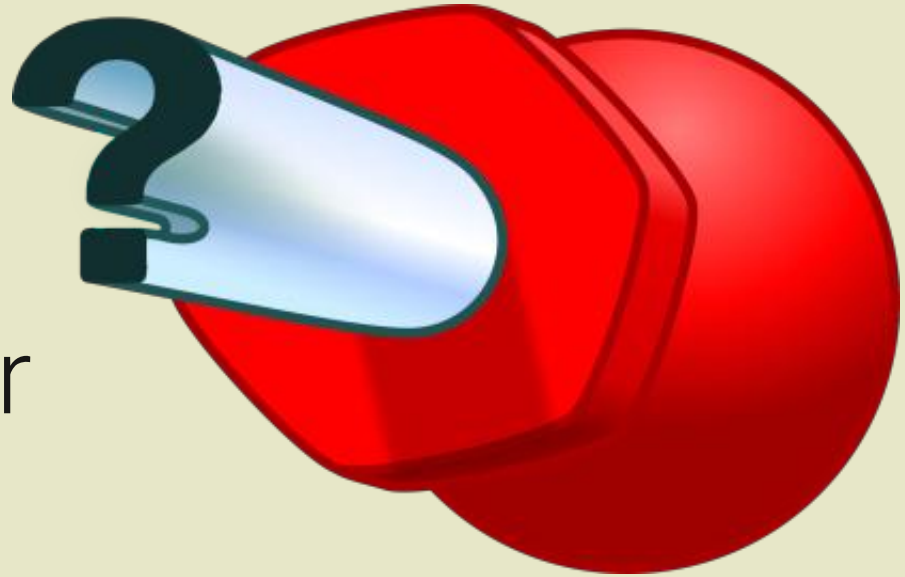
Konsequenz 4:



Es wäre verboten zum Beispiel ein texturiertes Klebeband um den Griff zu wickeln, damit uns der Schraubenzieher nicht so leicht aus der Hand rutscht.

© Franz Gratzer, CC-BY-SA

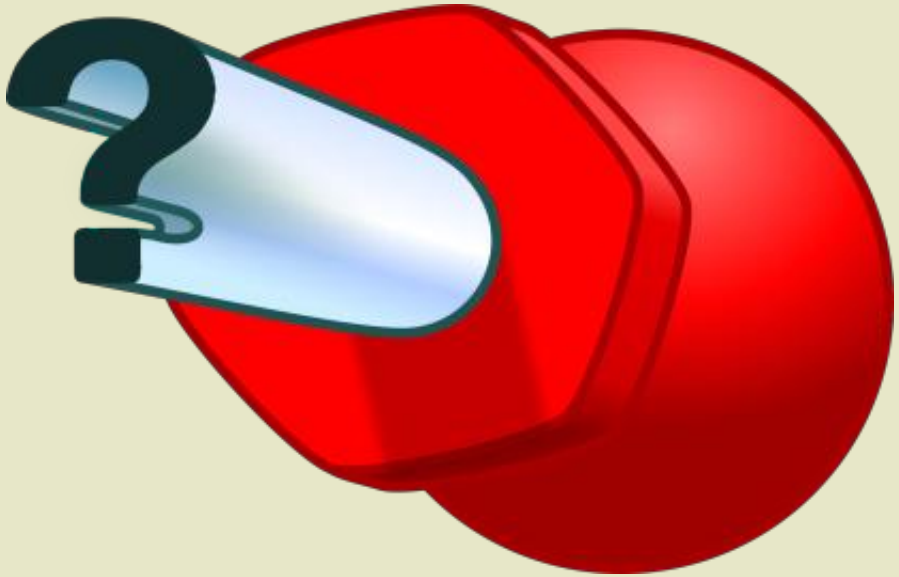
Konsequenz 5:



Es wäre ein Verbrechen, kaputte Schraubenzieher ohne Erlaubnis der herstellenden Firma zu reparieren.

© Franz Gratzer, CC-BY-SA

Konsequenz 6:

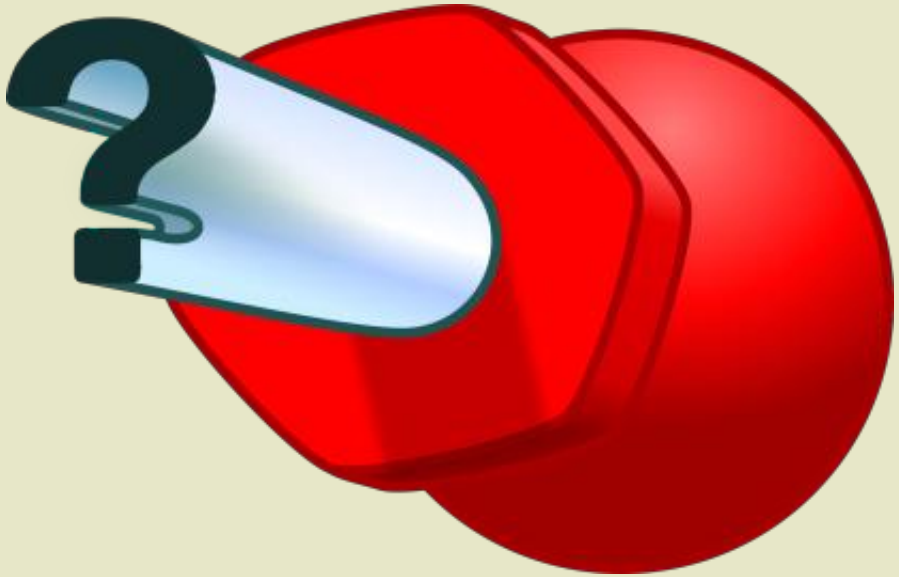


Wir müssten dauernd neue Schraubenzieher und Schrauben kaufen, weil alte nicht mit den neuen Modellen funktionieren.

© Franz Gratzer, CC-BY-SA

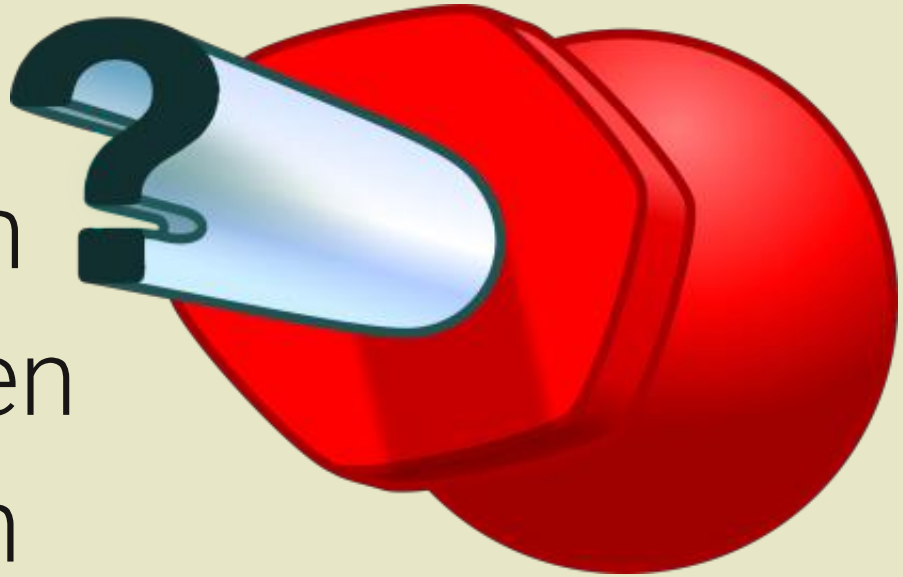
Konsequenz 7:

Es wäre strafbar, Schraubenzieher zu verleihen oder weiter zu verkaufen.



 © Franz Gratzer, CC-BY-SA

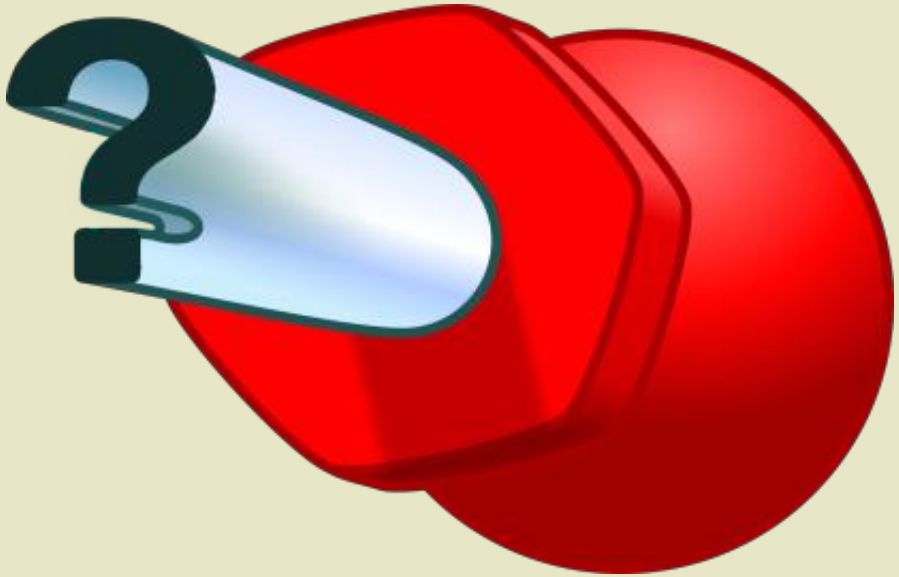
Konsequenz 8:



Schraubenzieher würden uns versteckt überwachen und die so gesammelten Informationen unmerklich an Unbekannte weiter-leiten.

© Franz Gratzer, CC-BY-SA

Niemand würde Schraubenzieher benutzen, deren Verwendung derart beschränkt ist.



Es gibt keinen guten Grund, solche Bedingungen am PC zu akzeptieren!

© Franz Gratzer, CC-BY-SA

DSGVO

- Datensouveränität ist damit nicht gesichert
- SCHIELD-Abkommen ist unzureichend
- Die großen Datensammler wie Google, Meta, Microsoft, Apple, Zoom, etc. können ungehindert weiter machen.

© Franz Gratzer, CC-BY-SA

Mehrere Sicherheitsaspekte

Alle Ebenen der Computer-Sicherheit müssen zusammenwirken. Wenn einzelne Aspekte unberücksichtigt bleiben, sollten wir unserer digitalen Arbeitsumgebung nicht vertrauen. Sicherheitslücken sind leider meist unsichtbar.

© Franz Gratzer, CC-BY-SA

Vier Sicherheitsebenen:

1) Hardware
2) Software
3) Netzwerk
4) Sozial

 © Franz Gratzer, CC-BY-SA

1) Hardware

Gefahren:

- Fremdzugriff über offene Schnittstellen
- Behinderung durch Komponenten
- Datenverlust über kaputte Hardware

 © Franz Gratzer, CC-BY-SA

1) Hardware

Lösungen:

- Alte Geräte (vor Multicore/ME), Libreboot
- Internet nur bei Bedarf aktivieren
- Vor Fremdzugriff schützen
- Regelmäßig Backups erstellen

© Franz Gratzer, CC-BY-SA

2) Software

Gefahren:

- Fremdzugriff durch Hintertüren
- Behinderung durch Sperren
- Datenverlust durch Updates

 © Franz Gratzer, CC-BY-SA

2) Software

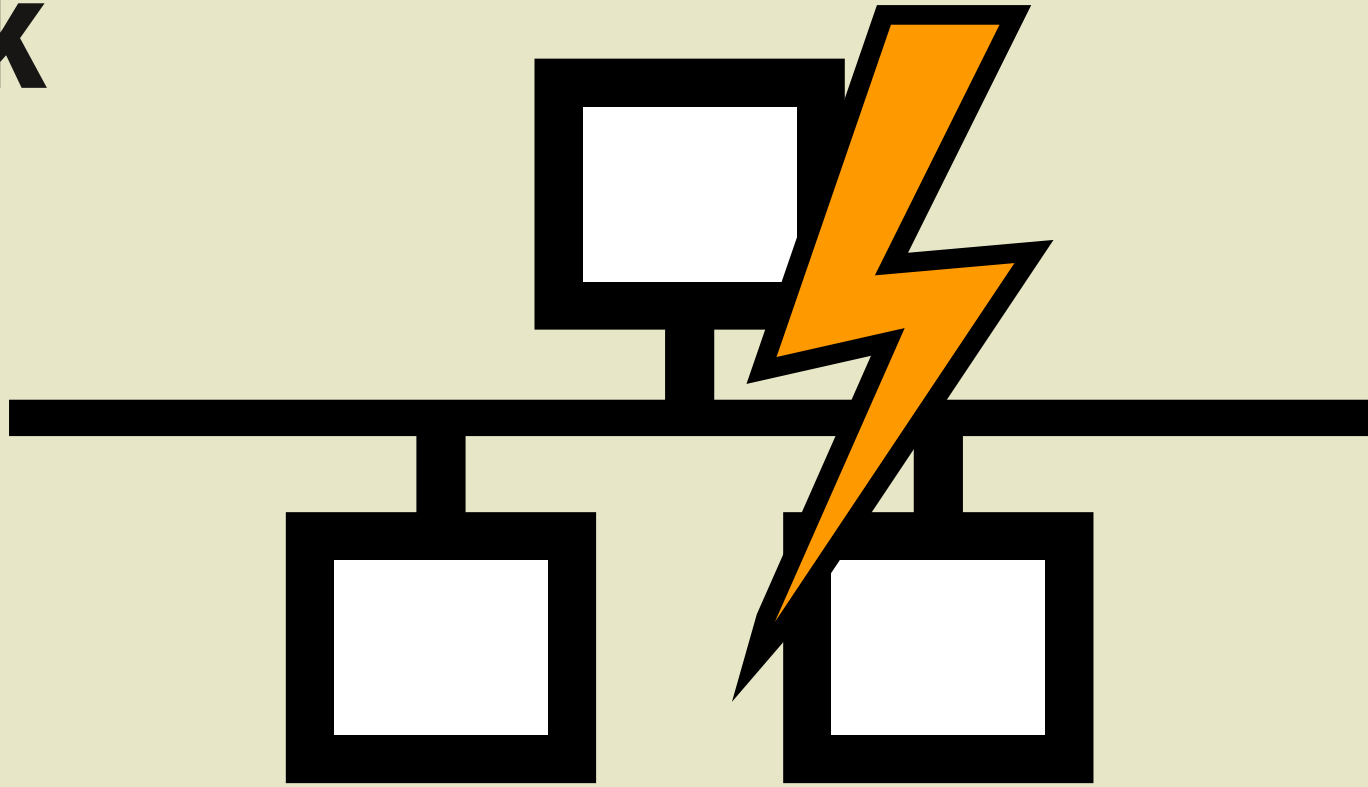
Lösungen:

- Freie Software
- Verschlüsselung
- Offene Standards (Austauschformate!)
- Regelmäßige Backups

 © Franz Gratzer, CC-BY-SA

3) Netzwerk

Gefahren:



- Fremdzugriff
- Behinderung
- Überwachung
- Unerreichbare Server-Daten

 © Franz Gratzer, CC-BY-SA

3) Netzwerk

Lösungen:

- Verschlüsselung
- „Dezentrale“ Netze bevorzugen
- Netzwerklösungen nur wo wirklich nötig
- Unabhängige/lokale Backups

© Franz Gratzer, CC-BY-SA

4) Sozial

Gefahren:

- Fremdzugriff
- Schwache oder verratene Passwörter
- Schadsoftware über Sticks & Downloads
- Geschlossene Dateiformate (Kooperation)

© Franz Gratzer, CC-BY-SA

4) Sozial

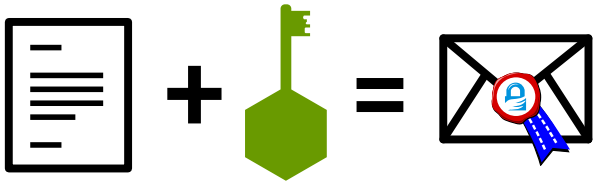
Lösungen:

- Gute Passphrasen verwenden
- Zugangsdaten geheimhalten
- Geräte im Auge behalten, Userprofile
- Auf Nutzung offener Standards bestehen

© Franz Gratzer, CC-BY-SA

So funktioniert GnuPG

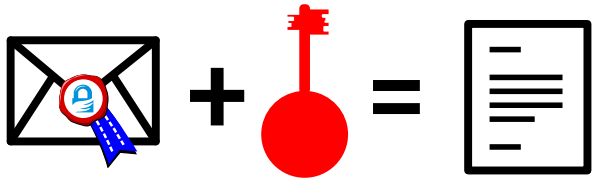
öffentlicher Schlüssel



verschlüsseln

Damit andere Menschen Ihnen verschlüsselte E-Mails senden können, benötigen diese Ihren „öffentlichen Schlüssel". Es gilt daher, je weiter Sie ihn verbreiten, desto sinnvoller.
Seien Sie unbesorgt: Ihr öffentlicher Schlüssel kann nur zum Verschlüsseln, nicht aber zum Entschlüsseln verwendet werden.

privater Schlüssel



entschlüsseln

Ihr „privater Schlüssel" ist wie ein Hausschlüssel, den Sie sicher auf Ihrem Computer verwahren. Achten Sie darauf, dass nur Sie Zugriff darauf haben.
Sie nutzen GnuPG und Ihren privaten Schlüssel, um an Sie verschlüsselte E-Mails wieder zu entschlüsseln und lesen zu können.

© Franz Gratzer, CC-BY-SA

Welches Passwort ist besser?

A) Wichtig sind vor allem Sonderzeichen.

Bum Beispiel: "**#*ä_:9W**"

B) Wichtig ist vor allem die Länge.

Zum Beispiel: "**aaklcnmaueondfknabu**"

© Franz Gratzer, CC-BY-SA

Exkurs Passphrasen 1

- Merkbarkeit & Länge sind am wichtigsten
- Mind. 12 Zeichen bzw. 5 zufällige* Wörter

*) siehe diceware-Link am Ende

- Groß-/Klein, Ziffern, Satzzeichen
- Beispiel: „w!_di1P,di?ü347/18mvh“

wichtig**! _ d**as **i**st **1 P**hrase**, d**ie **i**ch**? ü**ber **347/18 m**al **v**erwendet **h**abe

© Franz Gratzer, CC-BY-SA

Exkurs Passphrasen 2

- Immer nur für einen Account verwenden
- Geheimes System statt einzelne Phrasen
- Im Bedarfsfall nur mit Fehlern notieren
- Nie verraten bzw. danach ändern
- Passwortmanager verwenden oder üben

© Franz Gratzer, CC-BY-SA

Tipps fürs Homeoffice

Möglichst eigene Infrastruktur verwenden:

- Video: Jitsi meet, BigBlueButton, GNU Jami
- Audio: Mumble, Ekiga
- Dokumente/Text: Etherpad, Nextcloud

© Franz Gratzer, CC-BY-SA

Handys

- Mobilgeräte sind grundsätzlich unsicher
- Verschlüsselung über Signal hilft etwas
- Peilung ist trotzdem unüberwindbar

© Franz Gratzer, CC-BY-SA

Ziel: Selbstbestimmung

Freie Software und offene Standards sind nicht nur ein politisches Statement für Unabhängigkeit. Auch wo Freie Software mühsamer ist, stellt sie die einzige Chance für Systeme dar, die nicht grundsätzlich fremdbestimmt funktionieren.

© Franz Gratzer, CC-BY-SA

Wichtig

Eine Kette ist nur so stark wie ihr schwächstes Glied.

Besser einfache Maßnahmen zur Computersicherheit zuverlässig umsetzen, als uns mit komplizierten zu plagen!

© Franz Gratzer, CC-BY-SA

Nützliche Links 1

- duckduckgo.com
- emailselfdefence.fsf.org
- directory.fsf.org
- rempe.us/diceware
- vgt.at/aktiv/it-sicherheit

 © Franz Gratzer, CC-BY-SA

Nützliche Links 2

- fairmeeting.net
- buergernetzwerk.at
- vgt.at/kommunikation
- freie.it
- tehnoetic.com

Fragen gerne an: **franz.gratzer@vgt.at**

© Franz Gratzer, CC-BY-SA