Computersicherheit für Aktive

VGT.at
VEREIN GEGEN TIERFABRIKEN

Warum rede ausgerechnet ich über Computersicherheit?

- kein Techniker
- engagiert für Freie Software
+ Erfahrungen als Aktivist
+ Tierschutzprozess miterlebt

Was meine ich mit „Computer-Sicherheit“?

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

Verstandlose Diener

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

Wer ist in Kontrolle?

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

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 nicht unseren Bedürfnissen anpassen.

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.

Die vier Sicherheitsebenen:

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

1) Hardware

Gefahren:

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

1) Hardware

Lösungen:

- alte Geräte (vor Multicore/ME), Libreboot Bios
- Internetverbindung nur bei Bedarf aktivieren
- vor Fremdzugriff schützen
- regelmäßig Backups erstellen

2) Software

Gefahren:

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

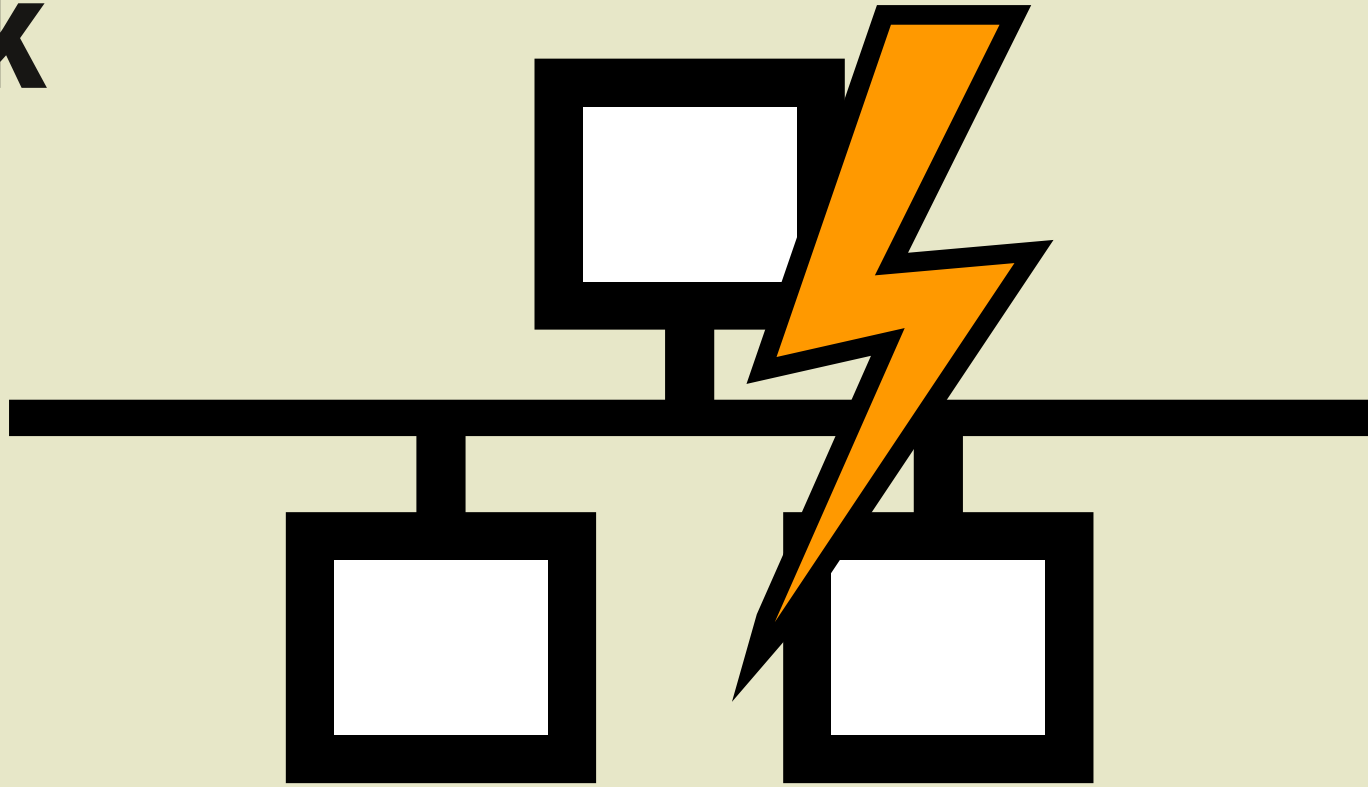
2) Software

Lösungen:

- Freie Software
- Verschlüsselung
- offene Standards (Austauschformate!)
- regelmäßige Backups

3) Netzwerk

Gefahren:



- Fremdzugriff
- Behinderung
- Überwachung
- unerreichbare Server-Daten

3) Netzwerk

Lösungen:

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

4) Sozial

Gefahren:

- Fremdzugriff
- schwache oder verratene Passwörter
- Schadsoftware über Sticks oder Downloads
- geschlossene Dateiformate (Kooperation)

4) Sozial

Lösungen:

- gute Passwörter verwenden
- Zugangsdaten geheimhalten
- Geräte im Auge behalten, Userprofile
- auf offene Standards beharren

Exkurs zu Passphrasen 1

- mindestens 12 Zeichen lang
- Buchstaben, Ziffern, Satzzeichen
- nichts was in Wöterbuchern vorkommt!
- 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

Exkurs zu Passphrasen 2

- tippen statt Passwortmanager (vergessen ...)
- nicht mehrfach und/oder ewig verwenden
- geheimes System statt einzelne Phrasen
- im Bedarfsfall nur mit Fehlern notieren
- nie verraten bzw. gleich danach ändern

Handys

Mobilgeräte sind leider grundsätzlich unsicher.
Verschlüsselung macht es zwar etwas besser,
aber bitte nie davon ausgehen, dass Mobil-
geräte tatsächlich vertrauenswürdig wären!
Betrachten wir sie besser als Turbo-Wanzen!

Ziel: Selbstbestimmung

Der Einsatz Freier Software und offener Standards ist nicht nur ein politisches Statement für Unabhängigkeit. Auch wenn Freie Software manchmal mühsamer scheint, so ist sie trotzdem die einzige Chance für Systeme, die nicht grundsätzlich fremdbestimmt funktionieren.

Kontakt für weitere Fragen:

franz.gratzer@vgt.at

Nützliche Links:

freie.it, directory.fsf.org, emailselfdefence.org, tehnoetic.com, duckduckgo.com