IT-Sicherheit? Freie Software!

Wie Offenheit zu Sicherheit beiträgt

Max Mehl – Programmmanager – @mxmehl

27. April 2019 – Grazer Linuxtage

fsfe

Die Free Software Foundation Europe ist ein gemeinnütziger Verein, der es Menschen ermöglicht, ihre Technik zu kontrollieren.

Freie Software

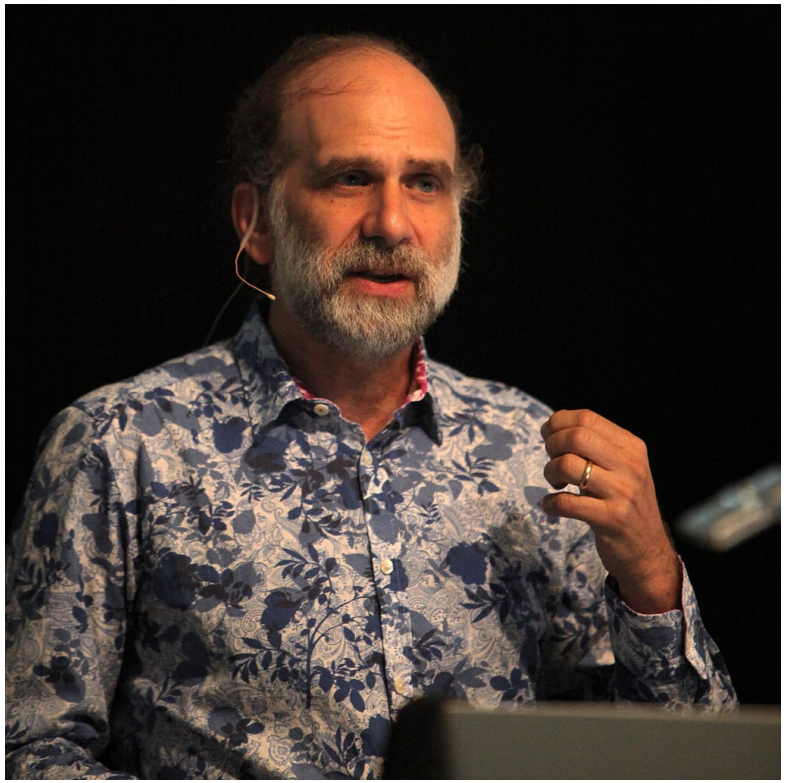
Verwenden
Die Software kann für jeden Zweck verwendet werden, ohne Einschränkungen.

Verstehen
Die Software kann uneingeschränkt untersucht werden.

Verbreiten
Die Software kann uneingeschränkt kopiert und weitergeben werden.

Verbessern
Die Software kann vom Nutzer oder anderen verbessert und verändert werden.

Was ist IT-Sicherheit?



„Security is not a product;
it itself is a process.“

– Bruce Schneier in „Secret & Lies“, 2000

Photograph by Rama, Wikimedia Commons, Cc-by-sa-2.0-fr

fsfe

IT-Sicherheit als Prozess

fsfe

1

Das Offensichtliche

Codefehler

Verschlüsselung

Fehlerbehebung

2

Der zweite Blick

Bibliotheken

Faktor Mensch

Customisation

3

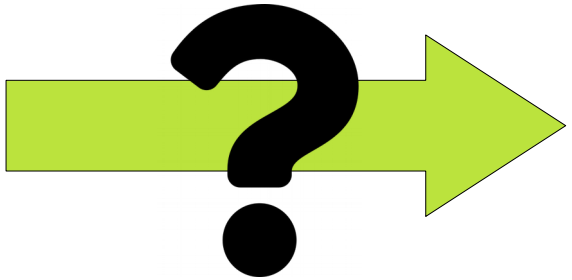
Fiese Details

Firmenstrategie

Supportzyklen

Haftung


AGPL v3
Free Software
LGPL v3
Free Software
GPL v3
Free Software

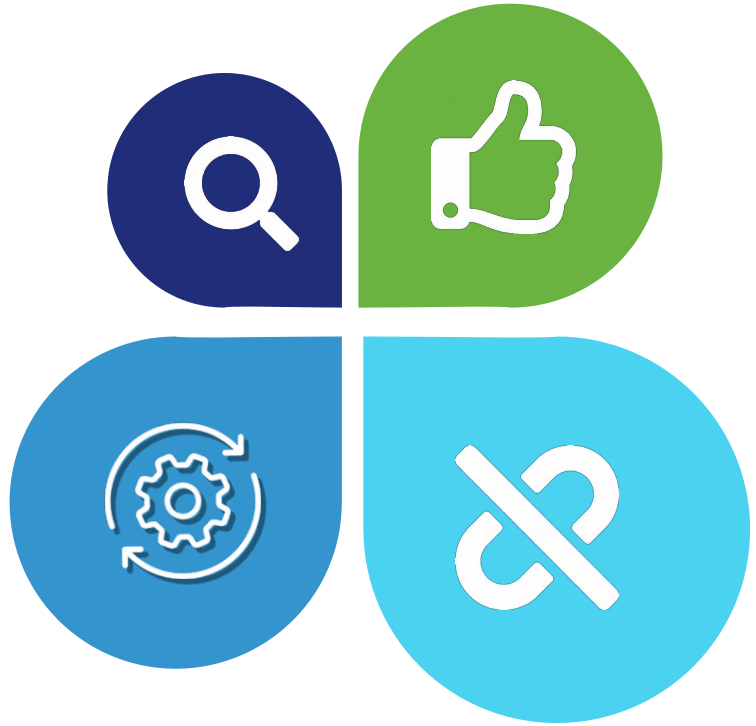


fsfe

Sicherheitsvorteile Freier Software

Transparenz für alle
Unabhängige Sicherheits-überprüfungen erhöhen Vertrauen, auch intern.

Synergie durch Teilen
Andere Nutzer und Community haben Interesse und steuern Mittel bei.



Druck von außen
Wenn der Code öffentlich gemacht wird, schaut man besser genauer hin.

Unabhängigkeit
Probleme können selbst gelöst werden, notfalls ein Projekt alleine weitergeführt werden.

Freie Software ist eine notwendige, aber nicht hinreichende Komponente von IT-Sicherheit

fsfe

Abwägungen

Zuständigkeiten

Wer ist für Sicherheit verantwortlich bei geteilten Projekten? Wie wird mit externen Bibliotheken umgegangen?

Grad der Wiederverwendung

Nutzung von vielen externen FS-Bausteinen, oder kleinere aber selbsterstellte Software?

„Nationale Sicherheit“

Gibt es Software, bei der es nachteilig wäre, sie zu veröffentlichen?

Andere Komponenten

Freie Hardware, Reproduzierbarkeit und andere Sicherheitsprozesse sind ebenfalls wichtig.

Häufige Gegenargumente

„Freie Software nur bei nicht-kritischen Dingen!“

Nein, gerade bei kritischer und öffentlicher Infrastruktur sind Vertrauen und offene Prozesse elementar.

Freie Software nur was von und für Hobbyisten

Nein, siehe Linux Kernel, RedHat, Apache, Microsoft, Virtualisierung, CMS...

Öffentlicher Quelltext = Risiko

Nein, „Security through obscurity“ ist mehrfach widerlegt worden. Quelltext kann oft rekonstruiert werden.
→ Kerckhoffs‘ Prinzip

Geschäftsgeheimnisse

Jein, bei vielen Geschäftsmodellen ist das aber kein Problem, sogar vorteilhaft.

Beispiel Huawei

Bedenken bei 5G-Infrastruktur

- Freie Software fördert Vertrauen
- Unabhängige Untersuchung möglich
- Behörden können Arbeit aufteilen
- Konkurrenz als zusätzlicher Druck
- Außerdem wichtig: Reproduzierbarkeit, freie Hardware
- Unrealistisch? Jetzt vielleicht ja, aber mittel- und langfristig nicht.

Vorteile Freier Software

Danke!

Danke an alle Unterstützer der FSFE, die unsere Arbeit ermöglichen. Sei auch dabei!

fsfe.org/support

Max Mehl | max.mehl@fsfe.org | @mxmehl (Mastodon, Twitter...)