GNU Privacy Guard

Funktionsweise und Nutzung

A. Kaiser T. Diebelt

Hochschule für Technik, Wirtschaft und Kultur

15.01.2021

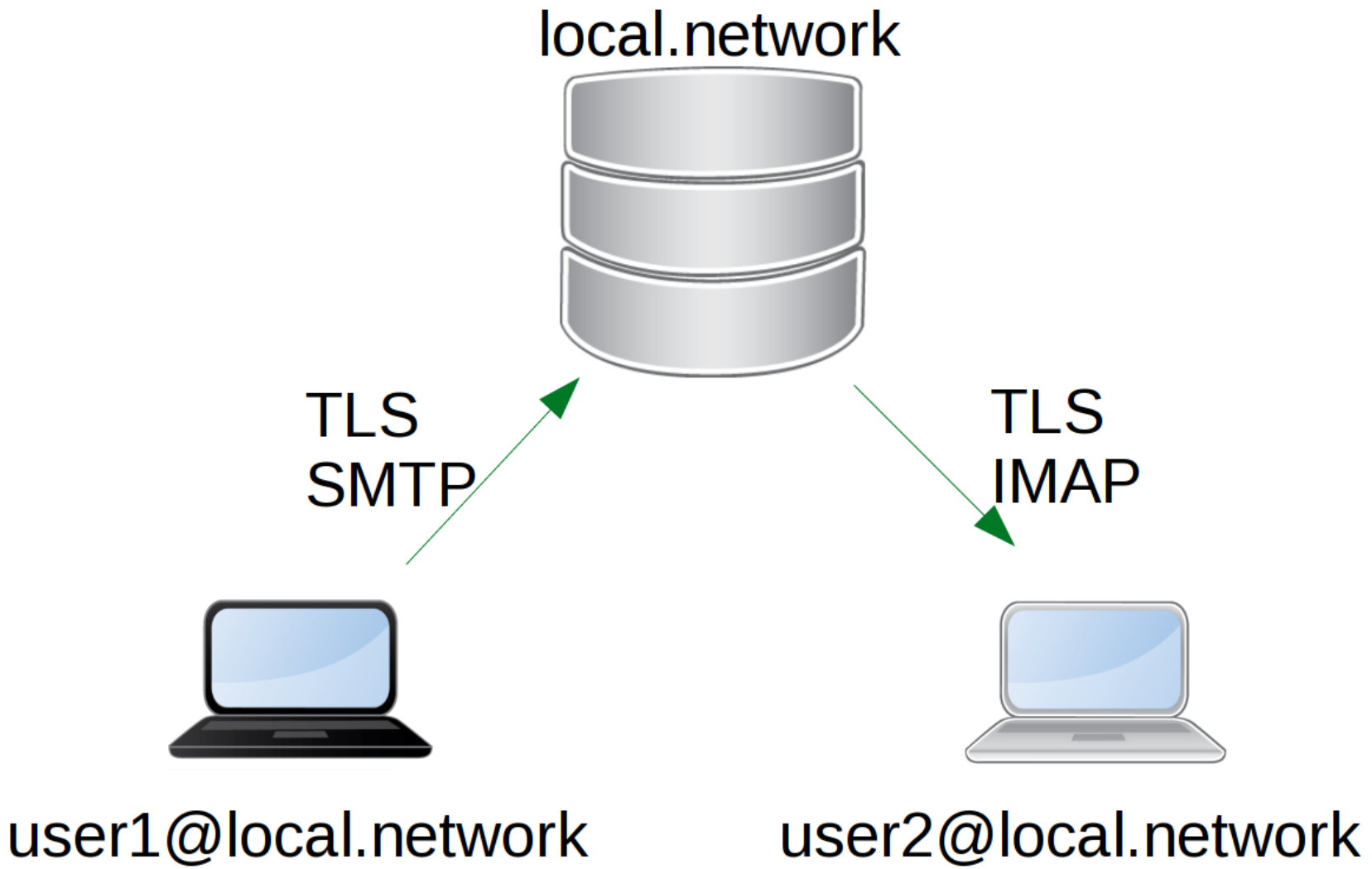
HTWK

GNU Privacy Guard

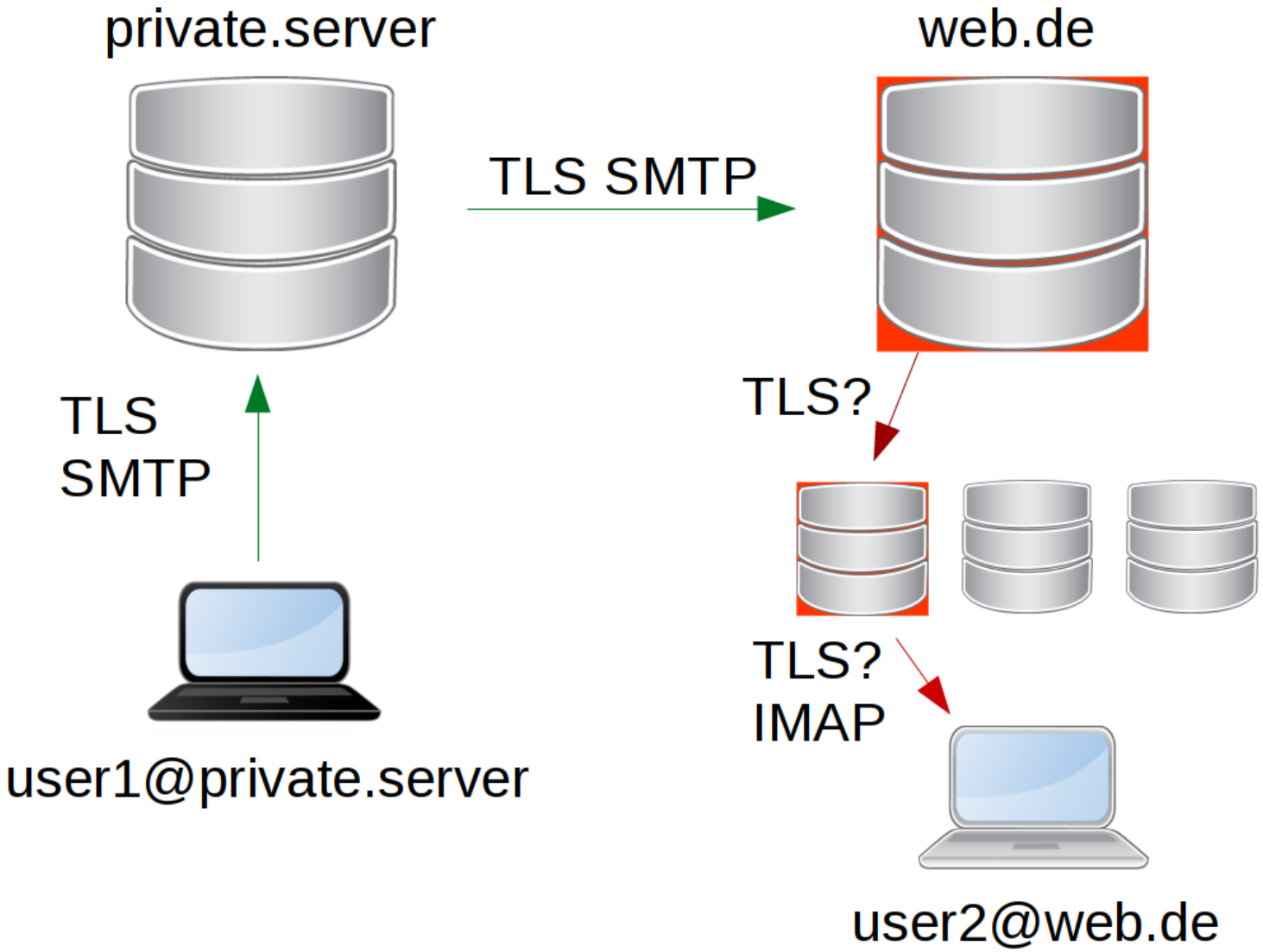
Motivation:

- abhörsichere Kommunikation (gegen Spionage)
- Privatsphäre

Mail-Verkehr im Privaten Netzwerk



Mail-Verkehr mit fremden Servern



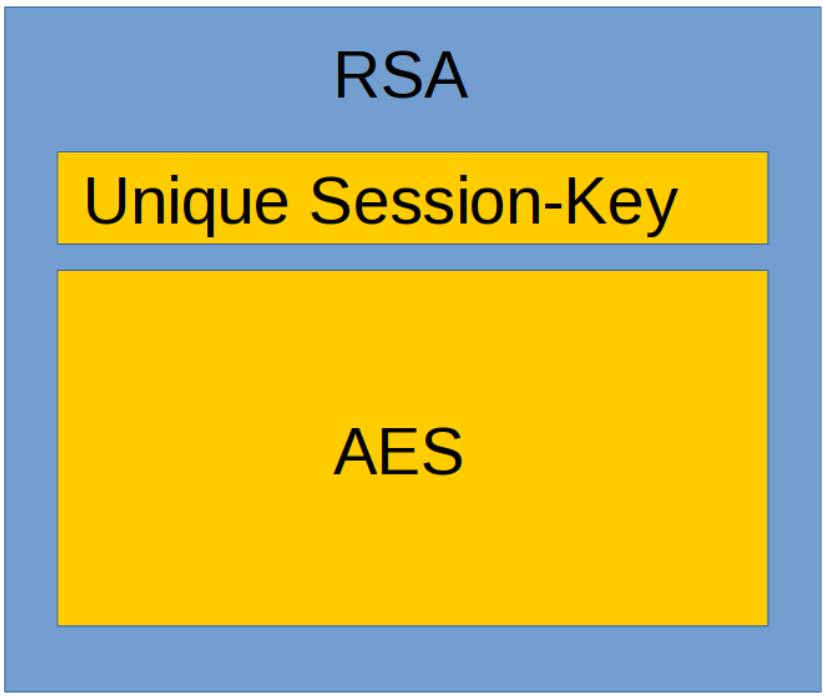
eMail-Versand mit Ende-zu-Ende-Verschlüsselung

- Pretty Good Privacy (PGP)
  - Symantec, 1991
  - Lizenz: Commercial proprietary software
  - OpenPGP standard
- Secure/Multipurpose Internet Mail Extensions (S/MIME)
  - RSA Data Security, 1996
  - Erweiterung des Mail-Standards ('application/pkcs7-mime')

Laut Electronic Frontier Foundation (EFF), Mai 2018:
Kritische Sicherheitslücken, schwer zu beheben ('EFAIL')

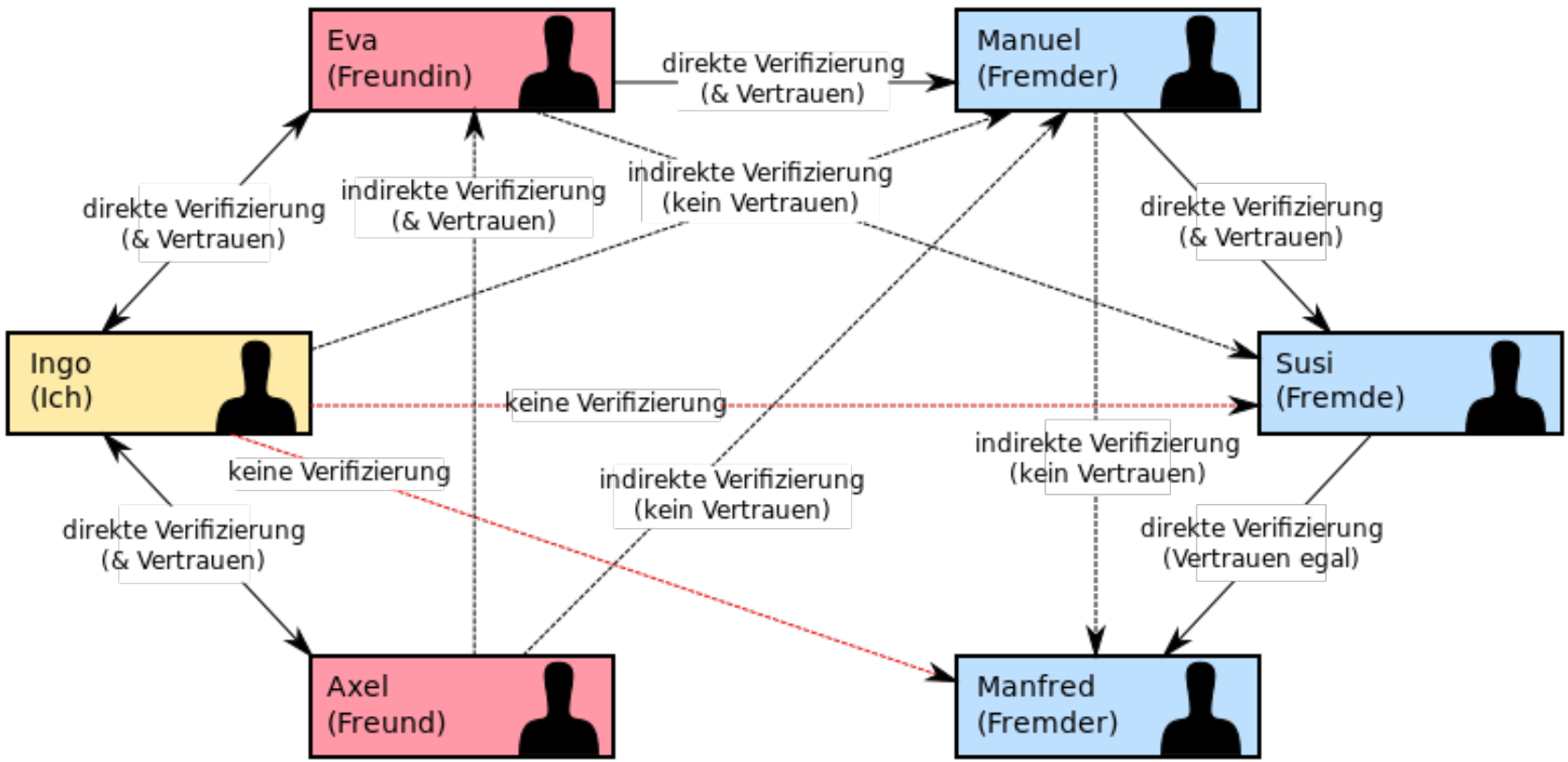
GNU Privacy Guard

- GNU Project, 1999
- Lizenz: GNU GPLv3 (FOSS!)
- Kompatibel mit OpenPGP
- Nutzt Hybrid aus Asymmetrischer und Symmetrischer Verschlüsselung
- Ermöglicht Signierung und/oder Verschlüsselung von Daten



Web-Of-Trust

- Begriffsdeutung



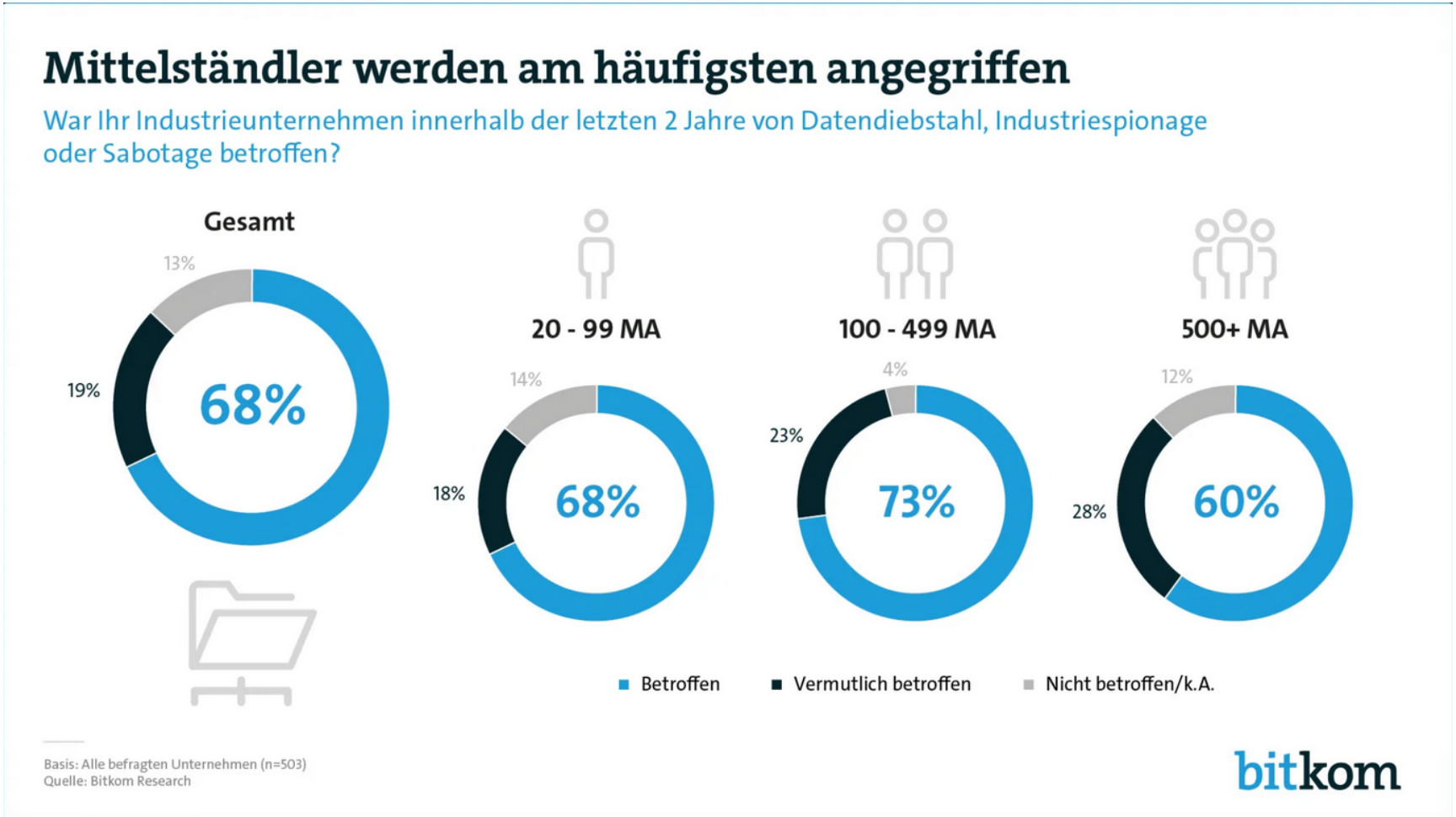
- Differenz zu PKI

HTWK

Risiken und Schäden

- WISKOS-Studie 2018: 100 Mrd Schaden
- “Unternehmen sollten E-Mail-Kommunikation auslagern“
- bitkom: mehr 53% der Unternehmen betroffen
- 41% der Informationen über E-Mail erlangt

Betroffene Unternehmen



Betroffene Daten

- Allgemeine E-Mails
- Finanzdaten (36%)
- Kundendaten (17%)
- Patente/Forschung (11%)
- Mitarbeiterdaten (10%)

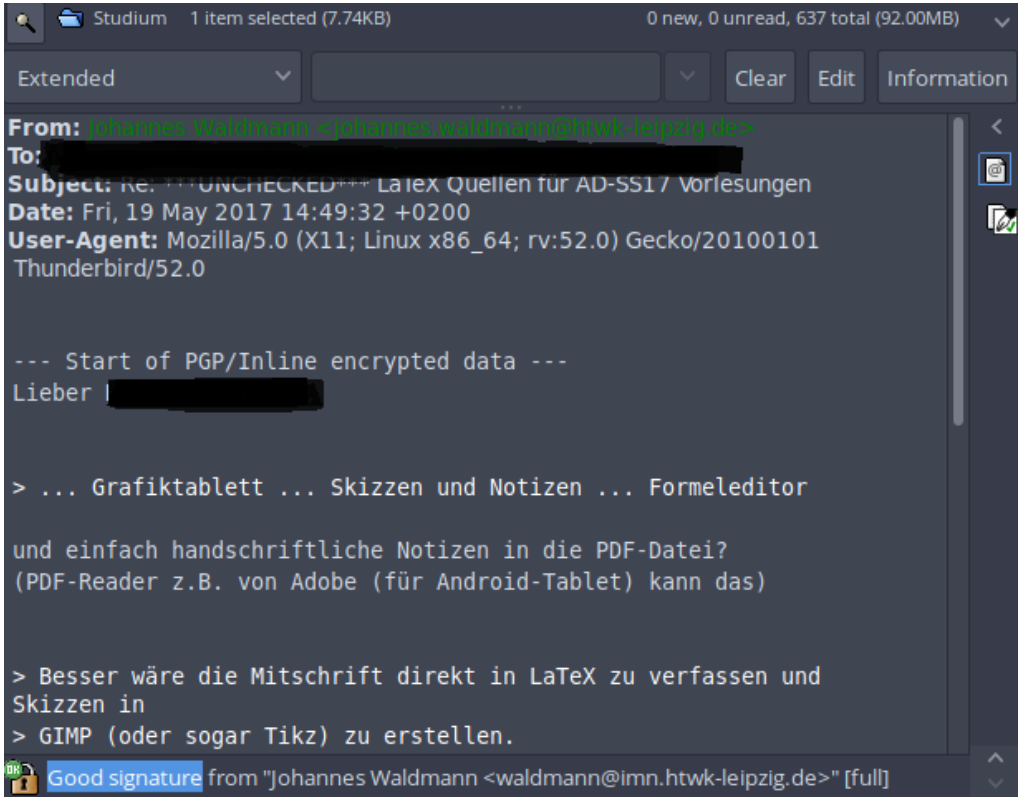
Täter

- ehemalige Mitarbeiter (62%)
- Kunden / Mitbewerber (41%)
- Hobbyhacker (21%)
- organisierte Kriminalität (7%)
- nur 1/3 der Angriffe aus Deutschland

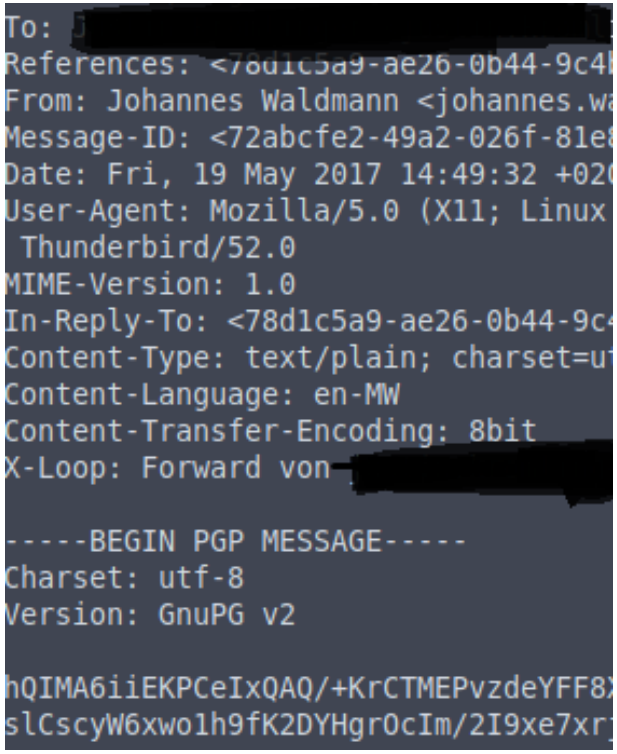
Beispielhafte Verwendung

```
$ gpg --gen-key
```

Nutzung in Mail-Clients



(a) Ansicht im Mail-Client

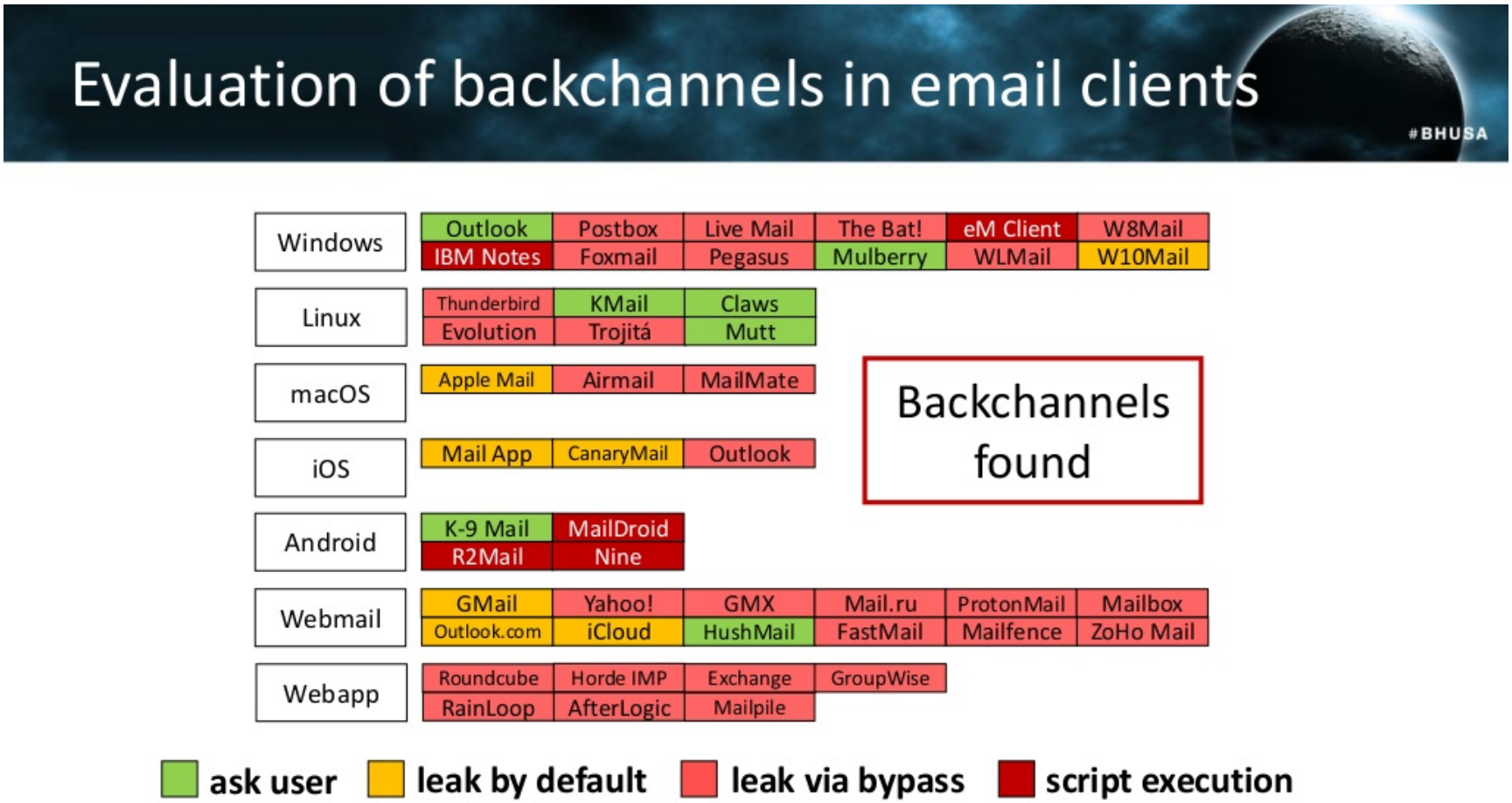


(b) Quellcode

HTWK

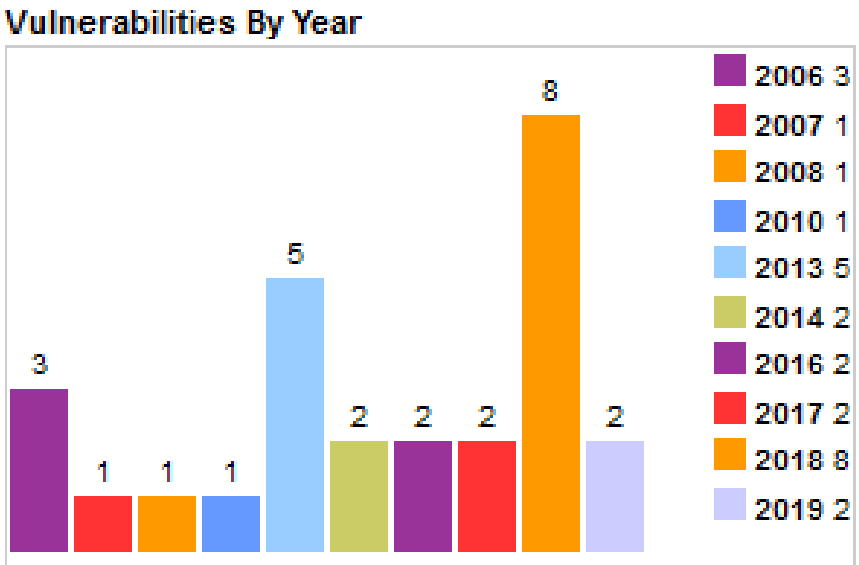
Sicherheitsrisiken

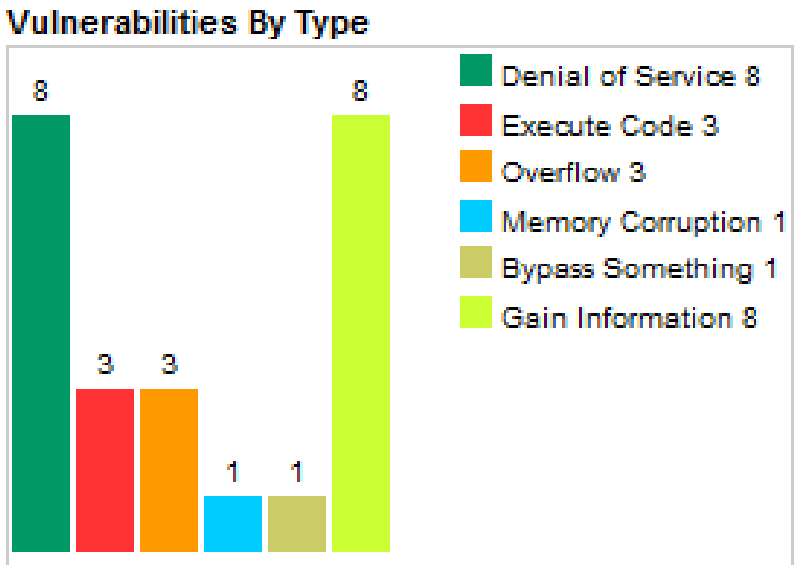
- Nutzer
  - Fehlerhafte Benutzung / Einrichtung
  - Nutzung inkonsequenter E-Mail-Programme



Sicherheitsrisiken

- GnuPG
  - unbekannte Lücken
  - CVE-2016-6313
  - CVE-2017-7526
  - SigSpoof





HTWK

Sicherheitsrisiken

- Regierungen
  - https://fm4.orf.at/stories/3008930/
  - Generalschlüssel für E2E-verschlüsselten Chats

Fazit

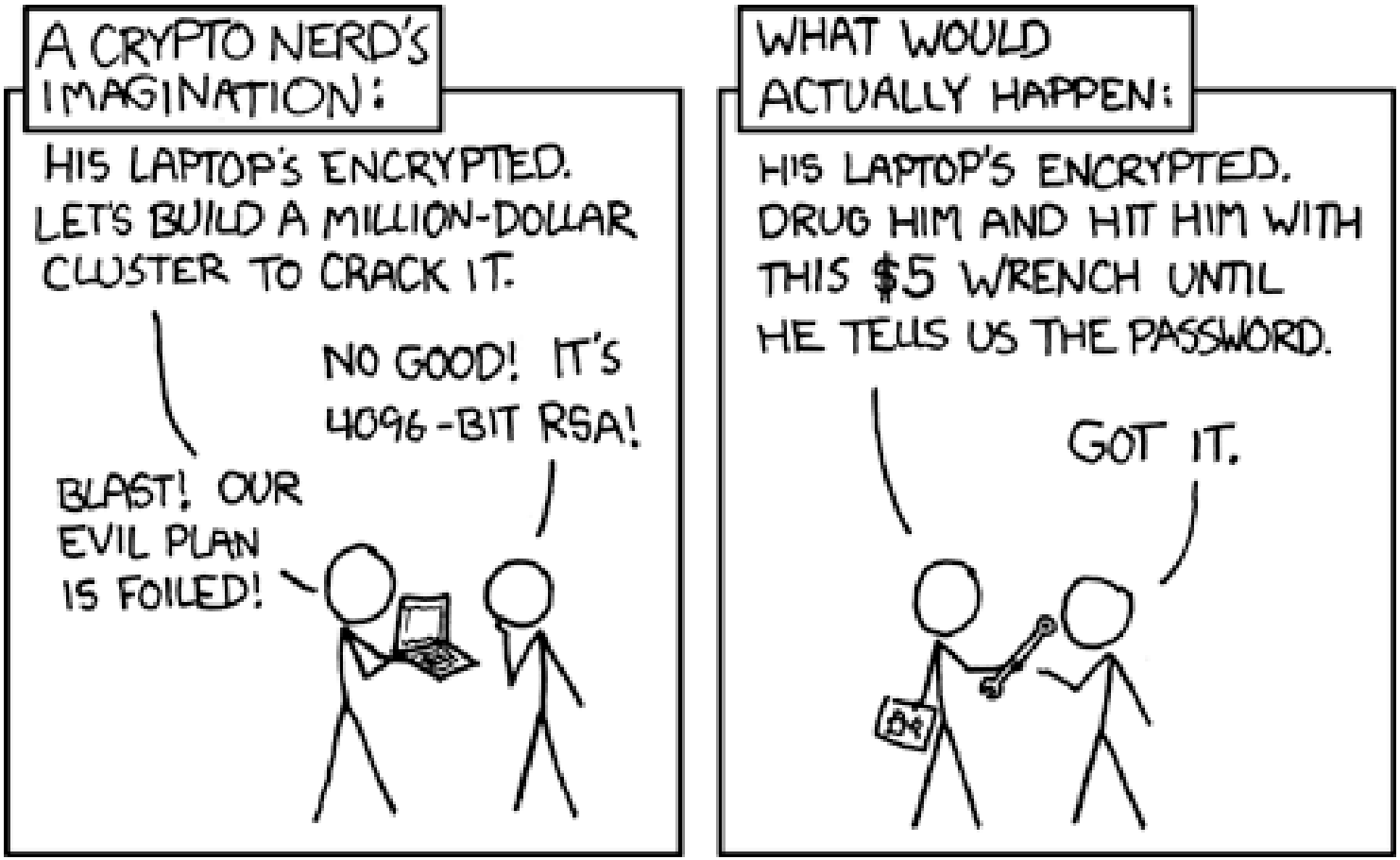
- Betrieblicher Mehrwert:
  - Bei korrekter Anwendung spart man Geld
  - technische Bildung
- Allgemeiner Mehrwert:
  - Privatsphäre
  - Umstieg auf sichere Systeme
  - Schutz vor Überwachungskapitalismus → https://www.imn.htwk-leipzig.de/waldmann/talk/19/ubkap/

Zitat von der Bitkom-Studie

»Gut geschulte Mitarbeiter sind der effektivste Schutz. So lassen sich unbeabsichtigte Schäden vorbeugen, Angriffe von außen werden besser abgewehrt und sind sie doch erfolgreich, lässt sich schnell gegensteuern.«

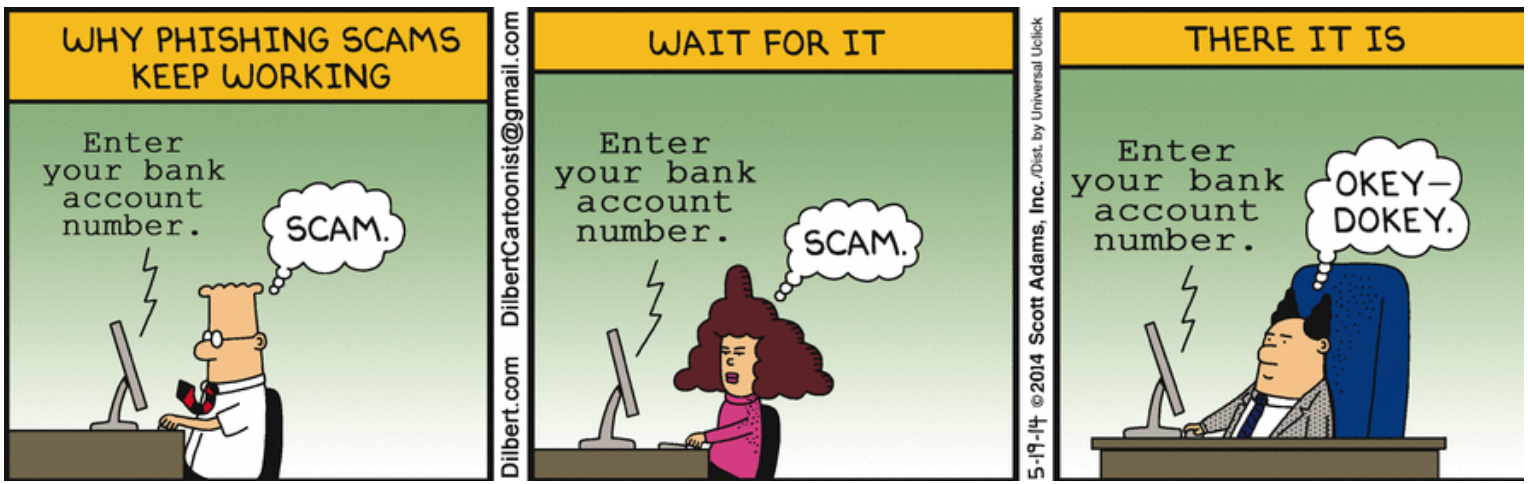
Achim Berg, Bitkom-Präsident, Berlin 2020

Memes



https://xkcd.com/538/

Memes



https://i.pinimg.com/originals/f6/78/7d/f6787d977847056dd8701707d5ba5c5b.gif

Literaturnachweis I

- https://en.wikipedia.org/wiki/Pretty_Good_Privacy
- https://en.wikipedia.org/wiki/S/MIME
- https://medium.com/@cipherpunk/efail-a-postmortem-4bef2cea4c08
- https://en.wikipedia.org/wiki/GNU_Privacy_Guard
- https://www.slideshare.net/cisoplatform7/efail-breaking-smime-and-openpgp-email-encryption-using-exfiltration-channels
- https://media.ccc.de/v/35c3-9463-attacking_end-to-end_email_encryption#t=295
- https://de.wikipedia.org/wiki/Datei:Web_of_Trust_2.svg
- https://www.cvedetails.com/vendor/4711/Gnupg.html

Literaturnachweis II

- https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf
- https://www.infopoint-security.de/wirtschaftsspionage-wiskos-studie-beziffert-schaden-bei-kmus-auf-100-mrd/a18166
- https://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/presse/p20170721-bfv-bitkom-vorstellung-studie-wirtschaftsspionage-sabotage-datendiebstahl
- https://www.heise.de/news/Terrorbekaempfung-und-Verschluesselung-EU-Rat-forciert-umstrittene-Crypto-Linie-4960069.html
- https://efail.de/
- https://wiki.archlinux.org/index.php/GnuPG