Heute: **digitale Selbstverteidigung: E-Mails privat**

Clemens Schweigler
ak-digit@bv-schwarzwald.vdi.de

- vertrauliche Kommunikation, Schwachstellenanalyse
- Lösungen, Thunderbird – Addons – Einstellungen
- PGP Grundlagen & How-to

Schwerpunkt meines Ehrenamts im VDI und FLUG
ist das Bewusstsein zu schaffen und Unterstützung zum
Thema Informationssicherheit und Datenschutz

Zuerst etwas Erwartungsmanagement:

Es gibt keine einfache Lösung für Alle...

Umfrage: Wo haben Sie von dieser Veranstaltung zuerst gehört?

Badische Zeitung → B
CCC / FLUG-Umfeld → C
VDI → D
Andere / Sonstige → A

Digitale Selbstverteidigung: vertrauliche E-Mails

VDI-Flug Vortragsserie:

- Weshalb Datenschutz?,
- Alternative Linux,
- Passwörter,
- Browser,
- **Sichere E-Mail,**
- Linux unter der Haube

1) Überblick
2) vertrauliche Kommunikation
3) Schwachstellenanalyse
4) erste Lösungen
5) Thunderbird
6) Pretty Good Privacy Grundlagen
7) PGP Einladung
8) Ausblick & Disclaimer

2) vertrauliche Kommunikation

IST
- keine Postkarte, kein Fax (obwohl als Schriftform rechtsverbindlich)
- keine SMS, kein Flur-Funk,
- keine closed Source oder veraltete HW & SW

Vertraulichkeit = nicht von außen einsehbarer (digitaler) Raum.
Ist **ein** "Guckloch" vorhanden, ist die Privatheit dahin.

dh. **alle** Gucklöcher (=Schwachstellen) müssen geschlossen werden!
In diesem Sinne ist auch IT-Sicherheit ein fortlaufender Prozess,
da immer neue Schwachstellen auftauchen werden.

Man unterscheidet grob zwischen technisch fehlerfreiem Funktionieren
und per Definition schützenswerten Inhalten.

Dies erfordert technische (eingebaute) wie organisatorische (machen!)
Vorkehrungen, was Inhalt des Vortrags mit Fokus auf den Privatanwender ist.

3) Schwachstellenanalyse

wunderfitzige Menschys:
- klicken auf alles zapplige und Bunte, was nicht bei drei auf den Bäumen ist…
- unbekannte Links, lustige Anhänge, wichtige must-have Downloads, Werbung…
- Phishing-Mails, aktive Inhalte
- "bequeme" Einstellungen & fiese Gewohnheiten
- löchrige Verkehrswege, Hard-& Software
- Kombination von Allem

Eine Nachricht muss erst be- und verarbeitet werden, bevor sie verschlüsselt wird. Vorrangig sollten erst die vorgelagerten Lücken geschlossen sein, bevor ein zusätzlicher Verschlüsselungsaufwand geleistet wird.
Unterwegs muss die Verschlüsselung dann durchgängig sein: d.h. Ende-zu-Ende-Verschlüsselt.
Eine PGP Ende-zu-Ende-verschlüsselte Nachricht benötigt zum knacken einen sehr erheblichen Aufwand: viel einfacher/billiger ist das Ausnutzen anderer Schwachstellen.

Wenn das nicht hilft, werden per Gesetz (nur für Schwerstkriminalität) Hintertüren eingebaut; eine Schwächung der Grundrechte für Alle!
Haben das alle Hersteller umgesetzt, wird man das auch für Kleinkriminalität nutzen wollen...

4) erste Lösungen:

-vertrauenswürdige HW: z.B. bestimmt kein Chromium-Tablet oder
Standard-Taschenspion etc. (Vortrag Januar: ...Augen auf vor Datenklau)

- vertrauenswürdige aktuelle, gepatchte SW, freies Betriebssystem
getrennte Benutzer-Rollen etc. (Vortrag März: alternative Linux)

- vertrauenswürdige E-Mail-Anbieter: sicher nicht Gmail und alle Anderen,
die Mails gratis nach Viren etc. "untersuchen" oder unsicheren Drittstaaten
verpflichtet sind. (Dismail-Server-Liste, Kuketz' Empfehlung)

- GMV! - Genau Meine Vorsicht:
- hinsehen auf Absender, Links, Anhänge "Zufälle" -> sofort + schmerzfrei löschen!
- keine Preisauschreiben, Kettenbriefe, Newsletter, wenig Mailinglisten
- wie im analogen Leben!
- Obacht: auch Phishing wird immer ausgefeilter
- notfalls beim Absender telefonisch nachfragen

- sichere Passphrasen für jeden Mail-Account extra, statt Einheits-"Scheunentor"
mit SMS-Kosten-Überraschung (Vortrag im Mai: sichere Passphrasen)

- E-Mail-Client als eigenes Abruf-Programm statt WEB-Surfbrett zwecks besserer
Handhabung, Funktions- u. Rollen-Trennung (Vortrag Juli: selbstsicher surfen)

5) Thunderbird

wird u.a. von Kuketz empfohlen, für Linux gibt es noch einige andere Mailclients

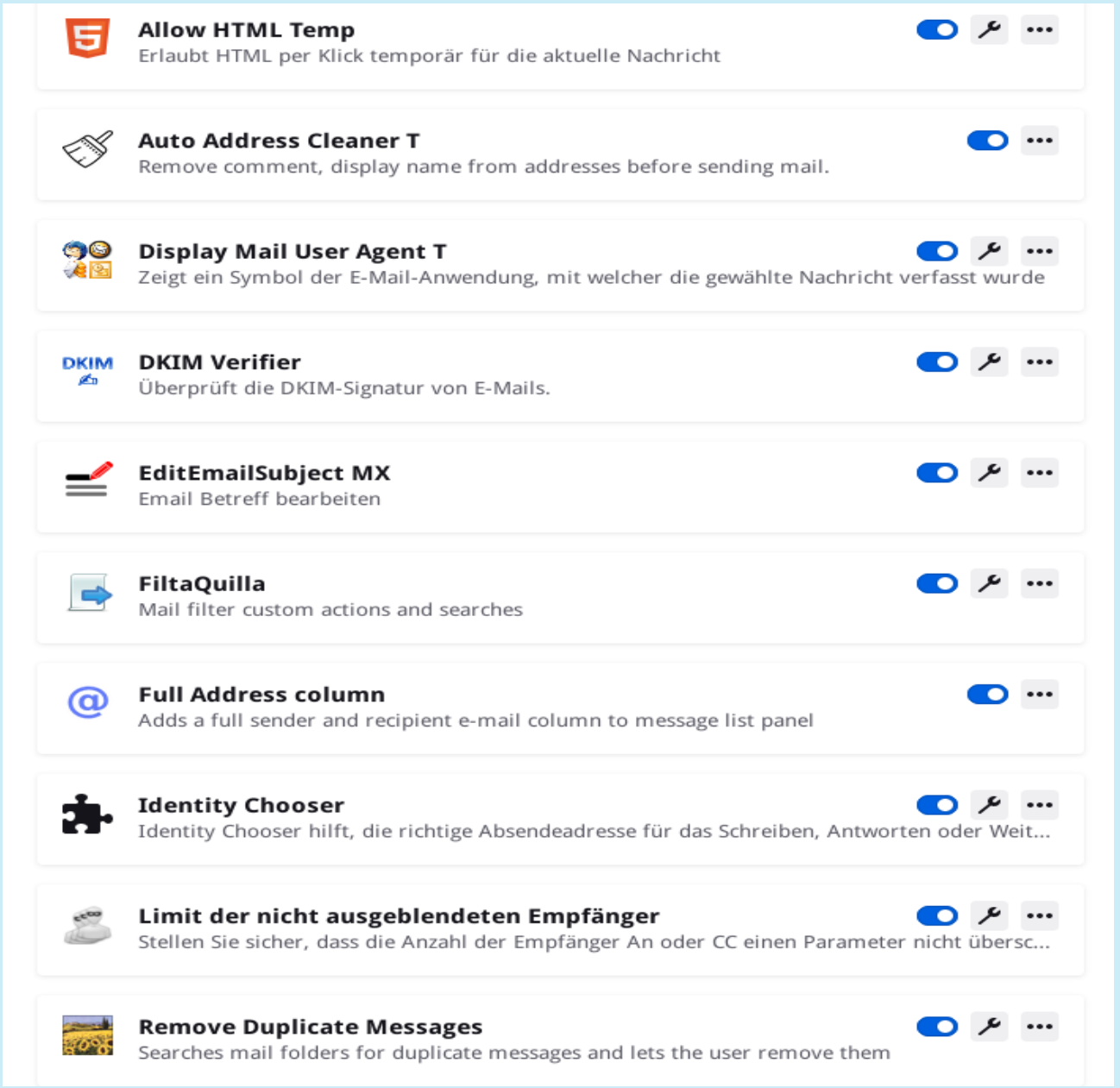
- Datenschutz-freundliche Einstellungen:
  Plaintext-Anzeige/Versand statt bunte HTML-Darstellung der Mail verhindert das ungefragte Tracking u. Nachladen von Programmen
    TB: Kontoeinstellungen - Verfassen & Adressieren

- Dateianhänge immer erst herunterladen, danach mit externem Programm PDF o. MS-Makro betrachten vermindert das Ausführen aktiver Inhalte.

- ggf. verschiedene Thunderbird-Profile für verschiedene Kommunikationskreise

- Thunderbird Add-On:
  ganze (Absender-) Mailadresse anzeigen lassen
  "Aufpasser" für maximale CC-"Verteiler"
  Allow HTML - kurzzeitge HTML-Ansicht erlauben
  immer Auswahl des Sende-Mail-Account
  Auto Adress Cleaner - enfernt vor dem Senden unnötige Infos
  DKIM-Verifier (Absender-Integritätscheck eingehender Mails)
  Enigmail ist überholt: die wichtigsten PGP-Funktionen sind bei TB eingebaut

5) Thunderbird Addons

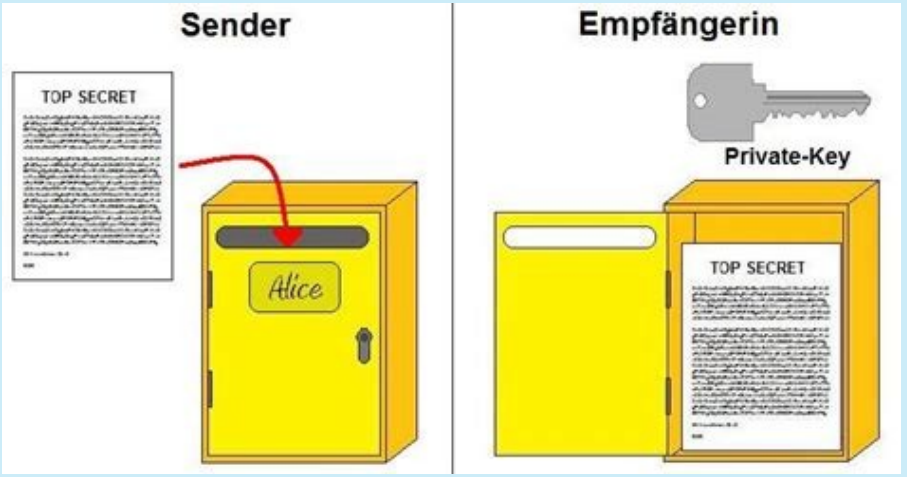


6) Pretty Good Privacy Grundlagen

- zwei mathematische Verfahren zum ver- und entschlüsseln

symmetrisch: ein Schlüssel für beide Vorgänge
Vorteil: schnell -> große Datenmengen: "Sitzungs-Schlüssel"
Nachteil: der gemeinsame Schlüssel muss geheim bleiben (Enigma)

asymmetrisch: ein "kurzer" öffentlicher Schlüssel nur zum Verschlüsseln
ein langer geheimer, privater Schlüssel zum lesbar machen
wie z.B. Postkasten, Schnappschloss
Vorteil: kein Geheimnis zum Verschlüsseln notwendig,
trotzdem kann Empfänger dechiffrieren
Nachteil: math. Einwegfunktion macht auch das Entschlüsseln aufwändiger
-> geheimer Transport eines Sitzungs-Schlüssels



6a) Pretty Good Privacy Grundlagen

1. Vorgang Vertraulichkeit herstellen

Infografik:
Alice hat Bob's öffentlichen Schlüssel und packt die Nachricht (via Sitzungsschlüssel) ein.

Nachricht ist verschlüsselt unterwegs.

!Nur der Empfänger Bob kann diese mit seinem geheimen, privaten Schlüssel öffnen und lesbar machen.

Bild: Redoxx-Infografik PGP
Lizenz: CC-BY-SA
https://www.reddoxx.com/produkte/mailsealer/infografik/

öffentlicher Schlüssel wäre als offenes Schnappschloss besser dargestellt
nur 1 öffentlicher Schlüssel muss getauscht werden!
dechiffrierter Brief sollte offen dargestellt sein

6b) Pretty Good Privacy Grundlagen

- nun ist die Mail unterwegs E2E verschlüsselt - Ist der Absender aber auch der Richtige?

2. Vorgang Authenzität prüfen

Wenn Alice ein Zeichen mitschickt, das nur sie gemacht hat,
ist das wie mit "Signatur" unterschrieben:

Jeder in aller Öffentlichkeit muss das ansehen und prüfen können.
Alice schickt zusätzlich eine Info (z.B. Nachrichten-Quersumme) mit,
die sie mit ihrem geheimen Schlüssel verschlüsselt.

Jeder kann mit Alice's öffentlichen Schlüssel die Info lesen.
Sind Nachrichten-Quersumme aus Nachricht und Signatur gleich,
ist Alice die Absenderin!

https://www.teletrust.de/projekte/abgeschlossene-projekte/elektronische-signatur/signierung/

6c) Pretty Good Privacy Grundlagen

- schwarzes Brett für öffentliche Schlüssel:
  - aktuell (ein) authorisierender Schlüsselserver: https://keys.openpgp.org/
  - WKS: öffentlicher Key ist beim Mailserver abrufbar
  - Zusätzlich muss man das Vertrauen herstellen,
    nämlich dass der öffentliche Schlüssel dem behaupteten Besitzer "gehört".
    -> die zugehörige Schlüssel-Kurzfassung (Fingerprint) ist auf sicherem Weg eigenhändig & augenscheinlich zu vergleichen
      - persönliches Treffen, Schriftstück/Visitenkarte, Website, QR-Code...
  - überholt: SKS-Keyserver, Web of Trust, Key-signing-Party

- PGP hält Metadaten (Absender, Empfänger, Betreff) nicht geheim!

- Stiftfilm aus 2014

7) PGP Einladung per Mail-Vorlage als How-To

8) Ausblick & Disclaimer

- die angegebenen Links / Unterlagen sind teilweise inzwischen überholt,
  bitte adaptieren.
- nichts ist 100% sicher, Lieferketten sind auch nicht mehr das was sie mal waren...
- immerhin: EFail wäre im oben beschriebenen Setup nicht weit gekommen.

- TB: verschlüsselte Mails lassen sich schwer durchsuchen,
  Workaround: in lokalen Ordner entschlüsselt archivieren
- die HW hat zunehmend mehr zu schaffen...

- andere Lösungswege, ggf. im KMU Sektor:
  Delta-Chat,
  Matrix/Element als Messenger,
  Proton-, DE-mail etc.
  Trutzbox vs. Metadaten
  CACert.org Vertrauen durch Zertifikate

Vielen Dank für die Aufmerksamkeit!

Wenn Ihnen der Vortrag gefallen hat: Ihre Spenden sollen an dismail und Thunderbird-Team gehen

VDI-Konto: DE37 6805 0101 0013 3541 45
Stichwort: Spende AK-DigIT-FLUG E-Mail

ak-digit@bv-schwarzwald.vdi.de

PGP-Key: https://keys.openpgp.org/search?q=ak-digit%40bv-schwarzwald.vdi.de

Fingerprint: 1952 732E 9F00 F41E 8C56 9543 B857 646A 8FC0 1031

Verein deutscher Ingenieure Bezirk Schwarzwald www.vdi-schwarzwald.de
Linux User Group Freiburg www.lug-freiburg.de

Copyrights, Lizenzen

Quellenangaben

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/E-Mail-Sicherheit/e-mail-sicherheit_node.html

https://kowabit.de/angriff-per-e-mail/

https://www.heise.de/news/Datenschutzbeauftragter-Gaengiges-Faxen-nicht-mit-der-DSGVO-vereinbar-6194254.html

https://www.kuketz-blog.de/empfehlungsecke/#email

https://lug-freiburg.de/pages/projekte.html
https://www.heise.de/security/dienste/Emailcheck-2109.html

https://www.hauke-laging.de/sicherheit/
https://www.vdi-nachrichten.com/technik/informationstechnik/e-mail-tracking-aufspueren-und-abstellen/

https://dismail.de/serverlist.html
https://www.sueddeutsche.de/digital/phishing-passwoerter-von-telekom-kunden-im-netz-entdeckt-1.3053819

Quellenangaben

https://www.thunderbird-mail.de/article-list/
https://www.thunderbird-mail.de/lexicon/entry/179-add-ons-liste-h%C3%A4ufig-genutzter-erweiterungen/
https://www.thunderbird-mail.de/forum/board/36-hilfe-zu-e-mail-und-allgemeines-arbeiten/
https://support.mozilla.org/en-US/kb/keyboard-shortcuts
https://blog.sys4.de/pgp-e-mails-dauerhaft-unverschlusselt-speichern-mit-thunderbird-de.html
https://thunderbird.topicbox.com/groups/e2ee
https://unsicherheitsblog.de/thunderbird-regel-kopfzeile-filtern-3993
https://www.mailhilfe.de/beitrag-thunderbird-regeln-exportieren-1192-html

https://addons.thunderbird.net/de/thunderbird/addon/limit-non-bcc-recipients/?src=search
https://addons.thunderbird.net/de/thunderbird/addon/lookout-fix-version/?src=search
https://addons.thunderbird.net/de/thunderbird/addon/quickfilters/
https://addons.thunderbird.net/en-US/thunderbird/addon/allow-html-temp/?src=search
https://addons.thunderbird.net/en-US/thunderbird/addon/auto-address-cleaner-t/?src=search
https://addons.thunderbird.net/en-US/thunderbird/addon/dkim-verifier/?src=ss
https://addons.thunderbird.net/en-US/thunderbird/addon/edit-email-subject/?src=ss
https://addons.thunderbird.net/en-US/thunderbird/addon/filtaquilla/?src=ss
https://addons.thunderbird.net/en-US/thunderbird/addon/full-address-column/?src=ss
https://addons.thunderbird.net/en-US/thunderbird/addon/identity-chooser/?src=ss
https://addons.thunderbird.net/en-US/thunderbird/addon/removedupes/?src=ss
https://addons.thunderbird.net/en-US/thunderbird/addon/threadvis/?src=ss

Quellenangaben

https://wikiless.org/wiki/Pretty_Good_Privacy?lang=de
https://wikiless.org/wiki/Asymmetrisches_Kryptosystem?lang=de
https://keys.openpgp.org/
https://metager.org/meta/meta.ger3?eingabe=Asym+verschluesselung.jpg&submit-query=&focus=bilder&s=&d=&c=&l=&t=&a=&co=&f=&m=
https://rmg.zum.de/wiki/Benutzer:Deininger_Matthias/Facharbeit/Asymmetrische_Kryptographie
https://wiki.zum.de/wiki/ZUM-Wiki:Lizenzbestimmungen
https://www.reddoxx.com/produkte/mailsealer/infografik/
https://digitalcourage.video/w/wVfxRz93q5eVVPg6VaXbXD
https://www.heise.de/security/dienste/Krypto-Kampagne-2111.html
https://www.openpgp-schulungen.de/fuer/bekannte/
https://www.openpgp-schulungen.de/#sachkenntnis
https://www.openpgp-schulungen.de/kurzinfo/
https://wiki.piratenpartei.de/PGP
https://digitalcourage.de/2018/05/21/e-mail-verschluesselung-und-sicherheitsnihilismus
https://userbase.kde.org/Concepts/OpenPGP_For_Beginners/de
https://wiki.ubuntuusers.de/GnuPG/#E-Mail-Verschluesselung-testen
https://support.mozilla.org/en-US/kb/openpgp-thunderbird-howto-and-faq#w_i-have-previously-used-enigmail-how-do-i-migrate-and-configure
https://help.gnome.org/users/seahorse/stable/index.html.de#pgp-keys
https://www.heise.de/ct/artikel/Einfach-erklaert-E-Mail-Verschluesselung-mit-PGP-4006652.html
https://www.msxfaq.de/signcrypt/ende_zu_ende_mailverschluesselung.htm
https://netzpolitik.org/2013/anleitung-so-verschlusselt-ihr-eure-e-mails-mit-pgp/

Quellenangaben

http://www.openpgp-schulungen.de/fuer/bekannte/
https://digitalcourage.de/digitale-selbstverteidigung/vertrauenswuerdige-e-mail-anbieter
https://www.gpg4win.de/doc/de/gpg4win-compendium_7.html
https://digitalcourage.video/w/wVfxRz93q5eVVPg6VaXbXD
https://www.kuketz-blog.de/verschluesselte-e-mails-mit-gnupg-als-supergrundrecht/
https://emailselfdefense.fsf.org/en/infographic.html
https://keys.openpgp.org/about
https://www.privacy-handbuch.de/handbuch_32j.htm
https://social.tchncs.de/interact/106781943780488878?type=favourite
https://www.teletrust.de/projekte/abgeschlossene-projekte/elektronische-signatur/signierung/

Quellenangaben

https://www.heise.de/security/meldung/S-MIME-und-PGP-E-Mail-Signaturpruefung-laesst-sich-austricksen-4411230.html
https://www.heise.de/newsticker/meldung/Posteo-unterstuetzt-PGP-Helfer-Autocrypt-3922498.ht
https://www.sueddeutsche.de/digital/verschluesselungssoftware-gnu-pg-wie-ein-mann-das-e-mai geheimnis-verteidigt-1.2355155-2#
https://www.thunderbird-mail.de/forum/thread/86957-verchl%C3%BCsselung-wenn-key-f%C3%B empf%C3%A4nger-vorhanden/
https://www.golem.de/news/verschuesselung-let-s-encrypt-verraet-7-618-e-mail-adressen-1606-121462.html
https://www.thunderbird-mail.de/forum/thread/85270-migrationshinweise-zu-funktionen-einschr %C3%A4nkungen-bei-openpgp-in-tb-78-2-2/
https://www.thunderbird-mail.de/forum/thread/87282-dauerhaftes-entschl%C3%BCsseln/
https://www.heise.de/forum/heise-online/Kommentare/Sicherheitsupdate-Thunderbird-78-4-gegen Abstuerze-und-Schadcode-geruestet/Re-Bitte-um-Rueckmeldungen-Erfahrungsberichte-zu-upda 68-12-mit-Enigmail/posting-37652615/show/
https://delta.chat/en/
https://doc.matrix.tu-dresden.de/
https://wir.freiburg.social/
https://matrix.org/
https://trutzbox.de/
http://www.nwlab.net/tutorials/dynamail.html
https://openpgpkey.info/
https://www.cacert.org/index.php?id=0&lang=de
https://wiki.cacert.org/ThunderBird