# T.I.S.P. Community Meeting 2023

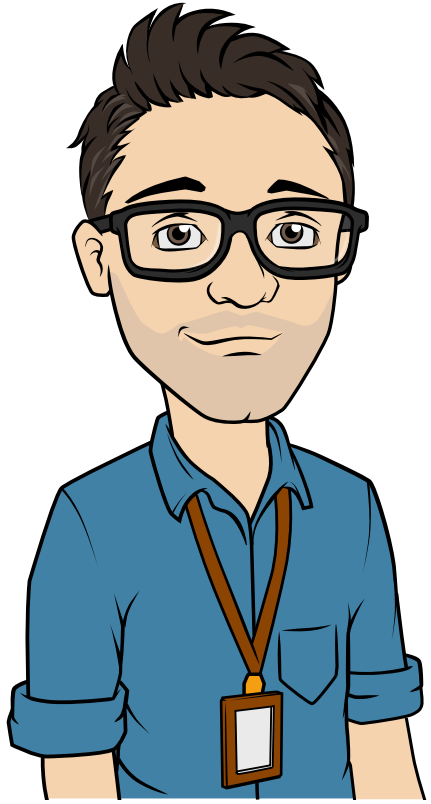
**Berlin, 07. - 08.11.2023**

# Automatisierte Sanitarisierung von Dokumenten

Florian Rienhardt

# Florian Rienhardt

- Diplom Informatiker (Uni Bonn)
- IT-Sec Professional (seit 2006)
- Software-Entwickler, Referent, Gründer



Quelle: f.rienhardt

# „Aktueller“ Stand – Ein ungleicher Kampf

- BSI Lagebericht 2023
- BSI Cyber-Sicherheitslage
- BKA-Bericht

# Aber wir sind doch gut geschützt?!

Quelle: midjourney/f.rienhardt

# Schutztechnologien

- Übliche Schutztechnologien
  - Perimeter: Firewalls, IDS, Web-Proxies, Spamfilter
  - Client: AV-Scanner, Applikationskontrolle, Schnittstellenkontrolle
  - funktionierendes Backup (!)
  - sensibilisierte Mitarbeiterinnen und Mitarbeiter / Security-Team

# Wer schützt sich wie

- „Big-Scale“
  - Security Gateways / Proxies
  - IDS, AVs, DLP, ReCoBS, …
  - Content Sandboxing
  - Incident Response Team
  - Künstliche Intelligenz 😂 🤯
- „Small-Scale“
  - AV-Scanner
  - Ad hoc Analyse
  - Admin = Incident Response
  - „hoffen, dass es gut geht“

# … und dann kommt das!





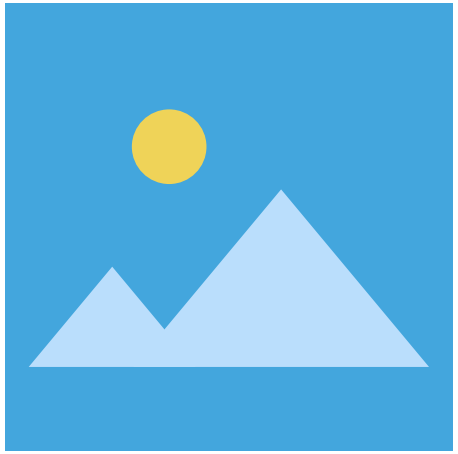
Quelle: midjourney/f.rienhardt

# Infektionswege

- Wie kommt Schadcode auf die Rechner / Server
  - Phishing-Mails mit Links, Anhängen, kompromittierte Webseiten
  - Sicherheitslücken in Dokumentenformaten
  - „Social Engineering“
  - … die Mitarbeitenden

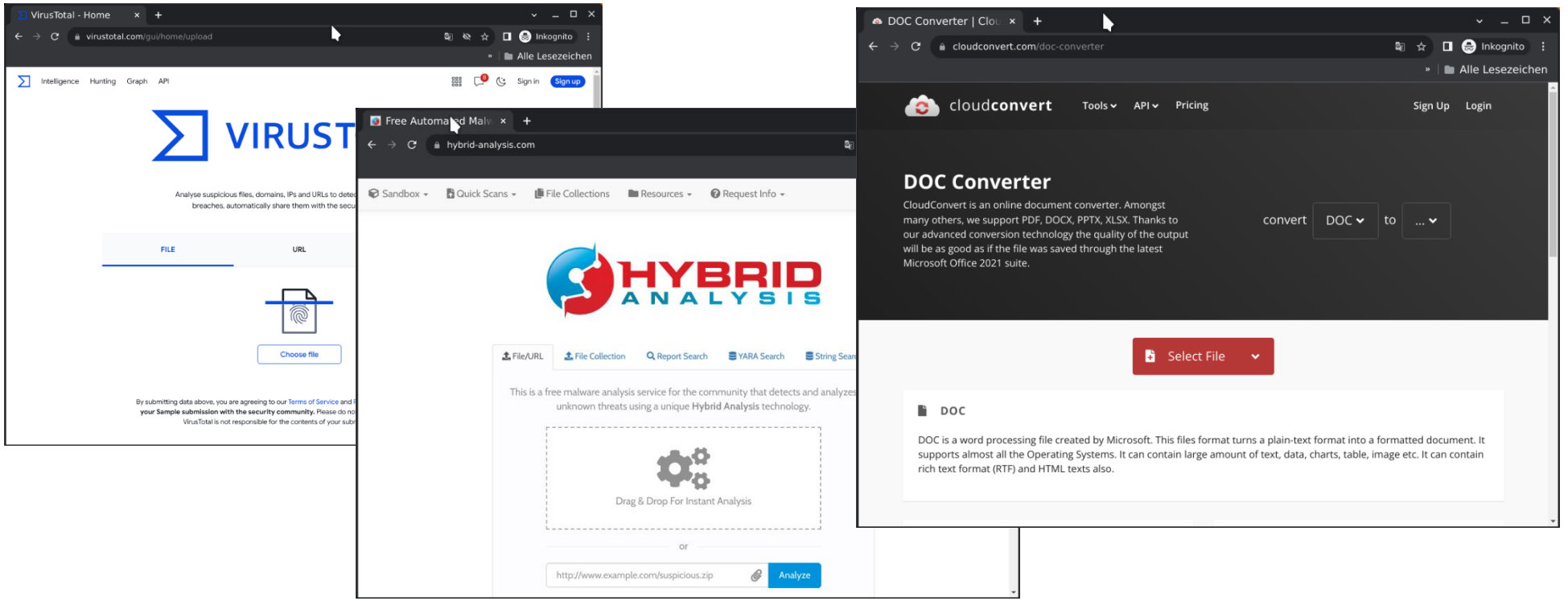
# Säubern von Dokumenten (sanitizing)

- Statt auf Schadcode analysieren → säubern
  - Analyse?
  - sicheres Format?
  - Umwandeln!



Quelle: f.rienhardt

# Gibt es da nicht etwas von … ?



# Nein! Nicht in die Cloud laden!!!

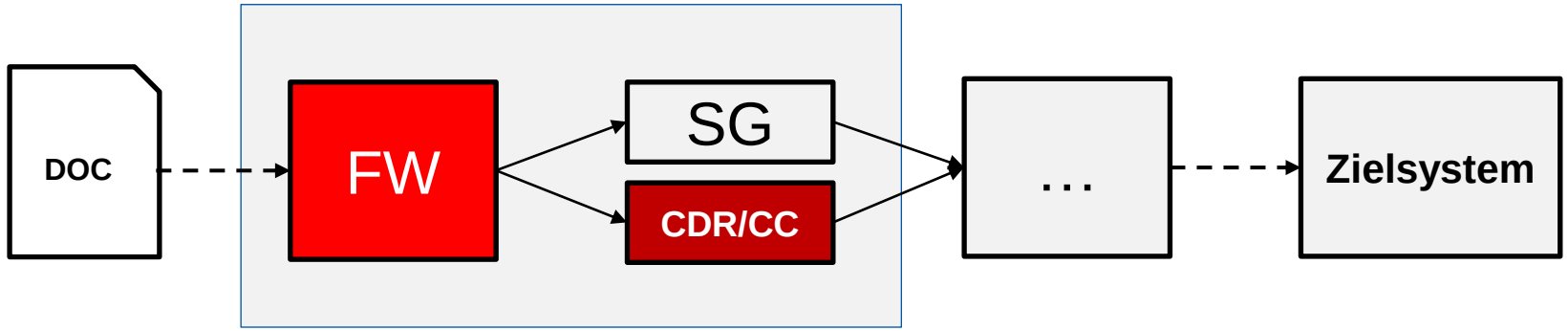
Quelle: midjourney/f.rienhardt

# … und auch nicht an das Security Team schicken

Quelle: midjourney/f.rienhardt

# Sanitarisierung von Dokumenten

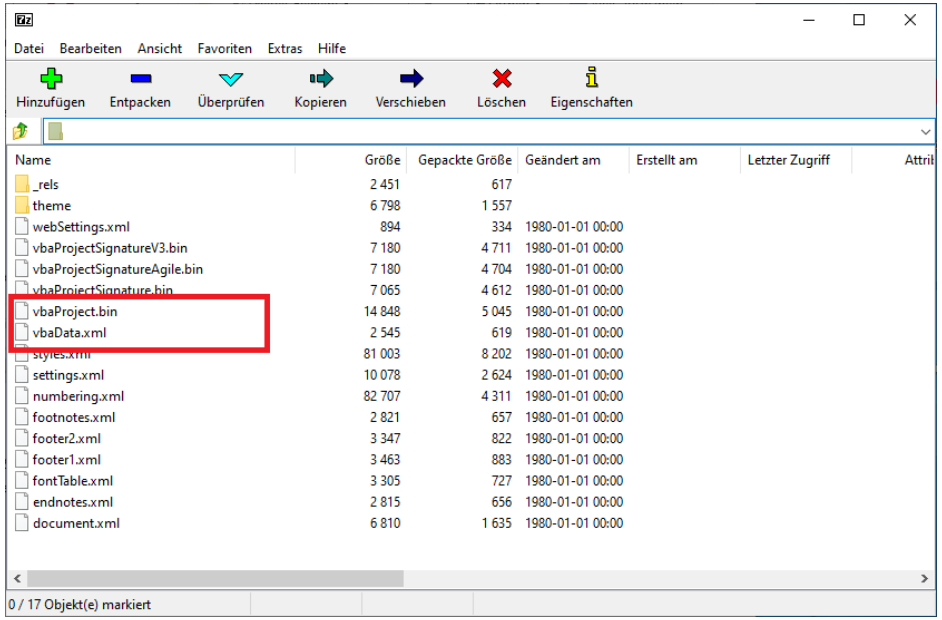
- Abseits des AVs zwei mögliche Lösungsansätze
  - Content Disarm and Reconstruction (CDR)
  - Content Conversion (CC)



# Content Disarm and Reconstruction



- Kritische Inhalte entfernen
  - filtert aktive/schädliche Inhalte
  - filtert sensible Inhalte („DLP“)




- Bewahrt ursprüngliches Format
  - Dokumente mit Standardanwendung weiterhin öffnen
  - wenig Einschränkung für Anwendende

# Content Conversion

- Umwandeln in ein sicheres Format
  - Bildformate oder PDF
  - keine aktiven (schädlichen) Inhalte
- Eine Standardanwendung für unterschiedliche Formate

# Content Conversion



- Konvertierung in Bild/PDF mittels OSS „recht einfach“

```
$> convert -density 300 -background white -strip „input.pdf" -quality 30 converted.JPG
$> mogrify -format pdf -- *.JPG
$> pdfunite converted*.pdf final-sample.pdf
$> ocrmypdf -l deu+eng --output-type pdf final-sample.pdf final-ocr-sample.pdf
```

# Content Disarm & Reconstruction, Content Conversion

- System ist nach Konvertierung potentiell infiziert

Quelle: midjourney/f.rienhardt

Quelle: midjourney/f.rienhardt

# Gruß aus der Sandbox-Hölle

Quelle: midjourney/f.rienhardt

# Content Disarm & Reconstruction, Content Conversion



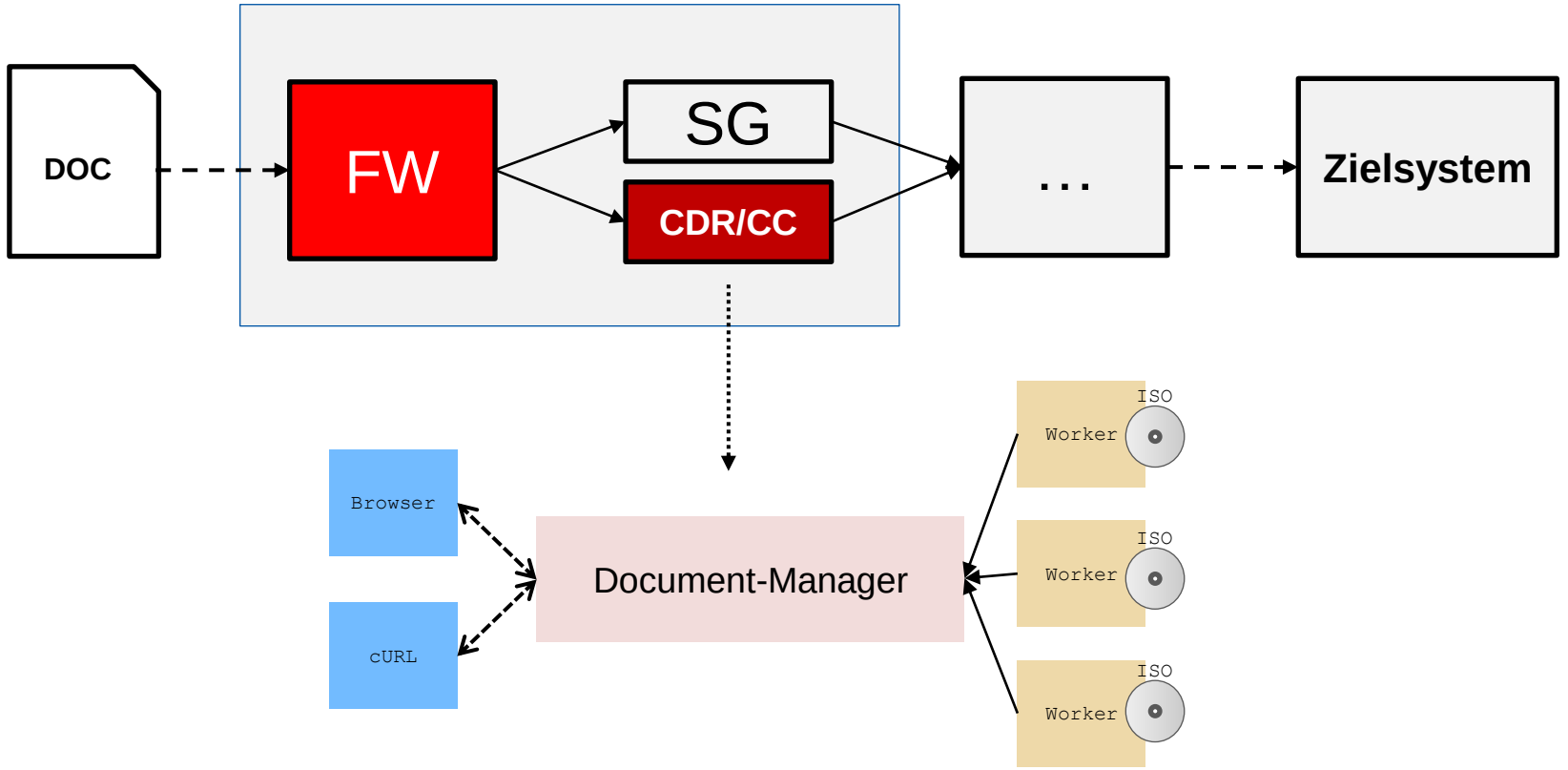
- System ist nach Konvertierung potentiell infiziert
- Und **nein!!11ELF!!!!** Docker ist keine Lösung
  - … denn Docker ist keine Security-Sandbox. PUNKT.

# … und hier kann GNU/Linux ins Spiel kommen

Quelle: midjourney/f.rienhardt

# Linux-Live-Systeme als mögliche Lösung

- Säuberung als Web-Dienst (REST-API)



# Linux-Live-Systeme als mögliche Lösung



- System zur Säuberung als Live-Image (ISO)
- lässt sich bare-metal oder virtualisiert realisieren
- nach Säuberung kommt der Reboot
- Funktioniert das? – das funktioniert!

# Vielen Dank!

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

## Fragen?

Quelle: midjourney/f.rienhardt

florian@rienhardt.it / github.com/hazelfazel