Digitale Selbstverteidigung

Best Practices aus dem Journalismus, die auch für Jurist:innen nützlich sein können

Daniel Moßbrucker – Journalist und Trainer für Digitale Sicherheit

5 Fragen aus dem Redaktionsalltag

- Wie können Quellen die Redaktion am sichersten kontaktieren?
- Wie kommuniziere ich am sichersten mit Quellen und Kolleg:innen?
- Wie sichere ich meine Recherchen?
- Wie arbeite ich sicher, aber gemeinschaftlich an sensiblen Texten?
- Was muss ich bei Recherche-Reisen ins Ausland beachten?

5 Fragen aus dem Rechtsalltag

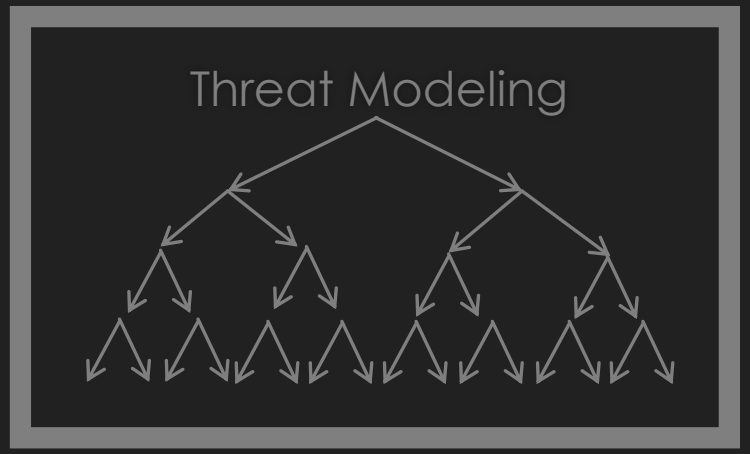
- Wie können Mandant:innen, Zeugen die Kanzlei, Behörde am sichersten kontaktieren?
- Wie kommuniziere ich am sichersten mit Mandant:innen, Zeugen und Kolleg:innen?
- Wie sichere ich meine Daten und Archive?
- Wie arbeite ich sicher, aber gemeinschaftlich an sensiblen Schriftsätzen?
- Was muss ich bei Dienstreisen ins Ausland beachten?

Threat Modeling

Denken in konkreten Bedrohnungsszenarien, statt in absoluter Sicherheit

Bedrohungssenzario

Wer bin ich?



1. Was möchte ich schützen?
2. Wer ist mein Gegner?
3. Was kann mein Gegner?
4. Wie wahrscheinlich ist es, dass mein Gegner mich angreift?

Bedrohungsseznario → Individuelles Sicherheitskonzept

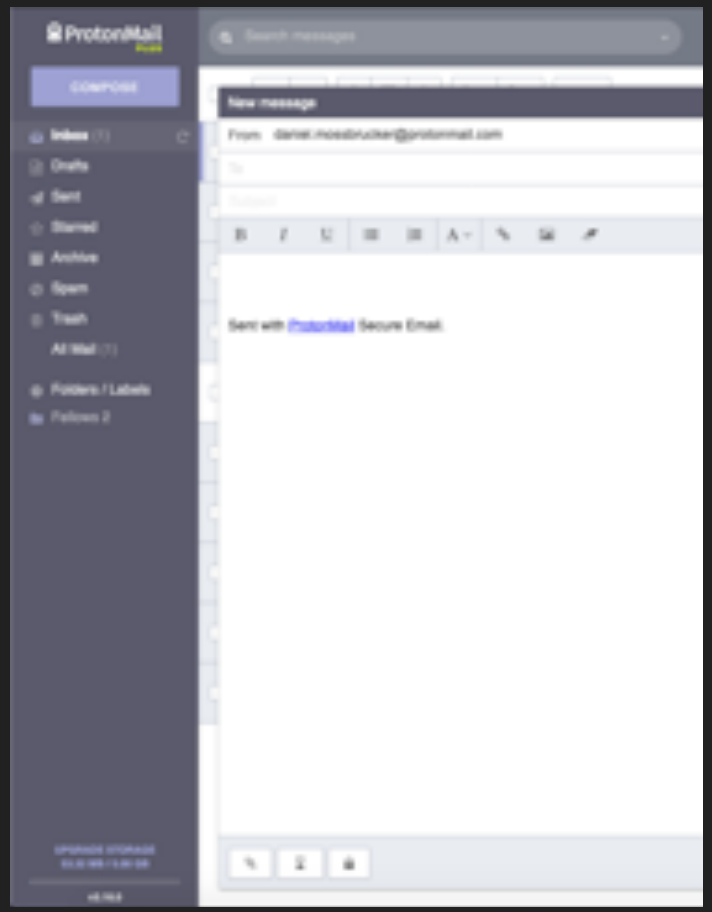
Sichere Kontaktaufnahme

So viele Kanäle öffnen wie möglich

Sichere Kontaktaufnahme

- Ansatz
  - möglichst viele Kanäle anbieten und offen halten
- Umsetzung
  - PGP-Schlüssel für Email-Verschlüsselung auf Website hochladen (Vorsicht: Metadaten!)
  - Protonmail-Account einrichten und Kontaktpersonen bitten, über Protonmail zu kommunizieren
  - Messenger-Nicknames und Nummern auf die Website stellen (z.B. Telegram Me, Wire, Threema)
  - anonymer Briefkasten über Darknet-Technologie (z.B. Secure Drop, Onion Share)
- Unterstützung
  - Zu allen Kanälen ein kurzer Erklärtext, wie es geht – und was es nicht schützt

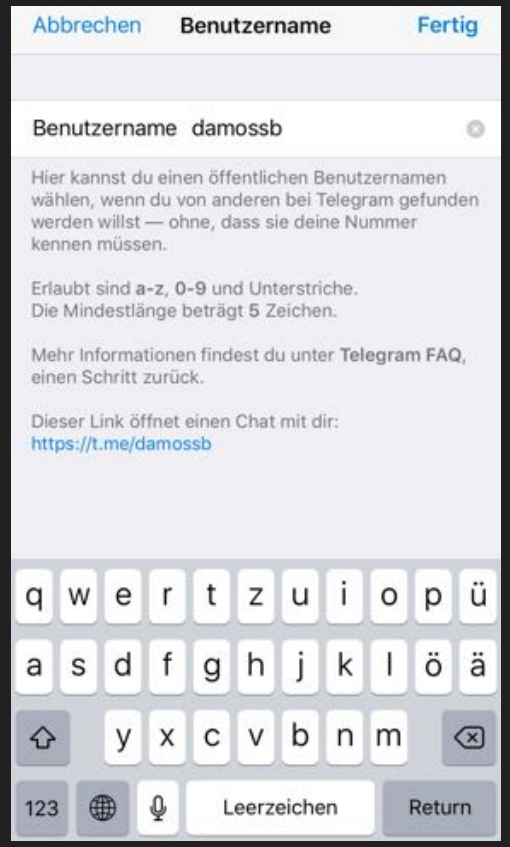
Sichere Kontaktaufnahme: Email

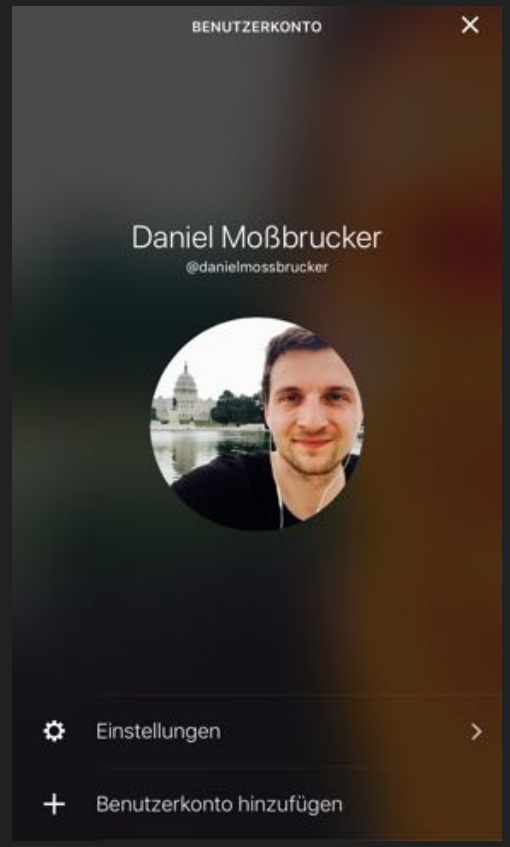


Email: mail@daniel-moosbrucker.de
PGP-ID: 9Ca8D004
PGP-Fingerprint: C440 5F09 7084 EA04 5394 E184 79AA 16D4 9Ca8 D004
Threema-ID: 8JVDFPND
Jabber-ID (XMPP): daniel.moosbrucker@jabber.de
Xing: xing.com/profile/daniel_moosbrucker
Twitter: @damoosb

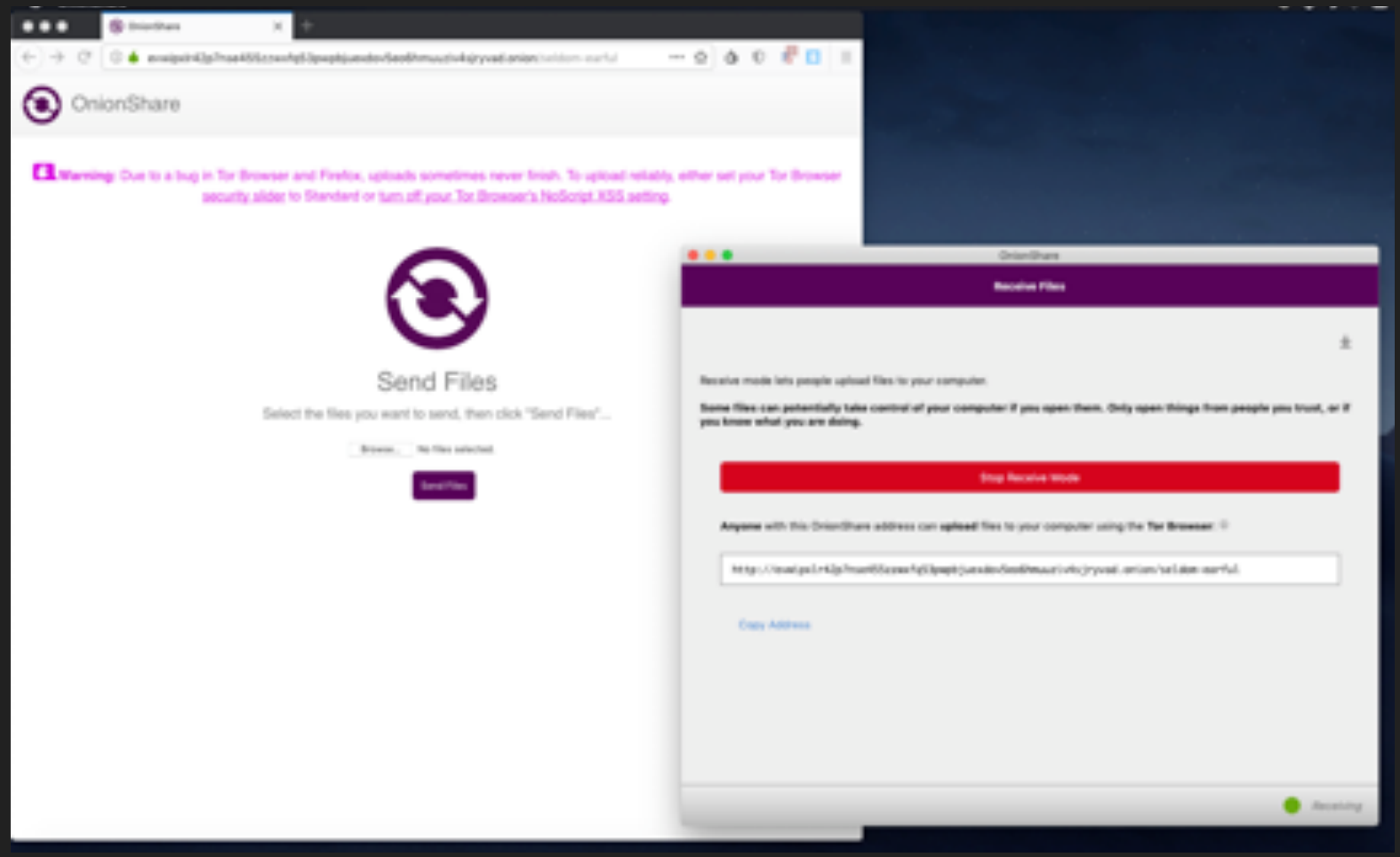
erreichbar über Signal, Telegram, Threema und Whatsapp

Sichere Kontaktaufnahme: Messenger





Sichere Kontaktaufnahme: anonymes Postfach



Sichere Kommunikation

Menschen dort abholen, wo sie sind

Sichere Kommunikation

- Ansatz
  - Menschen dort abholen, wo sie sind
  - so rasch wie möglich auf die sicherste Variante wechseln
- Umsetzung
  - Messenger sind häufig Ende-zu-Ende verschlüsselt, ihre Metadaten sind für staatliche Angreifer schwierig zu erlangen – und ihr Gebrauch ist für Kontaktpersonen sehr einfach

Sichere Kommunikation

1	2	3	4	5
Signal	Telegram	Threema	WhatsApp	Messenger
Ende-zu-Ende verschlüsselt	Ende-zu-Ende verschlüsselt	Ende-zu-Ende verschlüsselt	Ende-zu-Ende verschlüsselt	Ende-zu-Ende verschlüsselt
	!			!
Open Source	Open Source			
			M	M
			Im Besitz von Facebook	Im Besitz von Facebook

- Ende-zu-Ende verschlüsselt
- ! E2EE muss aktiviert werden
- Open Source
- M Metadaten-Speicherung
- Im Besitz von Facebook

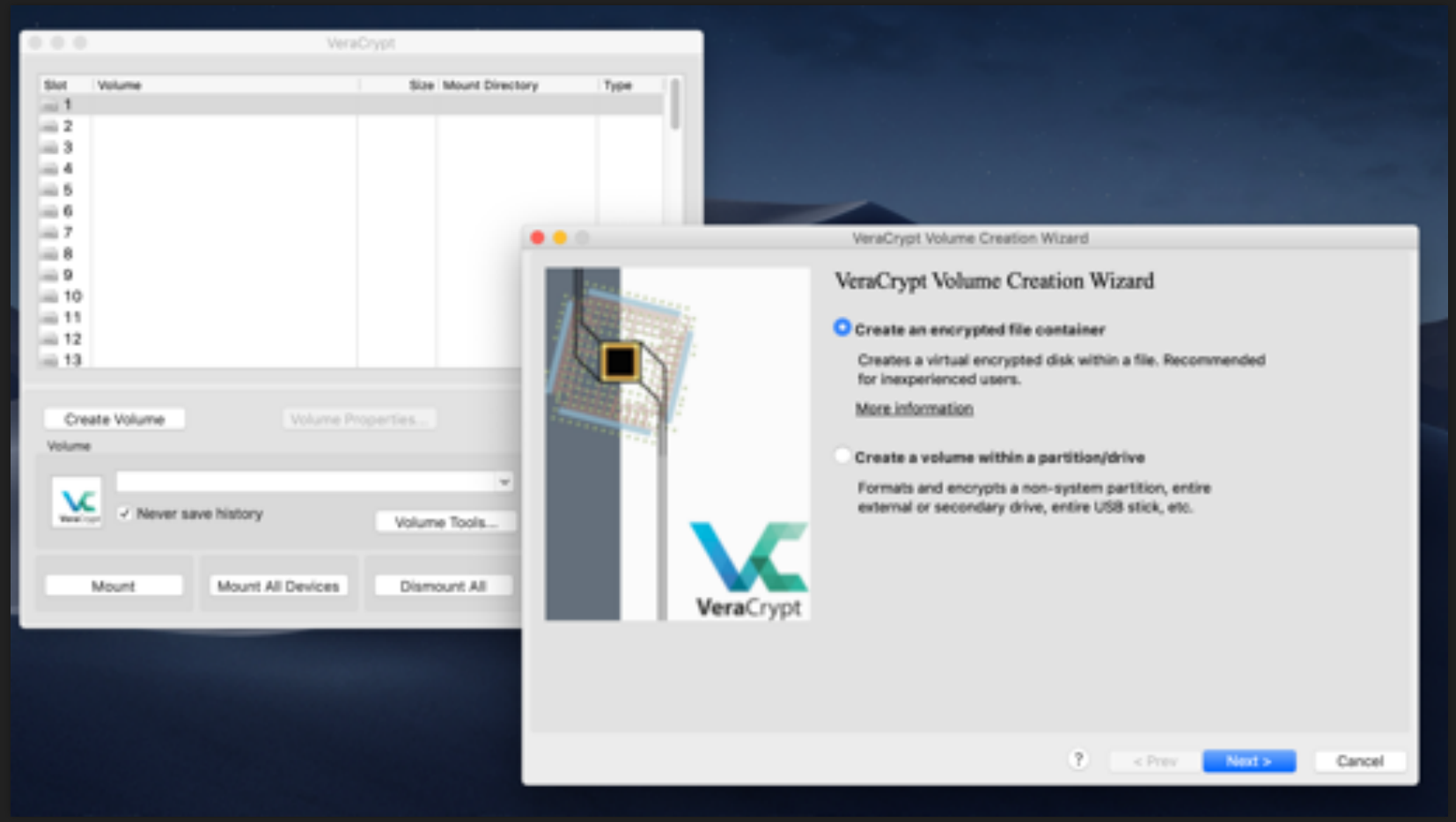
Datensicherung

Starke Verschlüsselung, egal wo

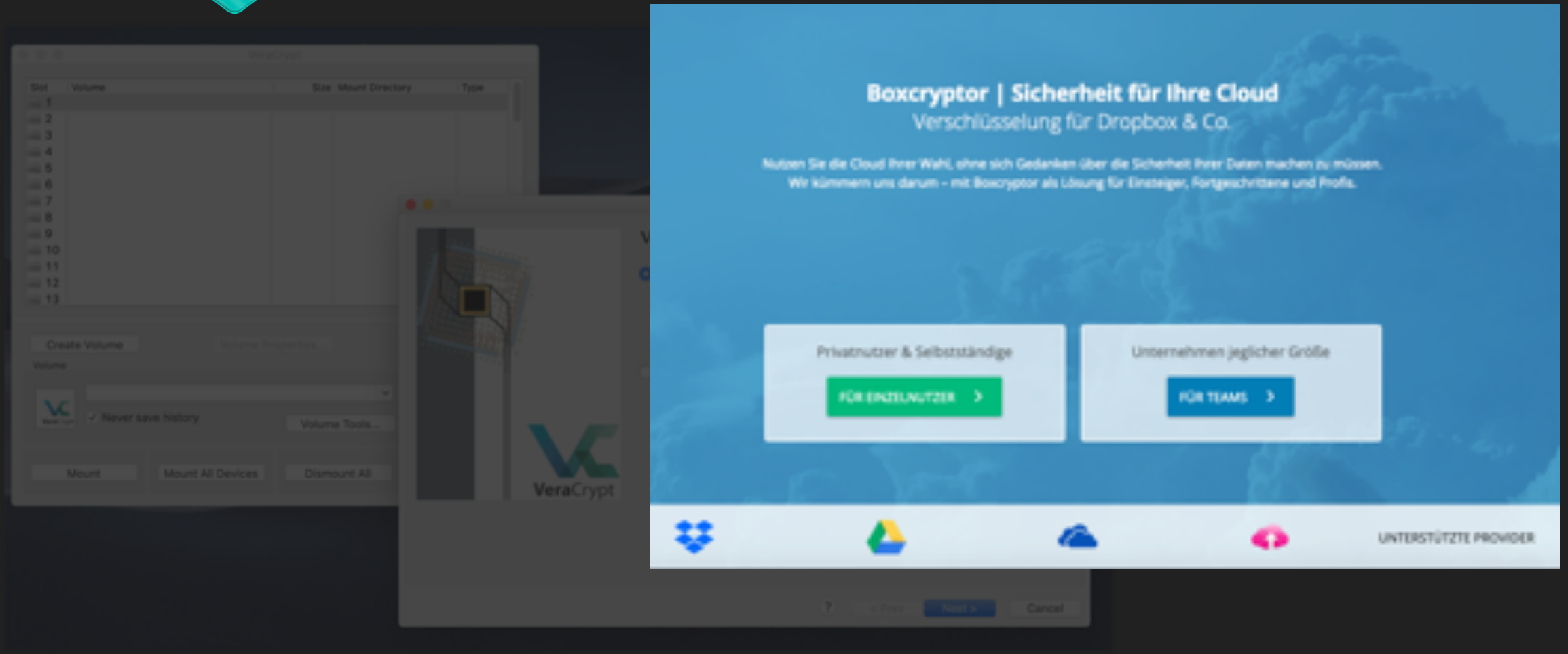
Datensicherung

- Ansatz
  - Daten verschlüsseln, egal ob auf dem PC oder in der Cloud
- Umsetzung
  - VeraCrypt für Verschlüsselung großer Datenmenger oder ganzer Festplatten
  - Boxcryptor für Verschlüsselung beim Upload in die Cloud

Datensicherung



Datensicherung



Kollaboratives Arbeiten

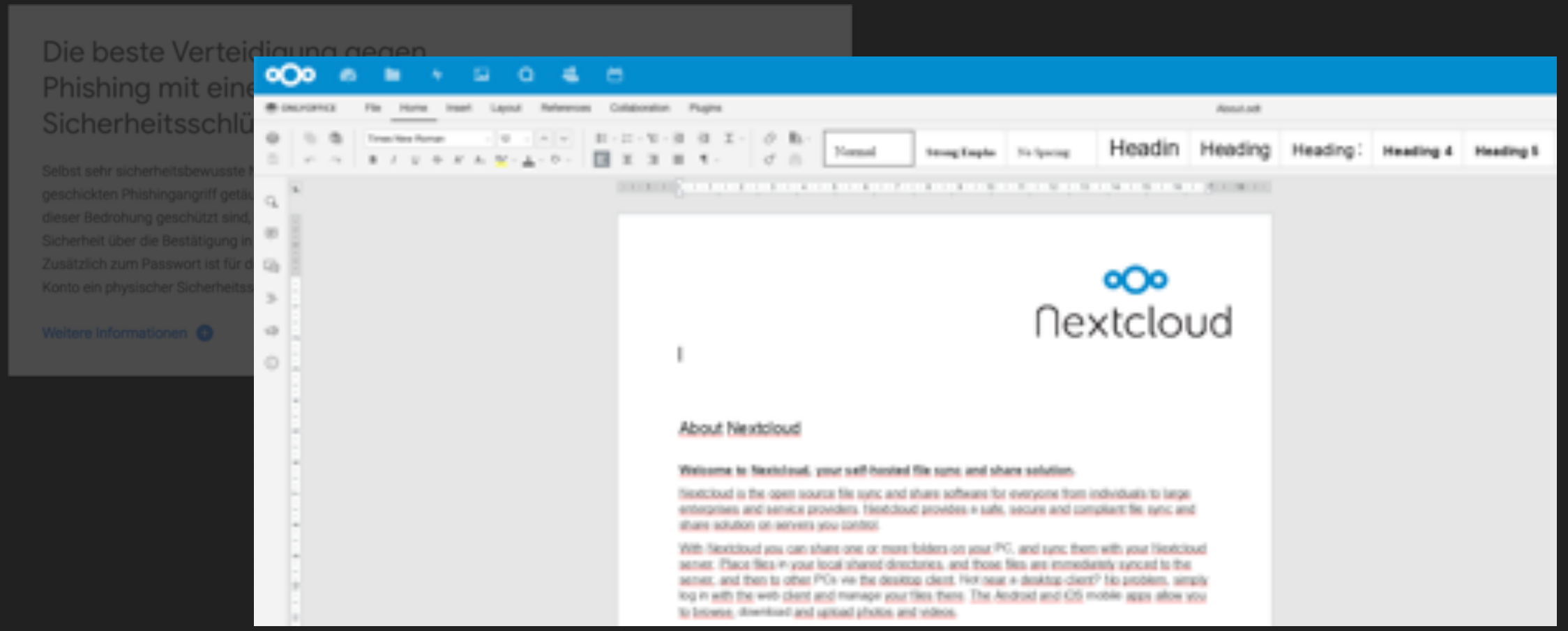
Starker Account-Schutz bei Drittanbietern – oder eine eigene Cloud

Kollaboratives Arbeiten

- Ansatz
  - Accounts der Kollaborateure gegen Hacking schützen und/oder eine eigene Cloud
- Umsetzung
  - Google Docs etc. mit restriktiver Nutzer:innen-Verwaltung und verpflichtender Zwei-Faktor-Authentifizierung
  - Aufsetzen einer eigenen Cloud, z.B. Nextcloud

Kollaboratives Arbeiten

Kollaboratives Arbeiten



Reisesicherheit

„Unschuldig“ an der Grenze

Reisesicherheit

- Ansatz
  - Beim Grenzübertritt keinerlei Möglichkeiten geben, an die eigenen Daten zu gelangen – weil sie gar nicht da sind
- Umsetzung
  - Log-Out bei allen Accounts, bestenfalls Löschen der Apps auf dem Smartphone
  - Dokumente verschlüsselt in die (eigene Cloud), und nach dem Grenzübertritt herunterladen

Daniel Moßbrucker I Trainer für Digitale Sicherheit

mail@daniel-mossbrucker.de (PGP: 9C4ED204)