

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 Schriftsätze?
- Was muss ich bei Dienstreisen ins Ausland beachten?

Threat Modeling

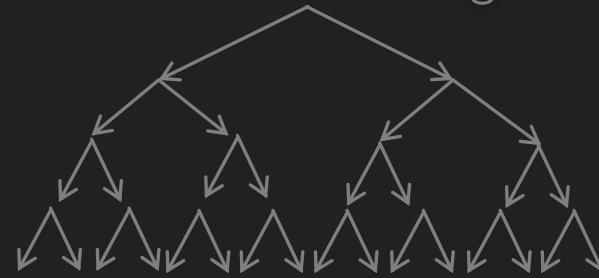
Denken in konkreten Bedrohungsszenarien, statt in absoluter Sicherheit

Bedrohungsszenario

Wer bin ich?



Threat Modeling



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?



Bedrohungsszenario



Individuelles Sicherheitskonzept

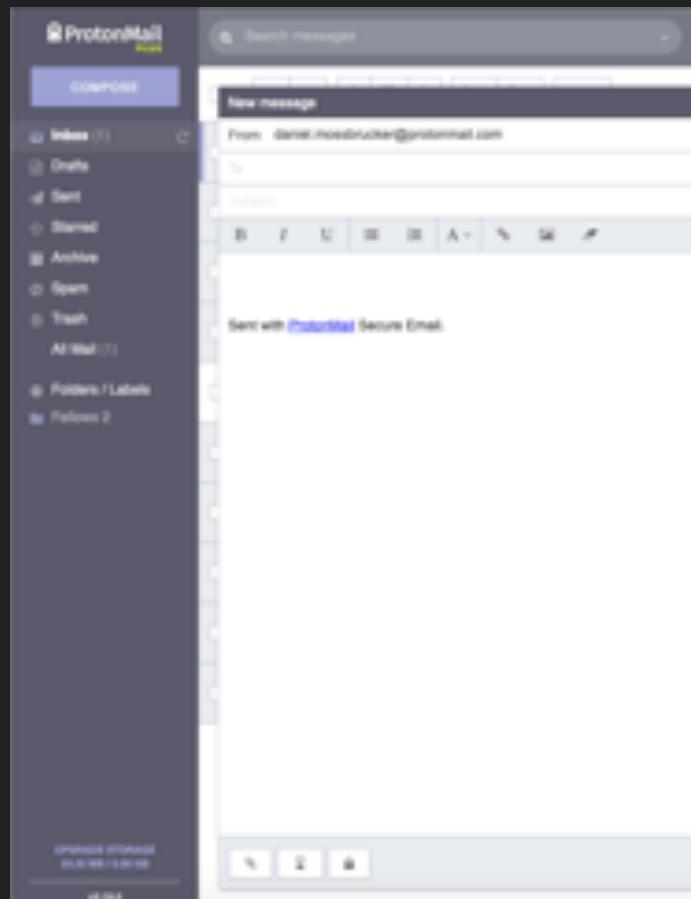
Sichere Kontaktaufnahme

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

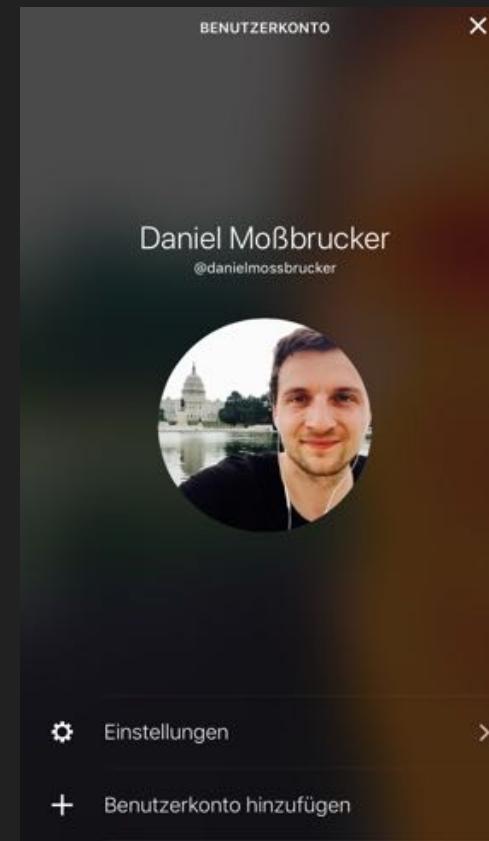
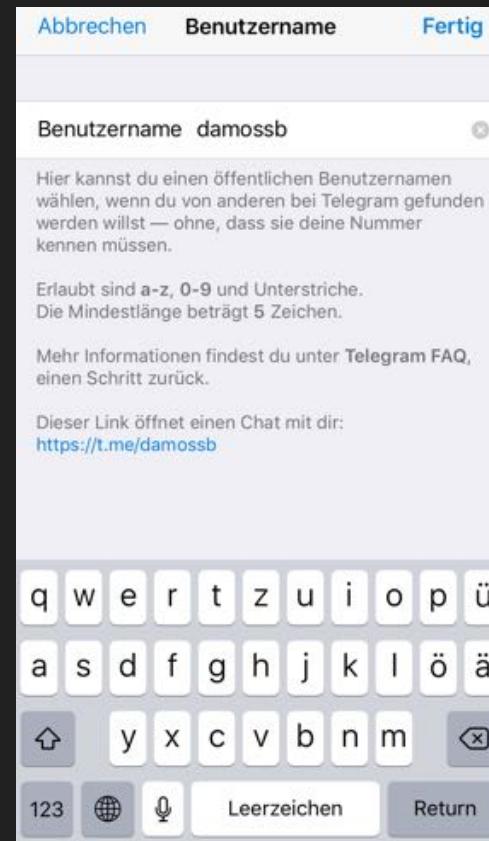
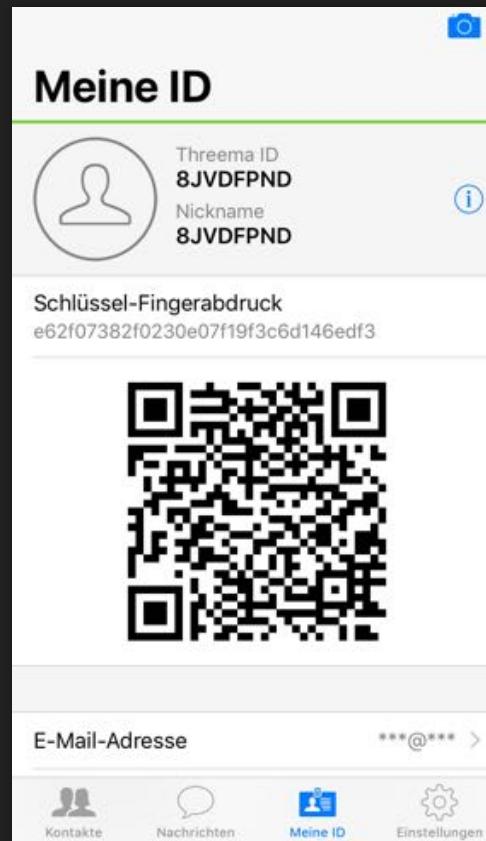
Sichere Kontaktaufnahme: Email



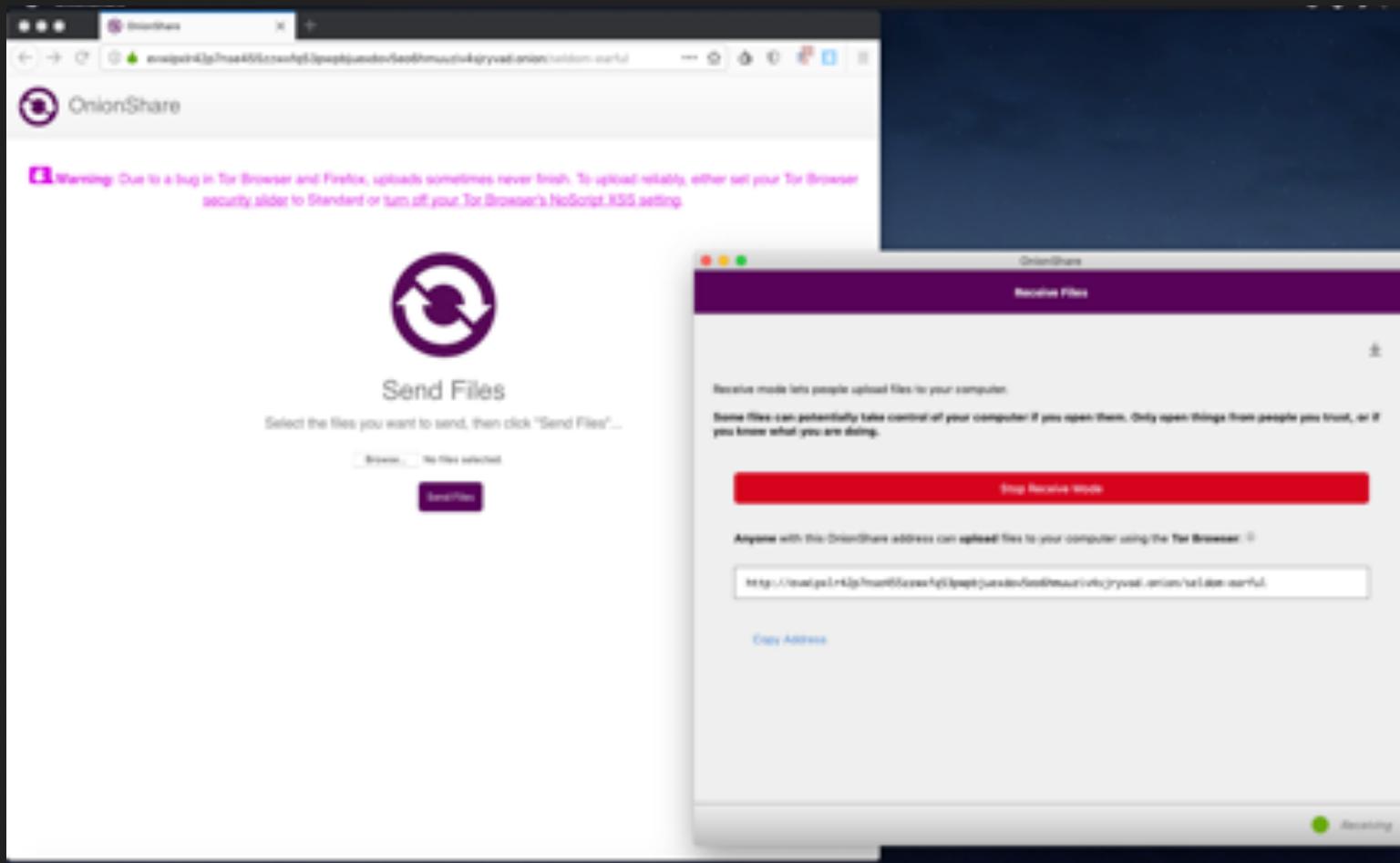
Email: mail@daniel-mosbrucker.de
PGP-ID: 9C49D2004
PGP-Fingerprint: CA49 5F99 70B4 E4M4 D394 E3E4 79AA 9D4 9C49 D2004
Threema-ID: 8JVDFFND
Jabber-ID (XMPP): daniel.mosbrucker@jabber.de
Xing: xing.com/profile/daniel_mosbrucker
Twitter: @damosob

erreichbar über Signal, Telegram, Threema und WhatsApp

Sichere Kontaktaufnahme: Messenger



Sichere Kontaktaufnahme: anonymes Postfach



Sichere Kommunikation

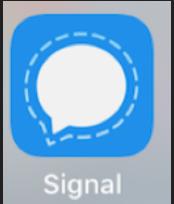
Menschen dort abholen, wo sie sind

Sichere Kommunikation

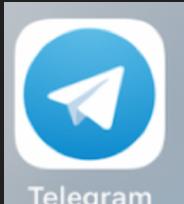
- Ansatz
 - Menschen dort abholen, wo sie sind
 - so rasch wie möglich auf die sicherste Variante wechseln
- Umsetzung
 - Messenger sind häufig Ende-zu-Ende verschlüsselt, ihre Metadaten sind für staatliche Angreifer schwierig zu erlangen – und ihr Gebrauch ist für Kontaktpersonen sehr einfach

Sichere Kommunikation

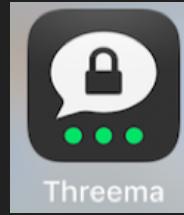
1



2



3



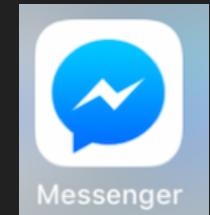
4



M



5



M



Ende-zu-Ende verschlüsselt



E2EE muss aktiviert werden



Open Source

M Metadaten-Speicherung



Im Besitz von Facebook

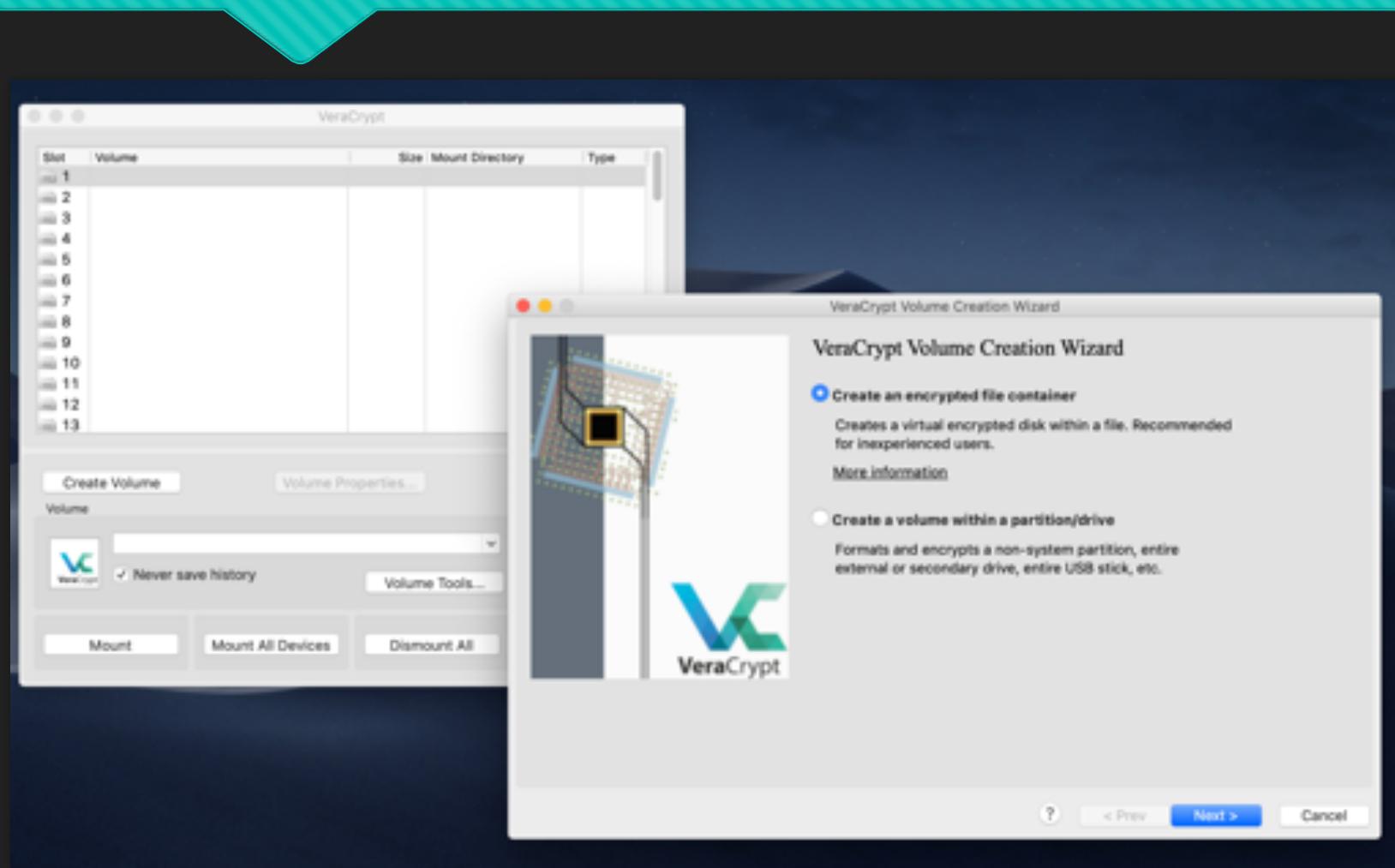
Datensicherung

Starke Verschlüsselung, egal wo

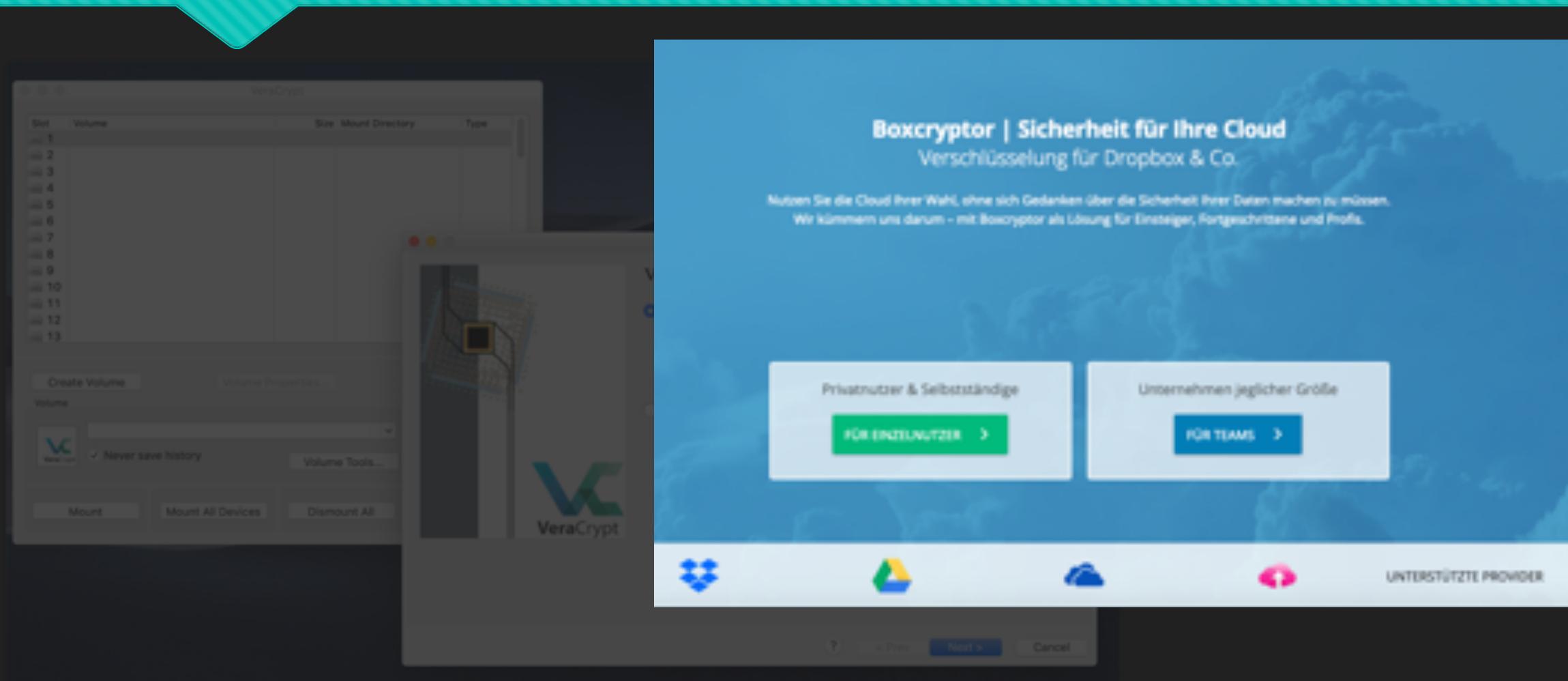
Datensicherung

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

Datensicherung



Datensicherung



The image displays two screenshots side-by-side. On the left is a screenshot of the VeraCrypt application interface, showing a list of volumes and options for creating new volumes or mounting existing ones. On the right is a screenshot of the Boxcryptor website, which offers encryption for cloud storage providers like Dropbox and Google Drive.

VeraCrypt

Volume

Size Mount Directory Type

1

2

3

4

5

6

7

8

9

10

11

12

13

Create Volume

Volume Properties...

Volume

Never save history

Volume Tools...

Mount

Mount All Devices

Dismount All

VeraCrypt

Boxcryptor | Sicherheit für Ihre Cloud

Verschlüsselung für Dropbox & Co.

Nutzen Sie die Cloud Ihrer Wahl, ohne sich Gedanken über die Sicherheit Ihrer Daten machen zu müssen.
Wir kümmern uns darum – mit Boxcryptor als Lösung für Einsteiger, Fangeschickte und Profis.

Privatnutzer & Selbstständige

FÜR INDIVIDUELLEN →

Unternehmen jeglicher Größe

FÜR TEAMS →

UNTERSTÜTZTE PROVIDER

?

< Prev

Next >

Cancel

Kollaboratives Arbeiten

Starker Account-Schutz bei Drittanbietern – oder eine eigene Cloud

Kollaboratives Arbeiten

- Ansatz
 - Accounts der Kollaboratoren 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

Die beste Verteidigung gegen Phishing mit einem Sicherheitsschlüssel

Selbst sehr sicherheitsbewusste Nutzer können von einem geschickten Phishingangriff geäuscht werden. Damit Sie vor dieser Bedrohung geschützt sind, gehen wir bei der erweiterten Sicherheit über die Bestätigung in zwei Schritten hinaus. Zusätzlich zum Passwort ist für die Anmeldung in Ihrem Google-Konto ein physischer Sicherheitsschlüssel erforderlich.

[Weitere Informationen](#) 



Kollaboratives Arbeiten

The screenshot shows a Microsoft Word document window. In the center of the page, there is a large watermark or background image of the Nextcloud logo, which consists of three blue circles arranged in a triangular pattern, followed by the word "Nextcloud". The document itself contains the following text:

Die beste Verteidigung gegen Phishing mit einer Sicherheitsschlü

Selbst sehr sicherheitsbewusste Nutzer können durch einen geschickten Phishingangriff getäuscht werden. Um sich vor dieser Bedrohung geschützt sind, ist eine zweite Sicherheit über die Bestätigung in Form eines QR-Codes. Zusätzlich zum Passwort ist für das Konto ein physischer Sicherheitsschlüssel erforderlich.

Weitere Informationen: [Link](#)

The Microsoft Word ribbon at the top includes tabs for FILE, HOME, INSERT, LAYOUT, REFERENCES, COLLABORATION, and PLUGINS. The HOME tab is selected, showing various font and style tools. The status bar at the bottom indicates "About: nextcloud".

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 | Trainer für Digitale Sicherheit
mail@daniel-mossbrucker.de (PGP: 9C4ED204)