Das Add-on Mailvelope verwenden

Mailvelope - eine Übersicht

„**Mailvelope**“ ist ein **Browser Add-on**, welches für Mozilla Firefox und Google Chrome verfügbar ist. Wenn Sie das mailbox.org-Office mit Mailvelope verwenden, ergeben sich **folgende Vorteile** für Sie:

- Die PGP-Verschlüsselung wird in den Webclient integriert. Sie können E-Mails problemlos verschlüsseln, entschlüsseln und signieren.
- Sie können Ihre PGP-Schlüssel auf Ihrem Rechner verwalten.
- Ihre öffentlichen PGP-Schlüssel können für alle anderen Kommunikationspartner über den mailbox.org-Guard oder über unseren HKPS-Schlüsselserver bereitgestellt werden.
- Ihr privater Schlüssel kann auf verschiedene Geräte via mailbox.org sicher übertragen werden.

Gleichzeitig hat die Nutzung des Add-ons Mailvelope auch einige Nachteile in Bezug auf Sicherheit, daher **folgende Warnhinweise**:

- Plugin-Lösungen im Browser - und damit auch Tools wie Mailvelope - können bei der Verwendung von Cloud-Datenspeichern oder E-Mail-Anhängen Probleme verursachen.
- Ihre Schlüssel werden auf Ihrem Computer **im lokalen Speicher des Browsers** aufbewahrt - das hat mehrere Implikationen:
  - Da der lokale Speicher zur Schlüsselaufbewahrung verwendet wird, ist Mailvelope für den Einsatz auf fremden oder unsicheren Rechnern (z.B. in Internet-Cafés oder im Urlaub) nicht geeignet.
  - Im HTML5 Security Cheat Sheet wird vom OWASP empfohlen, keine sicherheitsrelevanten Informationen im lokalen Speicher des Browsers aufzubewahren, da diese Daten mit XSS-Angriffen kompromittiert werden könnten.
  - Die Sicherheitsanalyse von Mailvelope durch Cure53 (pdf) weist am Ende auf das Risiko von XSS-Angriffe hin. Insbesondere Nutzer von Mozilla Firefox sind dabei gefährdet, da dieser Browser **weniger Schutzmechanismen bietet** als Google Chrome.
    Wir empfehlen allen Firefox Nutzern deshalb, **das Add-on Mailvelope in Kombination mit dem Add-on NoScript einzusetzen**.
    NoScript schließt Sicherheitslücken in Firefox, z.B. durch XSS-Protection.
- Javascript wurde nicht als Programmiersprache für Kryptographieanwendungen entworfen. Funktionen, die als Best Practice für die Implementierung von Kryptografie gelten, sind mit Javascript schlicht nicht realisierbar. Was in anderen Krypto-Implementierungen als schwerer Bug gilt, muss bei Mailvelope einfach als Limitierung durch Javascript hingenommen werden - zum Beispiel:
  - ist es mit Javascript nicht möglich, einen geheimen Schlüssel nach der Benutzung sicher aus dem Hauptspeicher zu löschen (Overwriting memory - why?). Normales Verhalten bei Mailvelope wird beim TOR-Projekt als Sicherheitslücke eingestuft.
  - bei der Programmierung können keine identische Ausführungszeiten für Code Verzweigungen erzwungen werden. Durch Seiten-kanal-angriffe ist es damit möglich, die Reihenfolge der Nullen und Einsen im privaten Schlüssel durch Beobachtung bei der Codeausführung zu rekonstruieren. In modernen Krypto-Bibliotheken ist das eine Sicherheitslücke (z.B. CVE 2016-7056 in OpenSSL, LibreSSL und BoringSSL). Wie einfach Seitenkanalangriffe auf Browser möglich sind, ohne den Rechner zu kompromittieren, haben Forscher in der Arbeit Practical Cache Attacks in Javascript (pdf) gezeigt.

Nach unserer Einschätzung bietet Mailvelope zwar **hinreichende Sicherheit**, ist aber für hohe Sicherheitsanforderungen nicht geeignet.

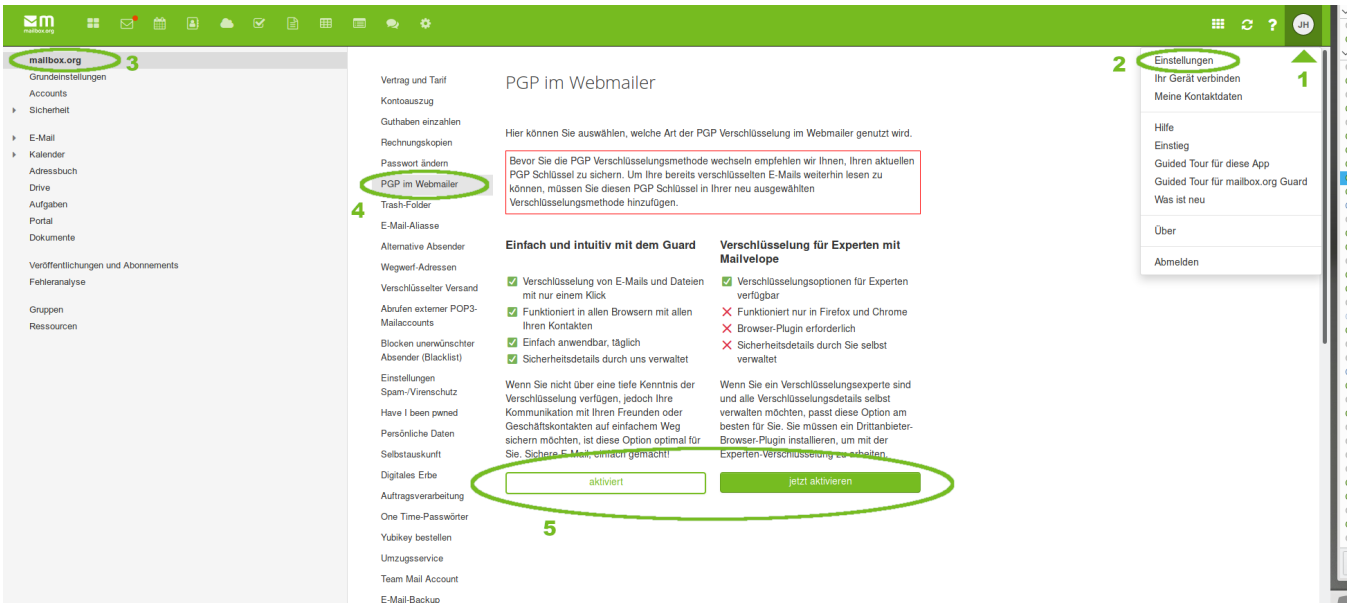
Mailvelope nutzen

Vorbereitung von Mailvelope

Um Mailvelope mit dem mailbox.org-Office zu nutzen, müssen Sie das Add-on zuerst installieren. Alle aktuellen Versionen sind für die Nutzung mit mailbox.org geeignet.
Damit sind die Vorbereitungen bereits abgeschlossen.

Aktivierung der Mailvelope Unterstützung

Nun können Sie im Webclient unter „**Einstellungen -> mailbox.org -> PGP im Webmailer**“ zwischen dem mailbox.org Guard und Mailvelope wählen. Konfigurieren Sie abschließend das Add-On.



Verwandte Artikel

- Wem ich bei mailbox.org vertraue
- Die Zwei-Faktor-Authentifizierung einrichten
- Das temporaere Postfach fuer externe Nutzer
- Den Tor Browser konfigurieren
- Den Tor-Exit-Node von mailbox.org verwenden