Einfuehrung in den mailbox.org-Guard

Wunderbare Neuigkeiten - der mailbox.org-Guard

Mit unserem mailbox.org-Guard haben wir die erste PGP-Implementierung im Webclient, die Sicherheit, Komfort und Unkompliziertheit so miteinander vereint, dass sie von jedermann flächendeckend und standortunabhängig verwendet werden kann. Damit endet die Ära, in der Verschlüsselung für die Massen an komplizierter Einrichtung, umständlichen Konsolenkommandos oder fehlender Unterstützung für Webmail- und Cloud-Systeme scheiterte. Der mailbox.org-Guard ist nicht als Ersatz, sondern als Ergänzung zu OpenPGP gedacht: er ist zu 100% mit OpenPGP kompatibel und kann eine bestehende Ende-zu-Ende-Verschlüsselung eines lokalen E-Mail-Clients ergänzen.
Der Guard ist ein Front-End in unserem Webclient.

Der Anlass

Verschlüsselte Kommunikation mit Hilfe von Plug-ins oder durch Add-ons wie Mailvelope umzusetzen scheitert typischerweise an E-Mail-Anhängen, bei der Verwendung von Cloud-Dateispeichern oder in nicht-vertrauenswürdigen Umgebungen (z.B. in Internet-Cafés oder im Urlaub). Zudem bezweifeln Krypto-Experten seit jeher, dass Kryptographie in einer JavaScript-Umgebung überhaupt sicher umgesetzt werden kann. JavaScript lässt zu viele Angriffsmöglichkeiten und potentielle Schwachstellen offen und kann daher nie als hinreichend sicher bezeichnet werden (mehr dazu in unserem FAQ-Artikel über Mailvelope).

Unsere Lösung

Der mailbox.org-Guard ist eine serverseitige PGP-Implementierung. Das bedeutet, dass das Ver- und Entschlüsseln auf unseren Servern durchgeführt wird. Jeder Nutzer (auch ohne Hintergrundwissen) kann sich im Guard ein Schlüssel(paar) selbst erzeugen. Technisch erfahrene Benutzer können auch ihre eigenen Schlüssel in den Guard laden und diesen parallel zu einer lokalen PGP-Installation verwenden.
Somit haben Sie auch unterwegs auf nicht-vertrauenswürdigen Rechnern jederzeit sicheren Zugriff auf ihre verschlüsselte Kommunikation.

Ihre Schlüssel werden bei uns, in einer sicheren Umgebung verwaltet - auf Servern, die von professionellen IT-Spezialisten administriert werden. Die Schlüssel sind dabei durch ein nur Ihnen bekanntes Passwort geschützt und somit selbst unserem Zugriff entzogen. Nur wenn sich ein mailbox.org-Nutzer eingeloggt hat, kann er seinen privaten Schlüssel (mit Passwortabfrage) zum Gebrauch entschlüsseln. Zahlreiche weitere Schutzmechanismen verhindern, dass diese PGP-Schlüssel im Programmspeicher auf den Servern im Klartext gespeichert werden und wir - oder jemand anderes - serverseitig selbst bei einem aktiven Login des Nutzers Zugriff auf die PGP-Schlüssel erhalten.

Natürlich kann und sollte man es trotzdem kritisch sehen, den eigenen privaten Schlüssel (Private Key) aus der Hand zu geben und auf fremden Servern speichern zu lassen. Wir wollen das nicht verheimlichen und betonen dieses Problem ausdrücklich. Es stellt sich aber die durchaus berechtigte Frage, ob diese (weiterhin passwortgeschützten) Schlüssel auf unseren Servern nicht trotzdem viel sicherer aufgehoben sind, als auf z.B. Ihrem Smartphone.

Sicherheitsexperten wie M. Cardwell warnen ausdrücklich davor, private (OpenPGP-) Schlüssel auf extrem unsicheren Geräten wie Smartphones zu nutzen. Der mailbox.org-Guard bietet Ihnen als Browser-Lösung auch ohne einen auf dem Smartphone gespeicherten Schlüssel jederzeit vollen Zugriff auf Ihre verschlüsselten E-Mails.

Da die Ver- und Entschlüsselung auf dem Server stattfindet, bietet der mailbox.org-Guard keine echte Ende-zu-Ende-Verschlüsselung. **Ziel des Guards ist es, „hinreichende Sicherheit“ zu gewährleisten und damit eine gute Mischung aus bequemer Benutzbarkeit zu bieten. Diese Sicherheitsstufe allein ist für z.B. Whistleblower oder Nutzer mit extrem hohen Sicherheitsanforderungen nicht ausreichend!**

So oder so bleibt der mailbox.org-Guard ein Angebot für diejenigen, die diesen **Service im Alltag nutzen wollen**. Wer zu anderen Schlüssen kommt oder höhere Anforderungen hat, kann und soll weiterhin die lokale PGP-Installation in seinem Mailclient verwenden.

Verschlüsselte E-Mails an Menschen ohne entsprechende Vorkenntnisse

Auch wenn Ihre Kommunikationspartner **keine Kunden bei mailbox.org sind und keine PGP-Schlüssel bereitstellen** können, bietet der Guard die Möglichkeit sicherer Kommunikation: wir erzeugen auch für externe Nutzer temporäre Postfächer auf einem unserer Server, in denen der jeweilige Empfänger die an ihn gerichteten, verschlüsselten E-Mails lesen und beantworten kann. Aus unseren gehobenen Ansprüchen an E-Mail-Sicherheit und Schutz Ihrer Privatsphäre resultiert ein einzigartiger Service: das temporäre Postfach, geschützt durch verschlüsselte Nutzer-Server-Verbindung auf dem neuesten Stand der Technik, serverseitige Verschlüsselung, individuelle Zugangsdaten und optionale Zwei-Faktor-Authentifizierung.

Zusammenfassung

Die Vorteile

- mailbox.org-Guard ist zu **100% kompatibel** mit dem etablierten OpenPGP-Standard
- Auch Menschen, für die Verschlüsselung Neuland ist, benötigen **nur wenige Klicks zur Aktivierung**.
- **Intuitive Bedienbarkeit** im Browser und auch unterwegs
- **Serverseitige PGP-Implementierung**, so dass der PGP-Schlüssel nicht in einen potentiell unsicheren Browser gelangt
- Ermöglicht das uneingeschränkte Lesen und Schreiben PGP-verschlüsselter E-Mails **auf Smartphones** mittels Browser

- **Temporäre Postfächer** für eine weltweite, sichere Kommunikation auch mit Menschen ohne Verschlüsselungsvorkenntnisse
- Business-Accounts bei mailbox.org einer Gruppe können auf eine **gemeinsame Schlüsselverwaltung** zurückgreifen

Die Nachteile

- Ver- und Entschlüsselung erfolgt auf dem Server, daher keine vollständige Ende-zu-Ende-Verschlüsselung.
- Speicherung von privaten PGP-Keys auf fremden Servern (als prinzipielles Problem)
- Der mailbox.org-Guard bietet „**hinreichende Sicherheit**“, aber keine „**absolute Sicherheit**“

Verwandte Artikel

- Den Tor Browser konfigurieren
- Den Tor-Exit-Node von mailbox.org verwenden
- Uebersicht: Team Mail - ehemals Familienaccounts
- Den Tor Messenger konfigurieren
- Uebersicht: Was ist Jabber XMPP