Wie der private Schluessel geschuetzt wird

Anmerkung: dieser Artikel beantwortet eine spezifische Frage, die Sie nur betrifft, falls Sie den mailbox.org-Guard aktiviert haben.

Wie wird verhindert, dass Dritte oder selbst die Administratoren von mailbox.org Zugriff auf Ihren privaten Schlüssel erhalten?

Die Absicherung des Schlüssels

Wenn Sie einen PGP-Schlüssel (1) hochladen oder über den Guard erzeugen, dann wird dieser Schlüssel mit einem, **nur Ihnen bekannten Passwort verschlüsselt**. **Dieses Passwort ist nirgendwo auf unseren Systemen gespeichert** und muss vom Ihnen separat eingegeben werden, wenn Entschlüsselung (z.B. zum Lesen einer verschlüsselten E-Mail oder zum Bearbeiten einer verschlüsselten Textdatei) notwendig wird. Solange Sie das Guard-Passwort nicht eingeben, liegen die Schlüsseldateien auf dem Server also verschlüsselt - und somit unzugänglich (auch für uns).

Die sichere Verwendung Ihres Schlüssels

Wenn Sie sich einloggen, wird Ihr Schlüssel (1) für genau eine Aktion entschlüsselt: um mit einem jedes Mal neu erzeugten, zufälligen Schlüssel (2) für diesen Login verschlüsselt und vorübergehend bei mailbox.org gespeichert zu werden. Das temporäre Passwort wird in Ihrem Browser zwischengespeichert, der temporär verschlüsselte PGP-Schlüssel (2) auf unserem mailbox.org-Server. **Weder Ihre jeweiligen Passwörter noch Ihr PGP-Schlüssel (1) werden damit dauerhaft auf Festplatte oder im Programmspeicher unserer Server unverschlüsselt abgelegt.**

Jede Seite hat nur „**halbes**“ **Wissen** über die Informationen, die notwendig sind, um auf den PGP-Schlüssel (1) - und damit Ihre verschlüsselten Daten - zuzugreifen. Auch wenn ein Dritter auf eine der beiden Informationen Zugriff erlangen könnte, könnte er damit nicht Ihre sensiblen Daten kompromittieren.

Sobald Sie sich ausloggen, wird die temporäre, verschlüsselte Kopie des Schlüssels (2) gelöscht. Selbst wenn jemand nachträglich das temporäre Passwort aus Ihrer Login-Sitzung ausliest, ist dieses mit Ihrem Ausloggen bereits unbrauchbar geworden.

Angriffsszenarien

Wenn ein Angreifer **während der Übertragung** an den Browser des Nutzers den temporären Schlüssel (2) abfangen würde, hätte er damit keine Möglichkeit, an den weiterhin nur auf dem Server gespeicherten, echten PGP-Schlüssel (1) zu gelangen. Ein Login des Angreifers würde **eine neue, unabhängige Sitzung starten**, in der das erbeutete, temporäre Passwort wertlos wäre.

Ein Angreifer hingegen, **der (direkten oder entfernten) Zugriff auf Ihr Gerät hat** und so bereits lokale Kontrolle über Ihren Webbrowser besitzt, könnte vom Browser die aktuelle Sitzung Ihres mailbox.org-Logins übernehmen und so auch grundsätzlich in Besitz des temporären Schlüssels (2) gelangen - wobei dieser nur kurzzeitig, während Ihres aktuell laufenden Logins Gültigkeit hat und damit nicht dauerhaft vom Angreifer verwendbar wäre.

Allerdings hätte der Angreifer zu diesem Zeitpunkt bereits lokalen Zugriff auf Ihr Gerät und Ihren Browser und damit auch Zugriff auf Ihre E-Mails und alle dort aktuell verarbeiteten Daten - unabhängig davon, ob diese durch eine lokale PGP-Installation auf Ihrem PC oder durch unseren Guard serverseitig ver- bzw. entschlüsselt werden.

Es stellt sich also die Frage der Sicherheit (des elektronischen Gerätes) eines jeden Anwenders. Die Verwendung des mailbox.org-Guard eröffnet keine Sicherheitslücken oder Angriffsmöglichkeiten, die nicht bereits durch die Hardware, das Betriebssystem und installierte Drittanbieter-Software gegeben sind. Im Gegenteil: man könnte sogar sagen, dass bei der Verwendung des Guards der Angreifer immerhin nicht sofort an die PGP-Schlüssel des Anwenders gelangen kann, da diese auf den mailbox.org-Servern liegen.

Verwandte Artikel

- Welche PGP-Standards Guard unterstuetzt
- Die Zwei-Faktor-Authentifizierung einrichten
- Den Tor-Exit-Node von mailbox.org verwenden
- Das temporaere Postfach fuer externe Nutzer
- Das verschluesselte Postfach