Richtlinie zum „Software-Sprint“

EMASS – E-Mail-Accountverwaltung mit Self-Service

Schlussbericht

Zuwendungsempfänger:

Dittler Meurer GbR

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 01IS18S33 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Kurze Darstellung der Aufgabenstellung und Motivation

Bei den meisten Webdiensten haben die technische Administrator*in auch die komplette Macht über den Inhalt des Systems. Datenschutzfreundliche Webdienste sollten den Nutzer*innen aber möglichst viel Autonomie bieten und den Administrator*innen möglichst wenig Macht.

Mit dem Projekt sollte eine bestehende E-Mail Accountverwaltung als Open Source Software weiterentwickelt und insbesondere um die neuen Funktionen E-Mail-Postfachverschlüsselung und Account-Wiederherstellungs-Prozess erweitert werden. Verschlüsselte Postfächer sind für Administrator*innen nicht mehr einsehbar und die Verschlüsselung kann nicht umgekehrt werden. Dazu waren folgende Meilensteine vorgesehen:

1. Heben der Codebase auf Symfony 4.0
2. Datenbankabstraktion
3. Interner Audit
4. Erweiterung der Tests
5. Integration des Alias-Self-Service
6. Einmal-/SPAM-Aliase
7. Integration von Trees
8. Integration Domain-spezifischer Admins
9. 2FA implementieren
10. Dokumentation erstellen
11. Bekanntmachung
12. Erfahrungen und Probleme aus Praxiseinsatz berücksichtigen

Beitrag des Projektes zu den Zielen der Förderinitative „Software-Sprint“

Wir wollten mit dem Projekt kleinere E-Mail-Provider und deren Nutzer*innen unterstützen. Dazu haben wir uns mit anderen unkommerziellen Mailbetreibern und ausgetauscht und sie über die Veröffentlichung informiert. E-Mail-Nutzer*innen profitieren konkret von dem Projekt, wenn sie einen E-Mail-Account bei einem Provider haben. Damit trägt das Projekt insbesondere zum Themenfeld „Datenschutz“ bei.

Ausführliche Darstellung der Ergebnisse

Die E-Mail Accountverwaltung wurde deutlich in ihren Funktionen erweitert, der Quellcode an vielen Stellen grundsätzlich überarbeitet und mit umfangreichen Unit-Tests, sowie funktionalen Tests, eine gute Grundlage für anhaltende Codequalität gelegt. Mit Ausnahme der Zweifaktorauthentifizierung konnten wir alle zu Beginn definierten Meilensteine erfolgreich erreichen. Die bedeutendsten neu eingeführten nutzer*innenseitigen Funktionalitäten sind:

- E-Mail Postfachverschlüsselung mittels Dovecot MailCrypt
- Wiederherstellungsprozess für Accounts bei verloren gegangenem Passwort
- Domainadmin-Selfservice: Optional Admin-Funktionen für ganze Domains
- Alias-Selfservice: Nutzer*innen können sich selbst gewählte sowie Zufalls-Aliases anlegen
- Grundlegende Arbeiten am User Interface für bessere Benutzer*innenfreundlichkeit

Die Projektbegleitung durch die Open Knowledge Foundation hat uns insbesondere bei der organisatorischen und administrativen Arbeit deutlich unterstützt. Auch die zwei in der Projektförderung enthaltenen Coachings (in unserem Fall UI/UX Coachings durch Simply Secure) haben uns stark weitergeholfen.

Zielgruppe, Nutzen und mögliche Weiterentwicklungen

Die erreichten Nutzer*innen profitieren unmittelbar in der Sicherheit ihrer E-Mail-Daten. Die Inhalte auf dem Server liegender E-Mails sind nicht länger den Administrator*innen der E-Mail-Server zugänglich.

Die Veröffentlichung der Software als Open Source bringt viele Vorteile mit sich. Einmal können auch andere (kleine) E-Mail-Provider die Software für sich verwenden, oder zumindest als Referenz für eigene Lösungen verwenden. Zum anderen aber ist es den Nutzer*innen und weiteren Interessierten möglich, die Funktionalität der Software zu überprüfen und damit zu verifizieren, dass die vom E-Mail-Provider versprochene Sicherheit auch erfüllt wird. Wissensverteilung, Vermeidung von doppelter Arbeit und Transparenz sind also starke Gründe für Open Source.

Wir haben bereits Ideen, das Projekt weiterzuentwickeln. So wollen wir die Accountverwaltung zu einem generischen Authentication- und Identity-Provider umbauen, welcher die Verwaltung von Nutzer*innen und ihrer Rechten service-unabhängig ermöglicht.

Als Beteiligte konnten wir unsere fachlichen Kompetenzen im Rahmen des Projekts ausbauen.

Kurze Darstellung der Arbeiten, die zu keiner Lösung geführt haben

Wir hatten zu Beginn vor eine andere Implementierung von E-Mail-Postfachverschlüsselung zu verwenden. Nach ausführlicher Untersuchung der verfügbaren Lösungen wurde uns klar, dass Dovecot MailCrypt die zukunftsträchtigere und technisch saubere Implementierung ist. Wir haben uns daraufhin für diese Lösung entschieden.

Kurze Angabe von Präsentationsmöglichkeiten für mögliche Nutzer

Unser Projekt findet sich unter https://github.com/systemli/userli. Die zugehörige Dokumentation ist unter https://systemli.github.io/userli/ zu finden.

Kurze Erläuterung zur Einhaltung der Arbeits- und Kostenplanung

Wir sind selbst überrascht, wie realistisch sich unsere anfängliche Projektplanung retrospektiv darstellt. Die Entwicklung von Unit-Tests zu Beginn war deutlich arbeitsaufwändiger als gedacht, da sie auch andere Probleme offenbarte. Die meisten anderen Teilaufgaben entsprachen aber in etwa dem geschätzten Arbeitsaufwand.

Kurze Darstellung von etwaigen Ergebnissen bei anderen Stellen

Es gab keine nennenswerten Einflüsse durch andere Institutionen, die den Verlauf des Projekts maßgeblich beeinflusst haben.