Richtlinie zum „Software-Sprint“

Cloud Native LEAP VPN – Making LEAP VPN Composable and Reusable by Using Cloud-Native Tools

Schlussbericht

Zuwendungsempfänger*in:

NuytsJohannesVeit GbR

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Forschung, Technologie und Raumfahrt unter dem Förderkennzeichen 01IS25S02 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei dem*der Autor*in.

Kurze Darstellung der Aufgabenstellung und Motivation in der regulären Förderphase (Entwicklung eines Prototypen)

Was war Deine Motivation? Welches Problem wolltest Du mit Deinem Projekt lösen? Wie war die geplante Vorgehensweise zur Problemlösung (auch Angabe der wichtigsten Meilensteine)?

Ziel des Projektes war es, den quelloffenen VPN-Stack von LEAP in die Cloud zu integrieren. Schon heute bietet diese Software bereits über 100.000 Nutzenden - auch aus der EU - durch die VPN Dienste von Riseup Networks, The Calyx Institute und Solitech einen starken Schutz ihrer Privatsphäre. LEAPs bisherige Open-Source-Plattform lilypad basiert auf Ansible und Float und ist ein minimalistisches System zur Container-Orchestrierung, das als Mittelweg zwischen Ansible und Kubernetes konzipiert ist. Die Integration von Float in bestehende Deploymentprozesse funktioniert jedoch nicht reibungslos und als Nischenlösung ist sie weithin unbekannt, was intensives Einarbeiten nötig macht. Die Integration von bekannten Cloud-nativen Lösungen wie Terraform und Kubernetes baut die Barrieren beim Aufsetzen von LEAP VPN für Administrator*innen ab, indem die Einrichtung stark standardisiert und modularisiert wird. Außerdem ermöglicht sie eine bessere Skalierung und Effizienz der VPN-Dienste. Von den Änderungen profitieren die derzeitigen LEAP VPN-Anbieter und die gesamte LEAP VPN-Landschaft wird gestärkt, da sich Einsatzmöglichkeiten für weitere Anbieter ergeben, die ihre Dienste bereits über Cloud-native Lösungen verwalten.

Im Rahmen der Förderung wurden die wichtigsten Komponenten des VPN Systems als wiederverwendbare, Cloud-native Bausteine zur Verfügung gestellt. Dabei lag der Fokus auf folgenden Komponenten: OpenVPN, das zum Erzeugen sicherer Tunnel genutzt wird, kresd - einem rekursivem DNS-Resolver zur Namensauflösung von Internetaddressen, menshen - einem Server, der die Konfigurationsschnittstelle für VPN-Clients bereitstellt, Prometheus - einer Komponente, die der Überwachung der Integrität der VPN-Dienste dient, sowie obfsvpn - einem Werkzeug zur Verschleierung von VPN Verkehr, das die Umgehung von Internetzensur möglich macht. Für diese Bausteine wurden Terraform Module und Helm Charts entwickelt, die die Infrastruktur als Code beschreiben und die Bereitstellung von Software ermöglichen.

Folgende Meilensteine strukturierten unsere Arbeit während der ersten Förderperiode:
M1 (Monat 2):
Terraform Prototyp - Terraform-Module zur vereinfachten Bereitstellung ausgewählter LEAP-Plattformkomponenten für Standard-Cloud-Anbieter (Hetzner, OVH).
M2 (Monat 4):
Kubernetes Protyp - Helm Charts, um die LEAP-Plattformkomponenten, die vom Clustering profitieren könnten (z.B. OpenVPN), innerhalb einer Kubernetes-Umgebung bereitzustellen.
M3 (Monat 6):
Terraform + Kubernetes - Erstellen von podlily: ein Git Repository mit Beispiel-Konfigurationsdateien für Terraform und Helm, das eine einfache Bereitstellung, Anpassung und Verwaltung von LEAP-Plattformkomponenten ermöglicht.

Beitrag des Projektes zu den Zielen der Förderinitiative „Software Sprint“

Welche Bezüge gibt es zu den Themenfeldern „Infrastruktur“ und „Sicherheit“ des Software Sprints oder zu weiteren gesellschaftlich relevanten Zielen bzw. Lösungsansätzen?

Die LEAP-Software bietet die (quelloffenen) Werkzeuge, um einen datenschutzfreundlichen, freien VPN-Dienst einzurichten, der ohne Benutzer*innennamen, E-Mails oder identifizierende Zahlungsdaten auskommt. Seit Jahren wird sie im Produktivsystem von Riseup Networks und The Calyx Institute verwendet, unseren Partner Providern, die sich digitaler Sicherheit und Datenschutz verschrieben haben. Kürzlich hat Solitech - ein in der EU ansässiger Verein mit dem Ziel der Förderung sozialer Teilhabe und Aufklärung über Datenschutz im digitalen Raum - einen offenen, auf Zensurumgehung fokussierten LEAP VPN Dienst aufgesetzt, der sich an ein russisches Publikum richtet. Durch die Entwicklung eines ethischen, kostenfreien VPNs hilft LEAP benachteiligten und zensierten Personengruppen freien Zugang zu Informationen zu erlangen und reduziert deren Risiko, von Internetfirmen und Regierungen überwacht und verfolgt zu werden. Dies sind wesentliche Eckpfeiler für freie, demokratische Meinungsäußerung und wichtige Voraussetzungen für zivilgesellschaftliches Engagement. Durch die Einführung von Cloud-nativen Werkzeugen bauen wir die Barrieren beim Aufsetzen von LEAP VPN für Anbieter ab, indem wir die Einrichtung stark standardisieren und modularisieren. Wir haben uns im Rahmen der Förderung um weitere Kooperationspartner*innen bemüht, sodass wir

neben den technischen auch die organisatorischen Voraussetzungen geschaffen haben, dass zukünftig weitaus mehr Menschen einen einfachen Zugang zu diesem datenschutzfreundlichen VPN Dienst erhalten können.

Ausführliche Darstellung der Ergebnisse in der regulären Förderphase (Entwicklung eines Prototypen)

Welche konkreten Ergebnisse hast Du erzielt? Konnten alle Meilensteine erreicht werden? Welche zusätzlichen Erkenntnisse hast Du aus der Projektarbeit gewonnen, auch im Hinblick auf die Begleitung durch die Open Knowledge Foundation?

Wir konnten alle Meilensteine innerhalb der regulären Förderphase erreichen:

- Terraform:

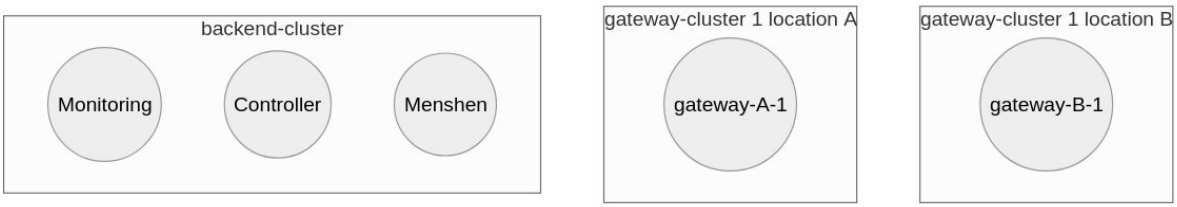


Abb. 1: Über Terraform bereitgestellte Kubernetes Cluster und Nodes

  - Zu Beginn galt es einige Designentscheidungen zu treffen: bei Cloud-Providern entschieden wir uns für Hetzner (Deutschland) und OVH (Frankreich). Beide sind vergleichsweise preiswerte Anbieter mit Sitz in der EU, die Terraform Module anbieten, was die Bereitstellung von Ressourcen dieser Provider mit Terraform ermöglicht. Wir haben uns dabei bewusst aus Datenschutzbedenken gegen US-amerikanische Big-Tech Anbieter, wie Google Cloud und AWS entschieden. Im Laufe des Projekts mussten wir allerdings feststellen, dass die Bereitstellung eines VPN-Dienstes mit den gewählten Cloud Providern nicht gleichermaßen gut unterstützt wird. So setzt OVH von Anfang an harte Grenzen bei der Anzahl der Server-Ressourcen, was die Skalierbarkeit des VPN Services beschränkt, und begrenzt außerdem mit Maßnahmen wie Throttling den Datendurchsatz beim Ausführen von Geschwindigkeitstests auf deren Servern. Zum Zeitpunkt des Förderungsendes warten wir nach wie vor auf eine Reaktion des Support-Teams von OVH, um diese Beschränkungen für unser Projekt aufzuheben.
  - Um eine optimale globale Skalierbarkeit zu gewährleisten, entschieden wir uns dazu, die LEAP VPN Backend Komponenten als K3S Cluster mit 3 Knoten zu realisieren und Gateways als Single-Node Cluster. So ist das LEAP VPN System jederzeit leicht durch weitere Gateways erweiterbar, sollte eins geblockt werden oder überlastet sein.
  - Die Cluster-Ressourcen, die zur Realisierung der Cluster in der Cloud nötig sind (Server, Subnetze, IP-Adressen, SSH-Schlüssel, ...) wurden als Module in der offiziellen Terraform Registry veröffentlicht. Dies ermöglicht eine einfache und schnelle, aber auch leicht konfigurierbare Bereitstellung.

Den Code für die Einrichtung auf Hetzner und OVH hosten wir auf Gitlab in den Repositories terraform-hetzner-k3s-vpn und terraform-ovh-k3s-vpn. Wird dort ein Commit als Release getaggt, wird automatisch eine neue Version in der Registry veröffentlicht. Die beiden Module sind hier zu finden: https://registry.terraform.io/modules/leapcode/k3s-vpn

  - Wir legten eine Entwickler*innendokumentation im jeweiligen Repository der Terraform Module an.

- Kubernetes:

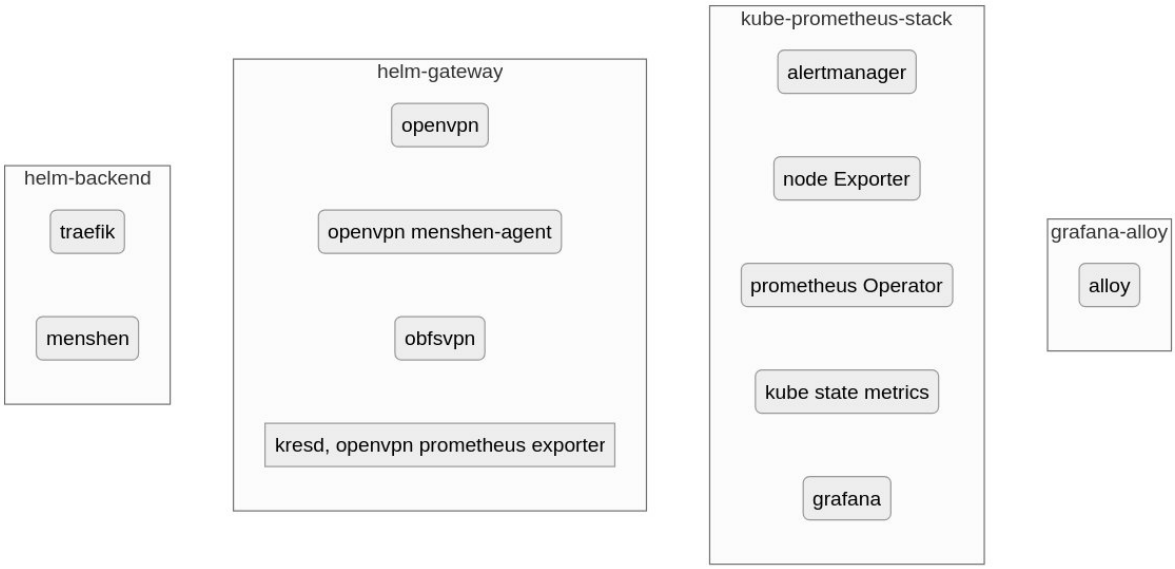


Abb.2: Übersicht über die entwickelten und integrierten Helm Charts

  - Wir entschieden uns für K3S, eine leichtgewichtigere Kubernetes-Distribution, die weniger Ressourcen benötigt und einfacher zu installieren und zu betreiben ist. Die Entscheidung passt gut zu unseren Zielen, das Installieren und Betreiben des LEAP VPN Stacks zu vereinfachen und Ressourcen zu schonen.
  - Auf dem Backend Cluster laufen die Management-Services eines K3S Controller Knotens, die Anbieter Konfigurations-API menshen und der Reverse-proxy Traefik. Wir haben sie in einem Helm Chart zusammengefasst, was das Anpassen und Installieren der Services sehr einfach macht. Der Code befindet sich im Gitlab Repository helm-backend, aber wird auch als komprimierte tgz Datei veröffentlicht.
  - Auf dem Gateway Cluster laufen die zuvor beschriebenen LEAP VPN Komponenten OpenVPN, obfsvpn und Kresd. Auch sie wurden als Helm Chart zusammengefasst und als tgz Datei veröffentlicht. Der Code ist im Gitlab Repository helm-gateway zu finden.

- Terraform und Kubernetes:
  - Um das Bereitstellen und Administrieren der beiden Cluster möglichst einfach zu machen, erstellten wir das Gitlab Repository podlily. Es enthält alles was dafür nötig ist und baut auf den veröffentlichten Terraform Modulen und Helm Charts auf.

- Teil von podlily sind neben Beispiel-Konfigurationsdateien für Terraform und Helm auch einige Hilfsskripte, die eine verschlüsselte und sichere Kommunikation gewährleisten: zum Erzeugen von x509-Zertifikaten für die sichere Kommunikation über OpenVPN, zum Erzeugen von Geheimnissen für die sichere Kommunikation zwischen Gateway und Backend, und mehr.
- Alle LEAP VPN Dienste laufen als Pods auf den Knoten der beiden K3S Cluster. Sie können über die Konfigurationsdateien in Podlily einfach angepasst werden und mit dem Kubernetes Kommandozeilen-Tool Kubectl verwaltet werden. Zu diesem Zweck gibt es in Podlily auch ein Hilfsskript, das den Zugriff und das Verwalten von Clusterressourcen mithilfe von SSH Port-Forwarding vom Arbeitsrechner aus möglich macht.

Kurze Darstellung der Aufgabenstellung und Motivation in der Second-Stage-Förderung (Aufbau einer nachhaltigen Projektstruktur)

Was war Deine Motivation? Welches Problem wolltest Du mit Deinem Projekt lösen? Wie war die geplante Vorgehensweise zur Problemlösung (auch Angabe der wichtigsten Meilensteine)?

Die Second-Stage-Förderung wollten wir nutzen, um den von uns entwickelten, Cloud-nativen LEAP VPN Prototypen langfristig auf stabile Beine zu stellen.

- M4 Hardening: Für unseren VPN Dienst sind Sicherheit und Datenschutz absolut zentraler Teil des Produktversprechens. In der Second Stage wollten wir bessere Lösungen für bekannte Schwachstellen finden, gerne mit der Unterstützung externer Auditor*innen.
- M5 Dokumentation und Tests: Die Hauptmotivation für die Cloud-native Bereitstellungsart war das vereinfachte Einrichten und Administrieren der LEAP VPN Komponenten. Doch das kann Interessierten nur gelingen, wenn es leicht verständliche Tutorials gibt und die Infrastruktur gut dokumentiert und erklärt wird. Darum wollten wir hierfür in der Second Stage viel Zeit einräumen.
- M6 Gründung und langfristige Finanzierung: Wir haben beschlossen, dass wir selber VPN Anbieter werden wollen. Wir erhoffen uns davon, das Projekt langfristig finanziell abzusichern und weiterzuentwickeln. Diesen enormen Schritt wollten wir in der Second Stage vorbereiten, um mit professioneller Unterstützung in den Coachings u.a. zu den Themen Grundwerte, Branding und Marketing zu arbeiten, sowie einen Geschäftsplan zu erstellen. Eine weitere langfristige Finanzierungsmöglichkeit liegt in B2B Service-Verträgen, eine Idee, die wir während der Second Stage weiter ausbauen wollten.

Ausführliche Darstellung der Ergebnisse in der Second-Stage-Förderung (Aufbau einer nachhaltigen Projektstruktur)

Welche konkreten Ergebnisse hast Du erzielt? Konnten alle Meilensteine erreicht werden? Welche zusätzlichen Erkenntnisse hast Du aus der Projektarbeit gewonnen, auch im Hinblick auf die Begleitung durch die Open Knowledge Foundation? Was

wurde unternommen bezüglich einer Konsolidierung und Verbreitung und besseren Verwertung der Ergebnisse aus der ersten Phase?

In der Second Stage haben wir bezüglich aller beschriebenen Ziele enorme Fortschritte und Ergebnisse erzielt. Die Coachings waren von großem Nutzen, insbesondere im Bereich Unternehmensgründung, in dem wir vorher über keine besonderen Kenntnisse verfügten. Der Workshop als Teil des Abschlussevents der Second Stage motivierte uns, gleich praktisch zu werden und ein User Testing durchzuführen.

- Hardening:
    - Wir entschieden uns, git-crypt für das Verschlüsseln von Geheimnissen zu nutzen. Das erlaubt es, alle podlily Dateien, die sensible Informationen zum Cluster enthalten (z.B. Zertifikate, Schlüssel, Terraform Informationen) verschlüsselt z.B. in einem Git Repository innerhalb eines Teams zu teilen. So wird das gemeinsame, sichere Administrieren von LEAP VPN Clustern erleichtert.
    - Leider konnte uns kein Coaching zum Thema Sicherheit angeboten werden, sodass wir andere sicherheitsrelevante Ziele wie den Betrieb von VPN Containern ohne Root-Rechte nicht im Rahmen der Förderung erreichen konnten. Wir bemühen uns momentan außerhalb der Prototype Fund Projektförderung darum, dafür Lösungen zu entwickeln.
    - Zentral für die Administrierung des LEAP VPN ist auch das Monitoring, also die Systemüberwachung der Cluster. Für das Backend entschieden wir uns für Kube-prometheus-stack, eine Sammlung von Kubernetes-Manifesten, Grafana-Dashboards und Prometheus-Regeln, ergänzt durch Dokumentation und Skripte, um mithilfe des Prometheus Operators eine einfach zu bedienende Ende-zu-Ende-Überwachung von Kubernetes-Clustern mit Prometheus zu ermöglichen. So funktioniert die Überwachung der Clusterressourcen ohne großen eigenen Konfigurationsaufwand. Die Installation erfolgt wieder einfach über einen Helm Chart. Kube-prometheus-stack ist eigentlich für die reguläre Kubernetes-Distribution konzipiert und musste für unser K3S Cluster leicht umkonfiguriert werden, was sich aber als kein großes Problem erwies.
    - Für die Überwachung des Gateway Clusters entschieden wir uns für Grafana Alloy, eine Open-Source-Distribution des OpenTelemetry Collectors mit integrierten Prometheus-Pipelines. Alloy sammelt Daten über das Gatewaycluster und Metriken von dem darauf laufenden OpenVPN und sendet sie verschlüsselt und authentifiziert an den Prometheus Operator auf dem Backend Cluster. Alle Metriken werden in Grafana visualisiert. Es gibt vorgefertigte Dashboards für Knotenmetriken von Kube-prometheus-stack und wir erstellten ein eigenes Dashboard zur Überwachung von OpenVPN-Metriken wie der Anzahl der mit einem Gateway verbundenen Nutzer*innen. Auf Basis dieser Daten können im laufenden Betrieb Entscheidungen getroffen werden, z.B. ob ein neues Gateway bereitgestellt oder IPs rotiert werden sollten.
- Dokumentation und Tests:

    - Neben der Dokumentation der einzelnen Repositories in deren README‘s erstellten wir ein ausführliches Tutorial im podlily README, das Interessierte durch den gesamten Prozess des Aufsetzens von LEAP VPN leitet.
    - Ebenfalls im podlily Repository erstellten wir weitere Dokumentationen im Unterordner docs, u.a. einen Überblick über die Infrastruktur mit Grafiken und eine Seite mit hilfreichen Tipps zum Thema Troubleshooting.
    - Um Administrator*innen einen einfachen Einstieg in die Software zu ermöglichen, haben wir uns zum Ziel gesetzt, die wesentlichen Informationen zum Deployment zentral auf docs.leap.se zu veröffentlichen. Wir haben Skripte geschrieben, die die README‘s, sowie Übersichts- und Erklärseiten der verschiedenen Repositories in das Repository unserer Dokumentationsseite kopieren. Dadurch erhalten wir langfristig einen Mechanismus, der es uns erlaubt die Dokumentation im Rahmen der Weiterentwicklung der einzelnen Repositories anzupassen und die Dokumentation auf docs.leap.se automatisch zu synchronisieren.
    - Wir testeten die Verständlichkeit und Anwendungsfreundlichkeit der Tutorials beim Abschlussworkshop der Second Stage mit Menschen, die Interesse am Bereitstellen und Administrieren von LEAP VPN haben. Wir holten vor Ort und in einem Fragebogen im Anschluss Feedback ein, auf dessen Basis wir die README‘s verbesserten.
    - Ebenfalls für den Abschlussworkshop stellten wir eine Präsentation zusammen, in der wir die Motivation für die Umstellung auf Cloud-native Bereitstellungsmethoden darstellen, unser ursprüngliches Deploymentframework lilypad mit dem neu entwickelten podlily vergleichen. Sie diente auch als Leitfaden für einen praxisbezogenen Workshop. Dieser wird voraussichtlich bereits Anfang Juli im Rahmen eines IT Camps wiederholt.
- Gründung und langfristige Finanzierung:
    - Der Schritt, einen eigenen VPN anzubieten ist aufregend und erfordert viele schwierige Entscheidungen unsererseits, mit denen wir uns ausführlich beschäftigten.
    - Mit Superbloom Coach Allen Gunn hatten wir Coachings zu den Themen Grundwerte und Mission. Wir erarbeiteten und verschriftlichten die gemeinsame Grundlage unserer Zusammenarbeit und das zentrale Wertversprechen unseres neuen VPN Dienstes, sowie Fokusgruppen möglicher Nutzer*innen.
    - Mit Superbloom Coach Matt Stempeck besprachen wir zentrale Fragen bezüglich Branding. Wir führten mit beinahe 100 Teilnehmenden eine Umfrage bzgl. des Namens für das VPN durch und einigten uns schließlich auf Coop VPN. Der Name steht gleichzeitig für unser Alleinstellungsmerkmal, den Betrieb des VPNs als Kollektiv in der Hand der Mitarbeitenden („worker-owned Cooperative“).
    - Für das Artwork von Coop VPN arbeiten wir mit dem fantastischen Künstler namens Roger Peet zusammen, der für uns Maskottchen zeichnet, die die Stati einer VPN Verbindung in der Client App

representieren werden. Sie werden außerdem Teil der Markenbildung werden.



Abb.3: Artwork von Roger Peet, gestaltet für Coop VPN

- Als besonders herausfordernd und aufschlussreich hat sich das Erstellen eines Geschäftsplans für die Unternehmensgründung erwiesen. Wir haben ein solides 7-Jahres-Geschäftsmodell entwickelt, das Annahmen zu Wachstum und Abwanderung enthält. Es umfasst monatliche und jährliche Zahlungsstrukturen mit der Möglichkeit, die prozentualen Annahmen für jede Struktur anzupassen. Die Geschäftsidee lautet: Aufbau eines datenschutzorientierten VPNs im Bootstrap-Verfahren. In den Monaten 1 bis 6 wird organisch eine Basis an kostenlosen Nutzer*innen aufgebaut. Im 7. Monat wird ein Teil der kostenlosen Nutzer*innen zu zahlenden Abonnent*innenen konvertieren. Die Arbeitsleistung der Gründer*innen wird als Verbindlichkeit zurückgestellt, bis sie durch Einnahmen finanziert werden kann. Das Modell zielt auf die vollständige Bezahlung der Arbeitenden, die Rückzahlung der Gründerschulden und eine positive Cash-Akkumulation über einen Zeitraum von 7 Jahren ab. Mit Hilfe von Jonas Herzer von VDI/VDE prüften wir die zugrundeliegende Annahmen und die Ergebnisse.
- Im Rahmen unserer Geschäftsmodellierung haben wir auf Grundlage der Wachstumsprognosen einen Marketingetat berechnet und eine initiale Marketingstrategie entwickelt, die Printmedien und Onlinewerbung beinhaltet.
- Wir entwickelten eine Landing Page für Coop VPN: https://coopvpn.net./. Die Seite befindet sich derzeit noch in einer Betaversion, enthält aber schon die grundlegenden Bausteine. Interessierte erfahren von Coop VPN, dem Produktversprechen und den möglichen Zahlungsmodellen, können sich über unsere Datenschutz- und Open Source Grundsätze informieren und eine Preview für das Artwork von Roger Peet erhalten.
- Als letzten Coach lernten wir Elizabeth Baird kennen, die uns von Superbloom vermittelt wurde. Sie beriet uns zu B2B Verträgen, ein Thema, das gegen Ende der Förderzeit durch intensiveren Austausch mit /e/OS für uns deutlich an Wichtigkeit gewann.

Wir schrieben einen Beitrag für den Prototype Fund Blog, „From Tech Sovereignity to Tech Solidarity“, in dem wir über unsere Intentionen und Hoffnungen bei der Gründung eines sicheren und solidarischen VPNs in der Hand der Mitarbeitenden reflektieren. Der Beitrag wird nach Prüfung durch den Prototype Fund veröffenlicht.

Zielgruppe, Nutzen und mögliche Weiterentwicklungen

Welche Maßnahmen zur Zielgruppen/Community-Ansprache und -Gewinnung wurden in unternommen? Welcher Nutzen ergibt sich für die Zielgruppe aus den Ergebnissen Deines Projekts? Welche weitergehenden Effekte ergeben sich aus der Open-Source-Stellung der Ergebnisse? Gibt es Ideen für die Weiterentwicklung Deiner Lösung und Pläne zu deren Umsetzung?
Hat die Arbeit in dem Projekt Dich in Deiner persönlichen, fachlichen Weiterentwicklung unterstützt?

Das PTF Abschlussevent war der erste Schritt, um neue Leute anzusprechen, die Interesse haben, selbst einen VPN auf Basis von LEAP einzurichten und zu administrieren. Über Matrix-Gruppen zum Thema luden wir ein und konnten durch den Workshop nicht nur wertvolles Feedback sammeln, sondern auch Beitragende gewinnen, die nun ihrerseits selbst auf einem IT Camp den LEAP VPN Stack präsentieren und verbreiten. Wir hoffen, dass die Quelloffenheit des gesamten LEAP VPN Stacks, das Vertrauen in LEAP, u.a. aufgrund der Nähe zu Riseup und die nun deutlich vereinfachten Verfahren zum Aufsetzen und Administrieren neue Menschen überzeugen, selbst einen individualisierbaren VPN Dienst anzubieten. Wir glauben, dass dies eine resiliente Strategie ist, um möglichst vielen Menschen freien und sicheren Zugang zum unzensierten Internet zu ermöglichen.

Darüber hinaus befinden wir uns derzeit in Verhandlungen über einen B2B-Vertrag mit /e/OS und haben bereits eine gemeinsame Förderung dafür beantragt. Im Laufe des Projekts hat sich diese Beziehung von anfänglichem Interesse über die gemeinsame Ausarbeitung von Förderanträgen zu einer klaren gemeinsamen Initiative zur Einführung von LEAP VPN für /e/OS-Nutzer*innen entwickelt. Teil der Förderung wären mögliche Weiterentwicklungen wie u.a. die Integration eines entkoppelten und dadurch anonymen Bezahlsystems, Unterstützung von Post-Quanten-Kryptographie und die Integration des schnellen VPN-Protokolls Wireguard. Wir hoffen, über /e/OS viele Nutzer*innen zu erreichen und von unserem VPN Dienst und den zugrunde liegenden Werten zu überzeugen.

Wir alle haben uns im Laufe des Projekts fachlich deutlich weiterentwickelt. Insbesondere die eingehende Beschäftigung mit Terraform und K3S hat unsere Kenntnisse geschärft und das Repertoire erweitert. Dank der Second Stage Förderung konnten wir uns ausführlich betriebswirtschaftlichen Fragestellungen widmen, ein Thema das in unserem Softwareentwicklungsalltag oft zu wenig Beachtung gefunden hat. Die Beschäftigung mit Zukunftsplänen hat uns auch als Team zusammengeschweißt, da wir dazu gebracht wurden, unsere Kernwerte und Absichten aufzuschreiben, zu diskutieren und aufeinander abzustimmen.

Kurze Darstellung der Arbeiten, die zu keiner Lösung geführt haben

Gab es Arbeiten bzw. Lösungsansätze, die nicht weiter verfolgt wurden? Was waren die Hintergründe, und wie bist Du alternativ vorgegangen?

Wir planten anfangs, Interesse für Coop VPN über eine Mailingliste abzufragen, in die sich interessierte Nutzer*innen eintragen lassen können. Ziel war es, so das Interesse einschätzen zu können, bevor wir große Ausgaben für Serverinfrastruktur auf uns nehmen. Wir gaben diese Idee jedoch auf, da VPNs sehr bekannt sind und wir vermuten, dass potentielle Nutzer*innen den VPN lieber gleich ausprobieren wollen als sich für ein bekanntes Produkt auf eine Mailingliste setzen zu lassen. Wir entschieden uns, Nutzer*innen gleich das VPN für 6 Monate gratis testen zu lassen und zu hoffen, dass ein Teil der zufriedenen Nutzer*innen zu zahlenden Nutzer*innen werden.

Kurze Angabe von Präsentationsmöglichkeiten für mögliche Nutzer*innen

Wo können sich Interessent*innen detailliert über Deine Projektergebnisse informieren? Bitte Link zum Code (z. B. GitHub, GitLab etc.) sowie zur Code- bzw. technischen Dokumentation einfügen, ggf. auch Webseite oder weitere Links.

- Technische Dokumentation und Tutorials: https://docs.leap.se/
- Terraform Repositories für Hetzner und OVH:
  - https://0xacab.org/leap/container-platform/terraform-hetzner-k3s-vpn
  - https://0xacab.org/leap/container-platform/terraform-ovh-k3s-vpn
- LEAP Module in der Terraform Registry für Hetzner und OVH:
  - https://registry.terraform.io/modules/leapcode/k3s-vpn/hetzner/latest
  - https://registry.terraform.io/modules/leapcode/k3s-vpn/ovh/latest
- Helm Charts für LEAP Backend und Gateways:
  - https://0xacab.org/leap/container-platform/helm-backend
  - https://0xacab.org/leap/container-platform/helm-gateway
- Podlily zum einfachen Aufsetzen und Administrieren des gesamten LEAP VPN Stacks: https://0xacab.org/leap/container-platform/podlily
- Beta Landing Page für Coop VPN: https://coopvpn.net/
- LEAP Website: https://leap.se/

Kurze Erläuterung zur Einhaltung der Arbeits- und Kostenplanung

Gab es im Projektverlauf Ereignisse, die eine Anpassung der Planung erforderlich machten – z. B. Mehr- oder Minderaufwand bei der Bearbeitung von Teilaufgaben?

Wir konnten uns gut an die Arbeits- und Kostenplanung halten.

Kurze Darstellung von etwaigen Ergebnissen bei anderen Stellen

Gab es Entwicklungen anderer Personen oder Institutionen, die Einfluss auf Deine Arbeiten und die Zielsetzung hatten? Wenn ja, worin bestand dieser und wie bist Du damit umgegangen?

Im Projektverlauf zeigte sich, dass die gewählten Cloud-Provider den VPN-Dienst unterschiedlich gut unterstützen. Da OVH die Skalierbarkeit durch strenge Ressourcen-Limits einschränkt, den Datendurchsatz bei Geschwindigkeitstests drosselt und der

Support bis Förderungsende nicht oder nur langsam auf unsere Anfragen reagierte, sind wir auf andere Provider ausgewichen. Für Coop VPN nutzen wir deshalb u.a. FlokiNET. Weitere Deployments (z. B. bei Scaleway) sind in Planung.
Im Übrigen gab es keine nennenswerten Änderungen.