FunnelBridge – Technisch organisatorische Sicherheitsmaßnahmen zum Schutz der Kundendaten

Die Landschaft der Cybersicherheit ist ständig im Wandel und mit ihr die Methoden und Techniken, die von Angreifern verwendet werden, um an wertvolle Daten zu gelangen. Angesichts dieser dynamischen Bedrohungslage ist es für Unternehmen von entscheidender Bedeutung, nicht nur reaktiv, sondern proaktiv zu handeln. In diesem Kontext stellen wir bei Ruhr Solutions für unser SaaS Produkt FunnelBridge sicher, dass unsere Sicherheitsmaßnahmen nicht nur den aktuellen Anforderungen entsprechen, sondern auch zukünftigen Herausforderungen gewachsen sind.

Maßnahmen für die sichere Nutzung der FunnelBridge SaaS durch den Kunden:

- Authentifizierung ohne Passwort

Maßnahmen für den sicheren technischen Betrieb der FunnelBridge SaaS:

- Verschlüsselung von gespeicherten Daten (data at rest)
- Verschlüsselung von übertragenen Daten (data in transit)
- Private Networking
- Zero Trust Principle für Netzwerkverkehr
- Firewall
- DDos-Schutz
- Rate-Limiting
- Trennung von Entwicklungs- und Produktivumgebungen
- Protokollierung
- Monitoring
- Incident Management
- Wiederherstellbarkeit von Daten
- Disaster-Recovery Ablaufpläne
- API-Token Rotation alle 60 Tage
- Automatische Sicherheitsupdates
- Geschultes Personal

Maßnahmen in der Entwicklung der SaaS

- Schwachstellenmanagement
- Verhinderung von SQL-Injection, Cross Site Scripting, Cross Site Request Forgery

Maßnahmen in der Organisation Ruhr Solutions

- Single Sign On & 2-Factor-Authentication
- Verschlüsselte Festplatten der Mitarbeiter-Notebooks
- Verbot von USB-Sticks und externen Festplatten
- OneDrive for Business

Authentifizierung ohne Passwort

Die Web-Oberfläche von FunnelBridge ist durch einen Authentifizierungs-Mechanismus geschützt, der temporäre Verifizierungs-Codes per E-Mail sendet. Bei jedem Login-Versuch muss der Nutzer einen aktuellen Verifizierungs-Code eingeben. Somit müssen die FunnelBridge Kunden sich nicht um die sichere Speicherung ihres Passworts kümmern, da es keine Passwörter gibt.

Verschlüsselung von gespeicherten Daten (data at rest)

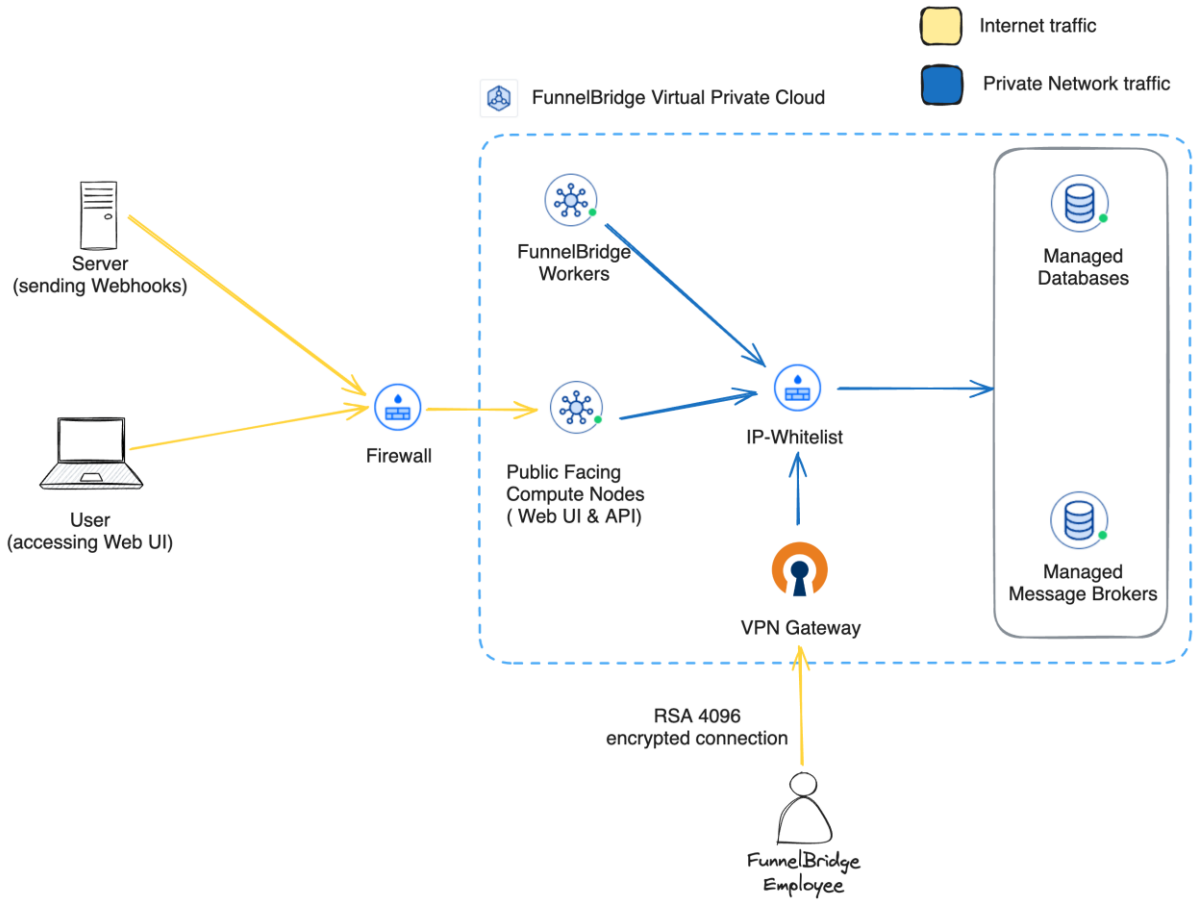
Alle Speicherorte, die für (personenbezogene) Kundendaten bei FunnelBridge verwendet werden, sind encrypted at rest:

- Sämtliche Festplatten von FunnelBridge Compute Instanzen sind per LUKS (Linux Unified Key Setup) verschlüsselt und somit vor unberechtigtem Hardware-Zugriff gesichert (Siehe DigitalOcean Volume Features)
- Dateiuploads von Nutzern werden in einem verschlüsselten Objekt-Speicher gesichert (Siehe DigitalOcean Spaces)
- Datenbanken sind per LUKS verschlüsselt (Siehe DigitalOcean Managed Databases)
- Backups werden in einem von Microsoft Azure verwalteten verschlüsselten Objekt-Speicher gespeichert (Siehe Azure Storage encryption for data at rest)

Verschlüsselung von übertragenen Daten (data in transit)

Für alle Datenübertragungen (sowohl über das Internet als auch im privaten Netzwerk) wird TLS 1.2 oder höher verwendet.

Private Networking



Datenbanken und Message Broker kommunizieren ausschließlich über ein privates Netzwerk mit anderen FunnelBridge Resourcen.

FunnelBridge Mitarbeiter erreichen Ressourcen innerhalb des privaten Netzwerks ausschließlich über eine gesicherte VPN-Verbindung.

Zero Trust Principle für Netzwerkverkehr

Es werden grundsätzlich alle Verbindungen zu Datenbanken blockiert, die nicht explizit gemäß der IP-Whitelist für berechtigte Compute Instanzen erlaubt sind.

Bei “Public facing Compute Nodes” werden grundsätzliche alle Verbindungen blockiert, die nicht über den Port 80 oder 443 geöffnet werden.

Firewall

Zur Durchsetzung der oben beschriebenen Regeln werden DigitalOcean Cloud Firewalls verwendet. Cloud Firewalls blockieren jeglichen Datenverkehr, der nicht ausdrücklich durch eine Regel zugelassen ist.

DDos-Schutz

Sämtliche öffentlich erreichbare Endpunkte sind auf Netzwerkebene mit einem DDos-Schutz geschützt.

Rate-Limiting

Auf Applikationsebene sind alle öffentlichen Endpunkte durch ein Rate-Limiting geschützt.

Trennung von Entwicklungs- und Produktivumgebungen

Die gesamte technische Infrastruktur wurde für Entwicklungszwecke repliziert. Änderungen am System werden ausführlich auf der Entwicklungsumgebung getestet, bevor sie auf die produktive Infrastruktur ausgerollt werden.

Protokollierung

- Ereignis-Protokolle sämtlicher Anwendungen werden zentral für einen Zeitraum von 30 Tagen gespeichert (siehe Grafana Promtail)
- Netzwerkzugriffe in das private Netzwerk werden auf unbegrenzte Zeit gespeichert (siehe OpenVPN Access Server Logging)

Monitoring

Alle relevanten technischen Komponenten werden automatisch alle 3 Minuten auf ihre Erreichbarkeit geprüft. Die Ergebnisse dieser “Health-Checks” werden automatisch auf https://status.funnelbridge.net/ veröffentlicht.

Darüber hinaus findet ein tägliches Monitoring der Systeme durch einen geschulten FunnelBridge Mitarbeiter statt. Es stehen mithilfe der Monitoring Software Grafana Dashboards bereit, um die folgenden Metriken zu prüfen:

- Ereignis-Protokolle sämtlicher Anwendungen
- Netzwerk-Auslastung im zeitlichen Verlauf (Ingress & Egress)

- CPU-Auslastung im zeitlichen Verlauf
- Arbeitsspeicher-Auslastung im zeitlichen Verlauf
- Ereignisse in der Orchestrierung der Container

Incident Management

Sollte sich in einem der Health-Checks ein Service als unerreichbar herausstellen, wird automatisch ein Entwickler per E-Mail und SMS benachrichtigt. Wenn der Entwickler nicht innerhalb von weiteren 3 Minuten im Incident Management System die Kenntnisnahme des Falls bestätigt, wird ein automatisches System den Entwickler per Anruf kontaktieren. Weitere Informationen: BetterStack Documentation

Wiederherstellbarkeit von Daten

Der gesamte Datenbestand kann per Point-in-time-Recovery (PITR) auf den Zustand einer beliebigen Uhrzeit innerhalb der letzten 7 Tage zurückgesetzt werden (Siehe DigitalOcean Managed Databases).

Um den möglichen Datenverlust bei einem Ausfall des Cloud Providers (DigitalOcean) zu begrenzen werden alle 24h vollständige Datenbank-Backups zu einem weiteren Cloud Provider (Microsoft Azure) transferiert.

Disaster Recovery Ablaufpläne

Die Disaster-Recovery-Strategie von FunnelBridge ist: Backup-Restore.

Da die gesamte technische Infrastruktur von FunnelBridge mithilfe von Infrastructure-as-Code Tools (Hauptsächlich Terraform) provisioniert wird, kann bei einem Totalausfall das gesamte System innerhalb von 2h wieder aufgebaut- und auf den Stand der letzten Datensicherung wiederhergestellt werden.

Dokumentationen für einen vollständigen Aufbau der gesamten Infrastruktur liegen intern vor.

Password Rotation

Sämtliche Passwörter und API-Tokens werden alle 60 Tage rotiert. Die Verantwortung hierfür liegt bei den Entwicklern. Um eine regelmäßige Rotation sicherzustellen, wurde firmenweit eine Regel aufgestellt, dass API-Token lediglich mit einer maximalen Gültigkeit von 90 Tagen ausgestellt werden dürfen.

Automatische Sicherheitsupdates

- Datenbank Softwareupdates werden vom Cloud Provider automatisch durchgeführt (Siehe DigitalOcean Managed Databases)
- Betriebssystem Updates werden vom Cloud Provider automatisch durchgeführt (Siehe DigitalOcean Kubernetes)
- Updates von Software Dependencies werden von den Entwicklern durchgeführt. Die Entwickler werden bei jedem Code-Commit durch eine Continous Integration Pipeline darüber benachrichtigt, ob Software Dependencies aufgrund von Sicherheitsbedenken aktualisiert werden müssen.

Geschultes Personal

Auf das produktive System haben nur Mitarbeiter mit der folgenden Zertifizierung Zugriff:

- AWS Certified Solutions Architect Associate

Schwachstellenmanagement

Sollte eine Software Dependency, die innerhalb der FunnelBridge SaaS verwendet wird, eine öffentlich bekannte Schwachstelle der Severety Stufe: HIGH oder schlimmer aufweisen, wird diese umgehend ausgetauscht oder auf eine höhere Version aktualisiert – sofern eine höhere Version die Sicherheitslücke schließt.

Die Prüfung auf Schwachstellen findet täglich im laufenden Entwicklungsbetrieb statt:
Weitere Informationen zum npm audit

Verhinderung von SQL-Injection, Cross-Site Scripting, Cross-Site-Request-Forgery

Zur Verhinderung von SQL-Injection, Cross-Site Scripting (XSS) und Cross-Site Request Forgery (CSRF) setzt Ruhr Solutions für die FunnelBridge SaaS auf den Einsatz von State-of-the-Art Libraries und Frameworks. Diese Bibliotheken sind speziell darauf ausgerichtet, bekannte Sicherheitslücken und Angriffsvektoren effektiv zu neutralisieren, indem sie robuste, vordefinierte Sicherheitsmechanismen und Validierungsverfahren implementieren. Durch die sorgfältige Auswahl und regelmäßige Aktualisierung dieser Tools gewährleisten wir, dass unsere Anwendungen von Anfang an mit den besten verfügbaren Schutzmaßnahmen ausgestattet sind.

Single-Sign-On und 2-Factor-Authentication

Jeder Ruhr Solutions Mitarbeiter verwendet für den überwiegenden Anteil der internen Anwendungen Microsoft Entra ID, um sich zu authentifizieren. Sollte eine Anwendung nicht über das Signle-Sign-On von Entra ID verwendet werden (z. B. das CRM System), ist die Aktivierung von 2-Factor-Authentication in diesen Anwendungen verpflichtend.

Verschlüsselte Festplatten der Mitarbeiter-Notebooks

Sämtliche Festplatten der Mitarbeiter-Notebooks (es werden ausschließlich MacBooks verwendet) sind mit FileVault verschlüsselt.

Verbot von USB-Sticks und externen Festplatten

Es ist unternehmensweit untersagt, USB-Sticks oder externe Festplatten für die Speicherung von Daten zu verwenden

OneDrive for Business

Ruhr Solutions nutzt OneDrive for Business als zentrale Plattform für die sichere Speicherung und gemeinsame Nutzung von Dokumenten innerhalb unseres Unternehmens. Diese Lösung fördert die Zusammenarbeit und Effizienz, indem sie unseren Mitarbeitern ermöglicht, auf wichtige Dateien zuzugreifen und diese zu bearbeiten, unter strikter Einhaltung von Datenschutz- und Sicherheitsstandards.

Haftungsausschluss: Dieses Dokument soll dem Leser einen allgemeinen Überblick über die Sicherheitsmaßnahmen geben, die Ruhr Solutions in Bezug auf sein SaaS Produkt FunnelBridge ergriffen hat. Einige Unterscheidungen oder Nuancen können übersehen werden. Bitte wenden Sie sich für spezifischere und/oder aktuellere Informationen an hallo@ruhrsolutions.com.