Security by Design

Delegator

Klassifizierung	intern
Status	in Arbeit
Programmname	Delegator
Projektnummer	1
Projektleiter	Tabinas Kenan
Version	0.1
Datum	26. März 2025
Auftraggeber	Tabinas Kenan
Autor/Autoren	Tabinas Kenan
Verteiler	

Änderungsverzeichnis

Version	Datum	Änderung	Autor
0.1	26.03.2025	Erstellung	Kenan Tabinas
0.2	16.04.2025	Rollenkonzept hinzugefügt	Kenan Tabinas

Tabelle 1: Änderungsverzeichnis

1 Prinzip

Folgende Entscheidung halfen bei der Sicherstellung von Sicherheitsrelevanten Features.

1.1 Grundprinzip

Ganz nach dem Motto «Sicherheit noch vor der ersten Code-Zeile» sind während jedem Schritt die Sicherheitsrelevanten Parameter beachtet worden.

Folgende 3 Grundprinzipen wurden beachtet:

«Angriffe erwarten: Security by Design fusst auf der Annahme, dass Cyber-Angriffe, Sicherheitslücken und Benutzerfehler erfolgen. Deshalb gilt es, deren Auswirkungen zu minimieren.

Security by Obscurity vermeiden: In der Praxis und in Studien haben sich offene Codes gegen geschlossene durchgesetzt: Leaks, Unfälle und Reverse Engineering gehören zur Realität. Deshalb haben sich Offenheit und Transparenz als sicherer erwiesen als die sogenannte Security by Obscurity, bei der die Codes geheim bleiben sollen.

Privilegien einschränken: Das Prinzip der eingeschränkten Privilegien (principle of least privilege, PoLP) basiert darauf, Benutzenden, Prozessen und Programmen nur Zugriff auf die Informationen und Ressourcen zu gewähren, die für ihre Arbeit unbedingt erforderlich sind.»[1]

[1] https://www.nexusgroup.com/de/security-by-design

2 Zero Trust Architektur

Im Rahmen der Möglichkeiten des Projekts orientiert sich die Architektur an Zero Trust Architektur. Nach dem Motto «Nein zu implizitem Vertrauen». Jeder Zugriff, jede Verbindung und jede Kommunikation muss authentifiziert, autorisiert und verschlüsselt erfolgen. Im Folgenden ist eine Liste mit den Prinzipen welche berücksichtig wurden.

Prinzip	Beschreibung
Cloudflare Tunnel	Schliessen aller Ports
Endpoint Authentication	Jeder Knoten muss sich Authentisieren. (mutual TLS, API Keys, usw.)
Least Privilege Access	Minimale Berechtigungen für jeden User und Serivce

Tabelle 2: Zero Trust

2.1 Darstellung

Es folgt eine Darstellung der Kommunikationswege innerhalb der Umgebung.

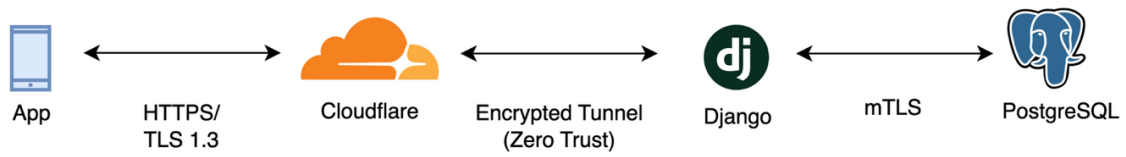

Abbildung 1: Zero Trust

2.2 Massnahnen Dokumentation

Zero Trust schreibt auch vor jeden Layer der Verbindung muss Dokumentiert werden.

Layer	Massnahmen
APP	Certificate Pinning (via Middleware) Flutter Secure Storage (via Middleware) Input Validation (via Regex)
Cloudflared	DDoS Protection (automatisch) Bot Management (automatisch) Rate Limiting (automatisch)
Django	CSRF Protection (via Middleware) SQL Injection Prevention (via Django ORM) Secure Cookie (via Middleware)
PostgresSQL	Field-level encryption (für z.B. Passwörter) Service User mit Least Privilege

Tabelle 3: Zero Trust Massnahmen

3 Stride

“STRIDE ist ein Modell von Sicherheitsrisiken. STRIDE unterscheidet folgende 6 Kategorien an Sicherheitsrisiken»[2]

Buchstabe	Beschreibung	Beispiel
S	Spoofing	Email Spoofing, IP Spoofing
T	Tampering	Man-in-the-middle, Database Tampering (Ändern von Fremden Daten)
R	Repudiation	Steht für «Abstreitbarkeit». Wenn ich z.B einen «Einbruch» nicht beweisen kann durch z.B: Fehlende Audit Logs
I	Information Disclosure	SQL Injection, Directory aufliesten, Banner grabbing,
D	Denial of Service	DDoS-Angriff, Resource Exhaustion
E	Elevation of Privilege	Token Manipulation, Buffer Overflow

Tabelle 4: Stride Auflistung

[2] https://de.wikipedia.org/wiki/STRIDE

3.1 Stride Analyse

	Bezug zum Projekt Delegator	Gegenmassnahmen
S	Stehlen von Credentials oder Tokens. Durch unsichere Verbindung oder fehlende Validierung	MFA Tokens mit kurzer Lebensdauer Risk-based Authentifizierung
T	Manipulation von fremden Aufgaben, Projekten oder Kalenderdaten Durch unsichere Endpoints oder direkten Datenbank zugriffen	Inter-Container-Verschlüsselung Zugriffskontrolle Least Privilege CSRF-Schutz SQL-ORM
R	Ohne Log sind Manipulationen nicht beweisbar	Logging mit zentralisiertem Logsystem (z. B. ELK Stack) SIEM-System (z. B. Wazuh)
I	Offenlegung sensibler Nutzerdaten Durch unsichere Endpoints oder unsichere Verbindungen	Zero Trust Tunnel (Cloudflare) HTTPS zwang Field-Level-Verschlüsselung in PostgreSQL Secure Cookies
D	Cloud-Service oder App ist nicht mehr erreichbar Durch Sperrung oder eigenes Versäumnis.	Cloudflare DDoS-Schutz Rate Limiting Redundanz Befolgen von Store Richtlinien
E	Ein regulärer Nutzer könnte unerlaubte Aktionen ausführen. Durch unsichere Endpoints.	Rollenbasiertes Zugriffssystem Keine Container auf Root Secrets Management Zero Trust auf API-Ebene

Tabelle 5: Stride Analyse

4 Rollenkonzept

Hier folgen die Berechtigungen welche die User erhalten.

ID	Rolle	Automatischer Zugriff
1	Admin	Alles
2	Long-Term member	Projekte, Verträge, Geld, User Verwaltung
3	Member	Projekte
4	Familie	Kalender Sychronisation
5	Fans	Zugriff auf öffentliche Kalender
6	Externer	Keine (Mixer*in, Videograph*in, Fotograph*in.)

Tabelle 6: Rollenkonzept

4.1 Berechtigungsmatrix

Endpoint	Read	Create	Update	Delete
users	Dein eigener User. User deiner Org	Ja	Nur dein eigener User	Nur dein eigner User
organisations	Via user-organisation	Nur als Premium User	Eigene Org durch user-organisation	Via user-organisation
roles	Alle	x	x	x
user-organisations	Eigene Org durch user-organisation	Als Admin von Org. Automatisch bei erstellung von Org.	Als Admin von Org	Als Admin von Org
calendars	Via Projects oder Personelle calender via user_id	Automatisch bei erstellung von Projekten	x	Automatisch bei löschen von Projekten. Automatisch bei entfernung von Mitgliedern
events	Via Kalender	Via Kalender	Via Kalender	Via Kalender
projects	Via Org. Via user-projects	Via org. (Min-Role: 3)	Via Org. Via user-projects	Via Org. Via user-projects
chats	Via Org. Via Projekte.	Via org. (Min-Role: 3)		Automatisch bei löschen von Projekten.
chat-users	Via Chat	Via Chat	Via Chat	Via Chat
messages	Via Chat	Via Chat	Via Chat. Via User (eigene)	Via Chat. Via User (eigene)
songs	Via org. (Min-Role: 3)	Via org. (Min-Role: 3)	Via org. (Min-Role: 3)	Via org. (Min-Role: 3)

Tabelle 7: Berechtigungsmatrix 1

Endpoint	Read	Create	Update	Delete
timetables	Via org. (Min-Role: 3). Via Projekt.	Via org. (Min-Role: 3). Via Projekt.	Via org. (Min-Role: 3). Via Projekt.	Via org. (Min-Role: 3). Via Projekt.
setlists	Via org. (Min-Role: 3). Via Projekt.	Via org. (Min-Role: 3). Via Projekt.	Via org. (Min-Role: 3). Via Projekt.	Via org. (Min-Role: 3). Via Projekt.
history	Via org. (Min-Role: 3)	Automatisch	x	x
statuses	Alle	x	x	x
tasks	Via org. (Min-Role: 4). Via Projekt.	Via org. (Min-Role: 3). Via Projekt.	Via org. (Min-Role: 3). Via Projekt.	Via org. (Min-Role: 3). Via Projekt.
recordings	Via org. (Min-Role: 3). Via Projekt.	Via org. (Min-Role: 3). Via Projekt.	Via org. (Min-Role: 3). Via Projekt.	Nur dein eigner User
user-projects	Via org. (Min-Role: 3).Via eigener User	Via org. (Min-Role: 3)	Via org. (Min-Role: 3)	Via org. (Min-Role: 3)

Tabelle 8: Berechtigungsmatrix 2

5 Backup und Restore

5.1 GFK

Auch beim Wechsel auf einen Managed Service, darf ein Backup and Restore Konzept nicht fehlen. Wieso wird später erklärt. Das (GFK) Grand-Father-Son Backup Prinzip hat überzeugt. Es gibt jedoch kein Zeitraum vor. Hier wird jetzt 7-4-12 dargestellt.

Woche	Mo	Di	Mo	Do	Fr	Sa	So
1							
2							
3							
4							

Tabelle 9: GFK Darstellung

Farbe	Backup Intervall
	Nach 24h wird ein Backup erstellt. Tägliches Backup mit 7-Tage-Retention.
	Nach 7 Tagen wird ein Wochen Backup erstellt. Wochen Backup mit 4-Wochen-Retention.
	Nach 4 Wochen wir der Monat Backup erstellt. Monats Backup mit 12-Monats-Retention.

Tabelle 10: GFK-Legende

5.2 Backup 3-2-1-1-0

Die bekannte 3-2-1 wurde durch weitere Ziffern ergänzt. Das System sieht folgendes vor. Dabei gibt 3-2-1 nicht vor in welcher Frequenz Backups gemacht werden sollten. Sondern auf Was und wo sie gespeichert werden soll.

5.2.1 3-2-1-1-0 Erklärung

Ziffer	Erklärung
3	Dieselbe Information sollte dreimal Existieren. Einmal Live und z.B. zweimal als Backup. Man kann bei hoch Sensiblen Daten auch eine Datenbank Replikation erstellen.
2	Backups sollten auf Verschiedenen Medien gespeichert werden.
1	Ein Backup muss an einem anderen Orten sein. Nur einem Cloud-Provider vertrauen verstösst gegen diesen Punkt.
1	Ein Backup muss offline und nicht beschreibar sein
0	Keine Fehler bei Wiederherstellung. Dies erfordert regelmässige Tests.

Tabelle 11: 3-2-1-1-0

5.3 Parameter

Damit wir die Frequenz bestimmen können orientieren wir uns an bestimmen «Kennzahlen». [3]

5.3.1 Parameter Erklärung

Abkürzung	Parameter	Erklärung
RPO	Recovery Point Objective.	Zeit Abstand zwischen Backups
RTO	Recovery Time Objective.	Zeit vom Incident bis zum Rollback
WRT	Work Recovery Time	Zeitraum vom Rollback bis Freigabe
MTD	Maximum Tolerable Downtime	Maximal erlaubter Zeitraum zwischen Incident und Freigabe

Tabelle 12: Parameter Erklärung

[3] https://www.cms.gov/tra/Infrastructure_Services/IS_0410_DR_Capability_Considerations.htm

5.3.2 RTO-Vergleichswerte

Diese Zeiträume definieren ist noch schwer. Es folgen Wert aus der Praxis als vergleich. Laut darwinsdata.com sehen die RTO Werte so aus.[4]

Branche	From (h)	To (h)
Finanz	1	4
E-commerce	1	24
Gesundheit	1	72
Produktion	24	48
Einzelhandel	24	72
Bund	24	72

Tabelle 13: RTO-Vergleichswerte

5.3.3 Tiers und Dynamische Backups

Selbst bei der Bank, erhalten nicht alle Daten dieselbe RTO. Zahlungen dürfen nach Bank Richtlinen wie z.B: SEC nur eine minimale Downtime haben. Hingegen Administrative Daten, für die Bank selbst, sind nicht so streng.

Eine Variante wäre es auch, Backups nicht nur nach einer gewissen Zeit zu machen, sondern auch nach Datenfluss. So wird werden bei einem Peak, auch häufiger Backups gemacht.

5.3.4 Parameter

Offlinesynchronisierung kommt definitiv auf den Plan. Es reduziert den Backup kosten massiv. Die Faustregel ist «halbe so lange ist doppelt so teuer.»

Abkürzung	Zeitraum (h)	Begründung
RPO	2-4	4 Stunden sind tolerierbar.
RTO	4-8	Als Ein-Mann-Unternehmen ist kürzer unrealistisch
WRT	8-12	So ein drittel bis einen halben Tag kann man Warten
MTD	24	Mehr als ein ganzer Tag ist zu lang

Tabelle 14: Delegator Parameter

[4] https://darwinsdata.com/what-is-industry-standard-rpo-rto/

6 Fazit

6.1 Security Controls

Basierend auf den Prinzipen, der Stride Analyse und der Zero Trust Architektur ergaben sich folgende 8 Security Controls. Diese kommen jeweils mit konkreten planen zur Umsetzung.

Security Controls	Geplante Umsetzung
Angriffsfläche minimieren	Cloudflared Zero Trust Tunnel ermöglicht Verbindung, ohne einen einzigen Port zu öffnen. Zugriff auf Server ist nur im privaten LAN erreichbar. (Zero Trust) Regelmässiges Container Image scanning
Verschlüsselung	Cloudflared Zero Trust Tunnel und eigenem Trusted CA zu Cloudflare Inter-Container Verschlüsselung mit z.B. Isito Backup Verschlüsslung
Authentifizierung	MFA für Logins Tokens mit kurzer Lebensdauer Automatisches Session Timeout Risk-based Auth (Standort-Anomalien, Gräte Profiling) z.B. loginradius API Access Rate limiting
Least Privilege	Keine Passwörter Secrets Management Container laufen nie auf Root. Zugriffe werden grundsätzlich abgelehnt.
Getrennte Systeme	Container Trennen die Kommunikation via VLAN
Monitoring	Zentralisiertes Log mit z.B: ELK Stack Security Information and Event Management (SIEM) z.B: Wazuh
Incident Reponse	Incident Reponse Framework erstellen und daraus konkrete Playbooks als Prozess ableiten
Compliance	Externer Penntest ins Budget einfliessen lassen Jährliche Audits

Tabelle 15: Security Controls

6.2 Backup Plan

Kombinieren wir das Wissen aus den vorgängigen Konzepten und Prinzipen ergibt sich folgender Backup Plan.

6.2.1 GFK-Strategie

Kind: 4h mit 24h Retention

Vater: 1 Tag mit 7 Tag Retention

Grossvater: 1 Woche mit 4 Wochen Retention

Tag	0	4	8	12	16	20
1						
2						
3						
4						
5						
6						
7						

Tabelle 16: GFK Strategie

6.2.2 3-2-1-1-0 Strategie

Ziffer	Strategie
3	1. Exoscale DBaaS 2 Exoscale backup service 3 Export zu Scaleway
2	1 Exoscale Cloudstorage 2 Scaleway Objectstorage
1	1 Backup bei Scaleway (Frankreich) (0.1752€ pro GB pro Jahr)
1	1 Raspi mit Script (Physical Air gapped Backup)
0	0 Fehler durch Test siehe mehr bei Disaster Recovery

Tabelle 17: 3-2-1-1-0 Strategie

6.2.3 Disaster Recovery Plan

Je nach Regulatorium muss es mehr oder weniger häufig getestet werden. 3 Monaten, 6 Monate und 12 Monaten sind mögliche Zeiträume. Es bietet sich jedoch an, vor grossen Updates ein Recovery Test durchzuführen.

Halbjährlich scheint vernünftig zu sein.

6.2.4 3-2-1-1-0 Zeitplan

Aus all diesen Informationen ergibt isch folgender Zeitplan.

Strategie	Zeitplan
1. Exoscale DBaaS 2 Exoscale backup service 3 Export zu Objectstorage	- 04h 24h
1 Exoscale Cloudstorage 2 Scaleway Objectstorage	04h 24h
1 Backup bei Scaleway	24h
1 Raspi mit Script	4 Tage
Disaster Recovery Plan	6 Monate

Tabelle 18: 3-2-1-1-0 Zeitplan

6.2.5 Wachstum

Was kostet dieser spass? Das hängt stark vom Speicherplatz ab. Nehmen wir an pro Monat ein GB erreicht die Aktuelle Menge User. Wenn wir uns das Wachstum anschauen werden Ende 2tes Jahr die 3 Fache Menge Daten sein.

Im ersten Jahr. Bei 12 GB und somit 204 GB Back Up Storage.

Scaleway (Frankreich) (0.1752€ pro GB pro Jahr)

Exoscale Backup Service (0.2409€ pro GB pro Jahr)

Bei 1€ = 0.94 CHF

Jahr	Storage (GB)	Scaleway (GB)	Exoscale (GB)	Kosten (CHF)
1	12	48	156	43
2	36	144	468	130
3	72	288	936	259
4	120	480	1560	432
5	180	720	2340	648
6	252	1008	3276	908
7	336	1344	4368	1210
8	432	1728	5616	1556
9	540	2160	7020	1945
10	660	2640	8580	2378

Tabelle 19

Abkürzungen und Glossar

Abkürzung / Fachwort	Erläuterung
API	Application Programming Interface
CSRF	Cross-Site Request Forgery
DDoS	Distributed Denial of Service
ELK	Elasticsearch, Logstash, Kibana (Stack)
GFK	Grossvater-Vater-Sohn (Backup-Prinzip)
HTTPS	Hypertext Transfer Protocol Secure
MFA	Multi-Factor Authentication
MTD	Maximum Tolerable Downtime
ORM	Object-Relational Mapping
PoLP	Principle of Least Privilege
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SEC	Securities and Exchange Commission
SIEM	Security Information and Event Management
SQL	Structured Query Language
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
WRT	Work Recovery Time
3-2-1-1-0 Backup	Backup-Strategie: 3 Kopien, 2 verschiedene Medien, 1 offsite, 1 offline, 0 Fehler
Air Gapped Backup	Physisch getrennte Backup-Lösung ohne Netzwerkverbindung
API Keys	Eindeutige Identifikatoren für API-Zugriff
Banner Grabbing	Sammeln von Informationen über Services durch Systemantworten
Bot Management	Automatische Erkennung und Abwehr von Bots
Certificate Pinning	Festlegung spezifischer Zertifikate für sichere Verbindungen
Cloudflare Tunnel	Sichere Verbindung ohne offene Ports
Container Image Scanning	Automatische Überprüfung von Container-Images auf Schwachstellen

Abkürzung / Fachwort	Erläuterung
Directory Listing	Unerlaubte Auflistung von Verzeichnisinhalten
Disaster Recovery	Wiederherstellungsplan nach Systemausfall
Field-Level Encryption	Verschlüsselung auf Datenfeldebene
Flutter Secure Storage	Sichere Datenspeicherung in Flutter-Apps
Incident Response	Reaktion auf Sicherheitsvorfälle
Input Validation	Überprüfung von Eingabedaten
Inter-Container Verschlüsselung	Verschlüsselung zwischen Containern
Least Privilege	Minimale Berechtigungen für Benutzer und Services
Man-in-the-Middle	Angriff durch Abfangen der Kommunikation
Mutual TLS	Gegenseitige TLS-Authentifizierung
Penetration Test	Sicherheitstest durch simulierte Angriffe
Rate Limiting	Begrenzung der Anfragerate
Resource Exhaustion	Erschöpfung von Systemressourcen
Risk-based Authentication	Risikobasierte Authentifizierung
Secrets Management	Verwaltung von Passwörtern und Schlüsseln

Tabelle 20: Abkürzungen und Glossar

Glossar erstellt bei Claude. Begriffe und Beschreibungen.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis