Security Dashboard Configuration Guide

Manuelle Sicherheitseinstellungen im Supabase Dashboard

Diese Einstellungen können nicht über Migrations vorgenommen werden und müssen manuell im Supabase Dashboard konfiguriert werden.

📍 Supabase Project URL

```
https://supabase.com/dashboard/project/gzczjscctgyxjyodhnhk
```

---

1. ⏱️ OTP Expiry Time Reduzieren

Problem: Die OTP-Ablaufzeit ist zu lang (Standard: 1 Stunde), was ein Sicherheitsrisiko darstellt.

Empfohlene Einstellung: 5-10 Minuten

Schritte:
1. Gehe zu **Authentication → Providers → Email**
2. Scrolle zu **Email OTP Expiration**
3. Setze den Wert auf `300` Sekunden (5 Minuten)
4. Klicke **Save**

---

2. 🔐 Leaked Password Protection Aktivieren

Problem: Benutzer können Passwörter verwenden, die in bekannten Datenlecks vorkommen.

Empfohlene Einstellung: Aktiviert

Schritte:
1. Gehe zu **Authentication → Providers → Email**
2. Finde **Compromised Password Protection**
3. Aktiviere die Option
4. Klicke **Save**

Alternative (HaveIBeenPwned Integration):
1. Gehe zu **Authentication → Hooks**
2. Erstelle einen Pre-Sign-Up Hook mit HIBP API Check

---

3. 📊 Postgres Version Upgrade

Problem: Eine ältere Postgres-Version kann Sicherheitslücken haben.

Empfohlene Version: PostgreSQL 15 oder höher

Schritte:
1. Gehe zu **Settings** → **Infrastructure**
2. Prüfe die aktuelle Postgres-Version
3. Falls ein Upgrade verfügbar ist:
- Erstelle ein **Backup** (Settings → Backups)
- Klicke auf **Upgrade Postgres**
- Wähle die neueste stabile Version
- Bestätige das Upgrade

⚠️ **Wichtig:**
- Plane das Upgrade außerhalb der Hauptnutzungszeiten
- Teste vorher in einer Staging-Umgebung
- Ein Upgrade kann 10-30 Minuten Downtime verursachen

---

4. 🔌 Extensions in separates Schema verschieben

Problem: Extensions im `public` Schema können Sicherheitsrisiken darstellen.

Empfohlene Lösung: Extensions in `extensions` Schema verschieben

Schritte (SQL Editor):

```
-- 1. Schema erstellen
CREATE SCHEMA IF NOT EXISTS extensions;

-- 2. Grants setzen
GRANT USAGE ON SCHEMA extensions TO postgres, anon, authenticated, service_role;

-- 3. Extension verschieben (Beispiel für pgvector)
-- ACHTUNG: Dies erfordert DROP und RECREATE!
-- DROP EXTENSION IF EXISTS vector CASCADE;
-- CREATE EXTENSION vector WITH SCHEMA extensions;

-- 4. Search path anpassen
ALTER DATABASE postgres SET search_path TO public, extensions;
```

⚠️ **Wichtig:**
- Backup vor dem Verschieben erstellen
- Alle abhängigen Objekte müssen angepasst werden
- In Production nur mit Wartungsfenster durchführen

---

5. 📧 Email Rate Limiting

Problem: Kein Rate Limiting für Auth-E-Mails kann zu Spam führen.

Empfohlene Einstellung: 4 E-Mails pro Stunde

Schritte:
1. Gehe zu **Authentication** → **Rate Limits**

2. Setze **Email send rate limit** auf `4`
3. Setze **SMS send rate limit** auf `4` (falls SMS aktiv)
4. Klicke **Save**

---

6. 🔒 MFA Konfiguration

Empfohlene Einstellung: MFA für Admin-Benutzer erzwingen

Schritte:
1. Gehe zu **Authentication → MFA**
2. Aktiviere **TOTP (Time-based One-Time Password)**
3. Optional: Aktiviere **Phone (SMS)**
4. Klicke **Save**

---

7. 🌐 CORS Einstellungen

Problem: Zu offene CORS-Einstellungen können Cross-Site-Angriffe ermöglichen.

Empfohlene Einstellung: Nur erlaubte Domains

Schritte:
1. Gehe zu **Settings → API**
2. Unter **Allowed Origins**, füge nur deine Domains hinzu:
- `https://getleanai.app`
- `https://www.getleanai.app`
- `http://localhost:3000` (nur für Development)
3. Entferne `*` (Wildcard) falls vorhanden
4. Klicke **Save**

Checkliste nach Migration

- [ ] OTP Expiry auf 5 Minuten gesetzt
- [ ] Leaked Password Protection aktiviert
- [ ] Postgres Version geprüft/aktualisiert
- [ ] Extensions-Schema erstellt
- [ ] Email Rate Limiting konfiguriert
- [ ] CORS nur für erlaubte Domains
- [ ] MFA für Admins aktiviert
- [ ] Backup vor großen Änderungen erstellt

Monitoring aktivieren

1. **Security Alerts:**
   - Gehe zu **Settings → Notifications**
   - Aktiviere E-Mail-Benachrichtigungen für Security Events

2. **Log Drain (optional):**
   - Gehe zu **Settings → Log Drains**
   - Verbinde mit Datadog/Logflare für erweiterte Überwachung

---

Support

Bei Fragen zur Implementierung:
- Supabase Docs: https://supabase.com/docs/guides/auth/security
- Discord: https://discord.supabase.com

Erstellt: 22. Januar 2026
Letzte Aktualisierung: 22. Januar 2026