

🔊 LUISTER DIT VERSLAG

-10%

1,0x

+10%

+25%

1,0x

↓ Download naar telefoon

Soort: vergadering · **Duur:** onbekend · **Deelnemers:** [Speaker 1] [Speaker 2]

Let op — sprekers niet bevestigd. Plaud nummert sprekers (Speaker 1, 2, ...) maar koppelt geen namen. Ga niet uit van wie wat zei; "ik/wij" hoeft niet dezelfde persoon te zijn.

[Vergaderinformatie]

Datum: 2026-05-18 09:08:04

Locatie: [Voeg locatie in]

Deelnemers: [Speaker 1] [Speaker 2]

[Vergadernotities]

Titel: Veilige omgang met API-sleutels en omgevingsvariabelen

Beschrijving:

Probleem: herhaalde "Secrets Exposure"-meldingen bij deploys op Supabase/Render en stressvolle sleutelrotaties.

Kernprincipe: nooit hardcoden; beheer geheimen via omgevingsvariabelen.

Lokaal: gebruik een .env-bestand; voeg .env toe aan .gitignore vóór de eerste commit.

Cloud: configureer Secrets/Environment Variables in het dashboard (Render, Supabase).

Frontend vs backend: Supabase Anon-key is publiceerbaar; krachtige sleutels (service role, cloud-API) blijven geheim.

Conclusie:

Proactief beheer met omgevingsvariabelen in plaats van reactief optreden is essentieel.

Titel: Praktische workflow bij Render en Supabase

Beschrijving:

Workflow: push code naar GitHub zonder .env; stel Environment Variables in bij Render; app leest via process.env/deno.env.

Supabase Edge Functions: beheer via Supabase Secrets Set.

Supabase Vault: voor databasegeheimen (pg-sodium), te gebruiken in functies/RLS.

Conclusie:

Consistente, gescheiden opslag van geheimen per omgeving en platform.

Titel: Zero-downtime sleutelrotatie en secret managers

Beschrijving:

Dual/overlapping key-strategie: voeg een nieuwe sleutel toe en behoud de oude; code probeert eerst de nieuwe, valt terug op de oude; trek de oude pas in na migratie.

Tools: centrale secret managers zoals HashiCorp Vault en Doppler; bieden auditing, versiebeheer en geautomatiseerde rotatie.

Supabase: verbeterde API voor directe rotatie en meerdere herroepbare sleutels.

Conclusie:

Met dual-key en centrale vaults kan rotatie zonder downtime plaatsvinden.

Titel: Veelvoorkomende valkuilen en mitigaties

Beschrijving:

Valkuil: per ongeluk .env committen of tijdelijk hardcoden; GitHub detecteert en kan sleutels intrekken (vangnet, geen vervanging).

Valkuil: inconsistentie tussen omgevingen; ontbrekende variabelen veroorzaken fouten.

Mitigatie: automatiseer via scripts/laC (Terraform) en secret managers; voer standaardprocessen in.

Conclusie:

Automatiseer en standaardiseer om menselijke fouten te beperken.

Titel: Samenvatting en kernlessen

Beschrijving:

Hardcode nooit geheimen; gebruik omgevingsvariabelen.

Lokaal .env en .gitignore; in de cloud Secrets/Environment Variables.

Professioneel beheer: dual-key rotatie; overweeg een centrale secret manager; Supabase Vault voor databasegeheimen.

Conclusie:

Een duidelijk, disciplinair beveiligingsplan reduceert lekken en stress.

[Volgende afspraken]

Huiswerk: kies één bestaand project en refactor één hardgecodeerde API-sleutel naar een omgevingsvariabele (lokaal en in productie).

Controleer .gitignore om zeker te zijn dat .env-bestanden worden uitgesloten.

Configureer Secrets/Environment Variables in Render of Supabase voor het gekozen project.

Documenteer een dual-key rotatieprocedure voor toekomstige sleutelwijzigingen en test een oefenrotatie.

Evalueer het gebruik van een centrale secret manager (bijv. HashiCorp Vault of Doppler) voor meerdere services/teams; definieer criteria, eigenaar en tijdlijn.

Voer een policy-audit uit voor RLS en voeg tests toe om frontend-publicatie van de Supabase Anon-key veilig te bevestigen.

Introduceer IaC/scripting om variabelen cross-omgeving te synchroniseren.

Definieer monitoring/alerts bij sleutelintrekking door GitHub/Supabase, plus notificatiekanalen en herstelplan.

[AI-voorstellen]

AI-voorstellen

AI heeft de volgende punten geïdentificeerd die niet zijn afgerond of waar geen duidelijke actie op staat; let hierop:

Er is geen expliciete planning of verantwoordelijke voor het implementeren van een centrale secret manager; bepaal criteria, eigenaar en tijdlijn.

Procedures voor rotatie (dual-key) zijn niet vastgelegd in code of runbooks; documenteer stappen en test een oefenrotatie.

Omgevingsconsistentie is genoemd maar niet geautomatiseerd; introduceer IaC/scripting om variabelen cross-omgeving te synchroniseren.

Monitoring/alerts bij sleutelintrekking door GitHub/Supabase ontbreken; definieer notificatiekanalen en herstelplan.

Frontend-publicatie van de Supabase Anon-key vereist bevestigde RLS-polices; voer een policy-audit uit en voeg tests toe.