CodeIQ Beveiligingsprogramma & Software

Beveiligingspraktijken & standaarden om klantgegevens en projectintegriteit te beschermen.

Anti-virus / Malwarebeleid

Apparaten die verbonden zijn met het netwerk worden routinematig gecontroleerd en onderhouden om te zorgen voor bescherming tegen virussen en malware. Anti-virussoftware is geïnstalleerd op alle werkstations en apparaten om een veilige werkomgeving te garanderen voor alle teamleden.

Gevoelige informatie

Klantgegevens worden veilig opgeslagen op productie-servers, waarbij de toegang beperkt is tot uitsluitend aangewezen medewerkers. Back-ups worden beheerd in beveiligde omgevingen met beperkte toegang, zoals voorgeschreven door de platformvereisten. Op verzoek kan data worden versleuteld om gevoelige informatie extra te beschermen. Klantgegevens en gevoelige informatie die op papier worden bewaard, worden versnipperd voordat ze worden weggegooid om de vertrouwelijkheid te waarborgen.

Toegangscontrole

Alleen teamleden die direct betrokken zijn bij een project hebben toegang tot de productieomgeving ervan. De toegang wordt onmiddellijk ingetrokken bij beëindiging van het dienstverband of na voltooiing van het project, om de veiligheid van gegevens te waarborgen.

Technologie

Software & Frameworks

Alleen teamleden die direct betrokken zijn bij een project hebben toegang tot de productieomgeving. Toegang wordt snel ingetrokken bij beëindiging van het dienstverband of project.

- **Laravel:** Ingebouwde functies voor versleuteling, authenticatie en gegevensbescherming.
- **Shopify:** Voor e-commerce oplossingen en webshops.

Beveiligingsupdates worden uitgevoerd als er een beveiligingscontract is afgesloten met de klant. Anders kunnen updates op verzoek of tegen een uurtarief worden uitgevoerd.

Hosting Provider

Onze virtuele servers worden gehost door 4AllBusiness Telecom BV en beheerd via Ploi.io. Alle servers zijn uitsluitend toegankelijk via SSH-sleutels, zonder toegang op basis van wachtwoorden. Wij bieden geen gedeelde hosting; alle servers worden privé beheerd en beveiligd met tweefactorauthenticatie (2FA).

Beveiligingscomponenten voor Laravel-projecten

1. **Veilige Communicatie – HTTPS**
   Voor alle projecten vragen wij SSL-certificaten aan om veilige verbindingen tussen server en client te waarborgen.
2. **SSH Access - Private Keys**
   SSH-toegang tot productie-servers wordt beheerd via privésleutels, beveiligd met wachtwoorden en alleen verstrekt aan een beperkt aantal ontwikkelaars.
3. **Wachtwoord Hashing – Bcrypt met Unieke Salt**
   Gebruikerswachtwoorden worden éénrichtings gehasht met unieke salts, zodat ze niet omgekeerd kunnen worden.
4. **Versleuteling van Gevoelige Data – AES Versleuteling**
   Gevoelige data kan versleuteld worden met AES-versleuteling; de versleutelingssleutel wordt veilig buiten de webomgeving en versiebeheer opgeslagen.

5. **Voorkomen van SQL-injectie – Geparameteriseerde Queries**
   Laravel's ORM maakt gebruik van geparameteriseerde queries om SQL-injecties te voorkomen.
6. **XSS Protection - Safe Output by Default**
   Veilige sjablonen zoals Twig of Blade worden gebruikt om XSS-aanvallen te voorkomen, waarbij variabelen standaard worden geëscaped.
7. **CSRF-bescherming**
   Een CSRF-token wordt gegenereerd voor elke sessie en is vereist voor alle POST/PUT/DELETE-verzoeken om Cross-Site Request Forgery te voorkomen.
8. **Authenticatie en Autorisatie**
   Laravel's ingebouwde authenticatiefuncties beschermen gebruikersgegevens en beperken de toegang tot specifieke routes op basis van inlogstatus en gebruikersrollen.
9. **Validatie**
   Laravel's validatietools verwerken gebruikersinvoer veilig, waarbij controle wordt uitgevoerd op vereiste bestandsindelingen en unieke rijen.
10. **Configuratievariabelen**
    Gevoelige configuratiedetails worden opgeslagen in een .env-bestand, ontoegankelijk vanuit versiebeheer en de webomgeving, en zijn alleen beschikbaar op de productie-server.

Versiebeheer en Back-ups

Applicatiecode wordt beheerd in een Git-repository zonder gevoelige informatie of databasewachtwoorden. Back-ups van essentiële gegevens worden bewaard in beveiligde omgevingen met beperkte toegang.