Beveiliging PraxCloud

Praxtour realiseert zich dat met de App (PraxCloud) oplossing een goede bescherming van persoonsgegevens (AVG) van essentieel belang is. Hieronder volgt de opsomming van de beschermingsmaatregelen van het PraxCloud platform.

Huidige beveiliging:

1. De algehele PraxCloud bevat een SSL certificaat van www.praxcloud.eu . Dat wil zeggen dat alle data via een versleutelde verbinding gaan. Het gaat om de volgende technieken: TLS 1.3, X25519, en AES_256_GCM. Dit certificaat is uitgegeven door Xolphin aan Praxtour BV.

2. Daarnaast is het Web beheer met CORS ingesteld op de API (data interface) met een CSRF token, dat wil zeggen dat er naast het web beheer niemand van buiten PraxCloud data verzoeken kan sturen.

3. Na authenticatie van een gebruiker, via de app of web beheer zal er aan ieder verzoek naar de server een unieke code worden toegewezen die bij diens account hoort. Deze is 16 karakters lang en bevat willekeurige karakters. Dit zit in een aparte http header. Zo wordt het zelfs met kennis van het platform adres erg lastig om alsnog bij de data te komen.

4. De database zit verborgen in een geïsoleerde omgeving in een virtual machine op het Digital Ocean platform. Deze wordt dan ook intern aangesproken en kan geen connecties van buitenaf toestaan. Hiervoor is de API laag eromheen gebouwd.

5. De code van de web beheer die via de browser is in te zien, minimaliseren, generaliseren en obfusceren we om de potentiele hacker het lastig te maken om inzicht te krijgen in de processen van de dataverzoeken naar en van het platform.

Toekomstige (uitbreiding) beveiliging:

1. Naast Gebruikersnaam en Wachtwoord is het zo dat na authenticatie van een Gebruikersnaam en Wachtwoord om in te loggen in de web beheer omgeving er later nog een Google Authenticator zal worden geplaatst voor MFA (Multi Factor Authentication). Dit levert een extra beveiliging op in het platform.

2. Mochten er berichten via het platform gestuurd gaan worden, dan zal hiervoor blockchain voor gebruikt gaan worden voor extra beveiliging.

Data obfuscatie
In het kader van de AVG en het ook als IT-afdeling niet mogen inzien van persoonlijke data het volgende:
Mocht data obfuscatie* van bijvoorbeeld het emailadres vanuit de instelling (klant) gewenst zijn, dan zullen we dat realiseren. We zullen dit opnemen in de contractvoorwaarden, zodat de klant hiermee akkoord kan gaan. Hiermee kan support geleverd worden waarbij het mailadres als communicatie voor het systeem gebruikt wordt om bijv. ‘wachtwoord vergeten’- functionaliteit in te bouwen.

Praxtour zal met haar PraxCloud platform voldoende veiligheid bieden om een goede weerstand te bieden tegen hackers. Uiteraard zal Praxtour er alles aan doen om in de toekomst te streven naar een goede beveiliging omtrent de data.

*Data obfuscatie is het versleutelen van gegevens die alleen door de eigenaar van de gegevens in te zien zijn.