Doc. naam : **Beveiliging Oxygis**

Versie : 18/06/2025

Samenvatting : Uw veiligheid is erg belangrijk voor ons! Hier is een samenvatting van wat we elke dag doen om ervoor te zorgen dat uw gegevens veilig zijn bij Oxygis en dat we de beste beveiligingsprocedures toepassen op onze gehoste versie, de Oxygis Cloud.

1 - Oxygis Cloud (Oxygis-cloudinfrastructuur)

I.Back-ups / noodherstel

- Wekelijkse back-ups 1 jaar bewaard
- Back-ups worden opgeslagen op Microsoft Azure
- Back-ups worden gerepliceerd in ten minste 3 verschillende datacenters in een beschikbaarheidszone in West-Europa. Op verzoek kunnen automatische replicaties worden gemaakt in andere beschikbaarheidszones (dit kan extra kosten met zich meebrengen, die worden doorberekend aan de Klant).
- Je kunt contact opnemen met onze helpdesk om een van deze back-ups terug te zetten naar je actieve database (of naar de zijkant).
- De daadwerkelijke locaties van onze datacenters staan vermeld in ons ***Privacybeleid***.
- **Hardware failover:** er worden geen diensten direct op baremetal gehost, maar alleen op virtuele servers of managed services van Microsoft Azure of Amazon Web Services.
- **Rampherstel: in** het geval van een complete ramp, waarbij een datacenter *voor langere tijd volledig buiten gebruik is,* waardoor failover naar onze lokale hot-standby niet mogelijk is (dit is tot nu toe nog nooit gebeurd, het is het ergste scenario), hebben we de volgende doelstellingen:
    - **RPO** (Recovery Point Objective) = 24 uur. Dit betekent dat je maximaal 24 uur werk kunt verliezen als de gegevens niet kunnen worden hersteld en we je laatste dagelijkse back-up moeten terugzetten.
    - **RTO** (Recovery Time Objective) = 24 uur voor betaalde abonnementen, 48 uur voor gratis proefabonnementen, educatieve aanbiedingen, freemium gebruikers, enz. Dit is de tijd die nodig is om de service in een ander datacenter te herstellen als zich een ramp voordoet en één datacenter volledig buiten gebruik is.
    - Hoe het werkt: we bewaken onze dagelijkse back-ups actief en ze worden gerepliceerd naar meerdere datacenters binnen een beschikbaarheidszone. We hebben een geautomatiseerd provisioningsysteem om onze services op een nieuwe hostingsite te implementeren. De restore van gegevens op basis van onze back-ups van de vorige dag kan dan worden uitgevoerd in een kwestie van uren (voor de grootste clusters).

Partners SRL
België : Eikelenbergstraat, 20, 1700 Dilbeek - België- Tel: +32 (0)2 736 10 17 - BTW : BE 0872.350.989
Frankrijk : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - BTW: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

II.Databasebeveiliging

- Klantgegevens kunnen worden opgeslagen in een speciale database - geen gegevensuitwisseling tussen klanten.

III.Wachtwoordbeveiliging

- Wachtwoorden van klanten worden beschermd door PBKDF2+SHA512-codering volgens de industriestandaard (salted + uitgerekt voor duizenden beurten).
- De medewerkers van Oxygis hebben geen toegang tot uw wachtwoord en kunnen het niet voor u achterhalen. De enige optie als u het kwijt bent, is om het opnieuw in te stellen.
- Inloggegevens worden altijd veilig verzonden via HTTPS.
- Wachtwoordbeleid: wachtwoorden moeten minstens 10 tekens lang zijn en minstens één hoofdletter, één kleine letter, één cijfer en één speciaal teken bevatten.

IV.Toegang personeel

- De supportmedewerkers van Oxygis kunnen inloggen op uw account om toegang te krijgen tot de instellingen die betrekking hebben op uw supportprobleem. Hiervoor gebruiken ze hun eigen inloggegevens, niet uw wachtwoord (dat ze op geen enkele manier kunnen weten).
- Deze speciale toegang voor medewerkers verbetert de efficiëntie en veiligheid: ze kunnen elk probleem dat je tegenkomt meteen reproduceren, je hoeft nooit je wachtwoord te delen en we kunnen de acties van medewerkers afzonderlijk controleren en monitoren!
- Onze helpdeskmedewerkers doen hun uiterste best om je privacy te respecteren en hebben alleen toegang tot de bestanden en parameters die nodig zijn om je probleem te diagnosticeren en op te lossen.

V.Fysieke beveiliging

Oxygis Cloud servers worden gehost op Microsoft Azure, er is geen fysieke toegang mogelijk.

VI.Communicatie

- Alle datacommunicatie naar Client-instanties wordt beschermd door de allernieuwste 256-bit SSL (HTTPS) encryptie.

2 - Oxygis (de software)

I.Software beveiliging

Oxygis is gecodeerd in C# voor de backend en AngularJS voor de frontend.

De R&D-processen van Oxygis omvatten codebeoordelingsfasen die de beveiligingsaspecten van zowel nieuwe als bestaande code-elementen omvatten.

II.Veiligheid door ontwerp

Oxygis is ontworpen om de introductie van de meest voorkomende beveiligingslekken te voorkomen:

- SQL-injecties worden voorkomen door een API op een hoger niveau te gebruiken waarvoor geen handmatige SQL-query's nodig zijn.
- XSS-aanvallen worden voorkomen door het gebruik van een high-level modelleringssysteem dat automatisch geïnjecteerde gegevens escapeert.

Zie ook de sectie **OWASP Top Kwetsbaarheden** om te zien hoe Oxygis vanaf het begin is ontworpen om dergelijke kwetsbaarheden te voorkomen.

III.OWASP's top kwetsbaarheden

Hier is het standpunt van Oxygis over de belangrijkste beveiligingskwesties voor webtoepassingen, zoals opgesomd door het **Open Web Application Security Project** (OWASP):

- **Kwetsbaarheden door injectie:** Kwetsbaarheden door injectie, vooral SQL-injectie, komen vaak voor in webtoepassingen. Injectie treedt op wanneer door de gebruiker verstrekte gegevens naar een interpreter worden gestuurd als onderdeel van een opdracht of query. De vijandige gegevens van de aanvaller zorgen ervoor dat de interpreter ongewenste opdrachten uitvoert of gegevens wijzigt.

  Oxygis gebruikt een ORM dat de constructie van queries abstraheert en SQL-injecties voorkomt. Ontwikkelaars construeren SQL-query's normaal gesproken niet handmatig, deze worden gegenereerd door het ORM, en parameters worden altijd correct geëscaped.

- **Cross Site Scripting (XSS):** XSS-fouten doen zich voor wanneer een toepassing door de gebruiker ingevoerde gegevens naar een webbrowser stuurt zonder deze inhoud eerst te valideren of te coderen. XSS stelt aanvallers in staat om scripts uit te voeren in de browser van het slachtoffer, wat gebruikerssessies kan kapen, websites kan beschadigen, mogelijk wormen kan introduceren, enz.

Partners SRL
België : Eikelenbergstraat, 20, 1700 Dilbeek - België- Tel: +32 (0)2 736 10 17 - BTW : BE 0872.350.989
Frankrijk : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - BTW: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

Oxygis escapet alle gegevens, wat XSS voorkomt.

- **Cross Site Request Forgery (CSRF):** Een CSRF-aanval dwingt de browser van een verbonden slachtoffer om een vals HTTP-verzoek, inclusief de sessiecookie van het slachtoffer en andere automatisch opgenomen verificatiegegevens, naar een kwetsbare webtoepassing te sturen. Hierdoor kan de aanvaller de browser van het slachtoffer dwingen om verzoeken te genereren waarvan de kwetsbare applicatie denkt dat het legitieme verzoeken van het slachtoffer zijn.

  Oxygis bevat een geïntegreerd CSRF-beschermingsmechanisme. Het voorkomt dat een HTTP-controller een verzoek ontvangt zonder het bijbehorende beveiligingstoken. Dit is de aanbevolen techniek voor CSRF-preventie.

- **Kwaadaardige bestandsuitvoering:** Code die kwetsbaar is voor remote file inclusion (RFI) stelt aanvallers in staat om vijandige code en gegevens op te nemen, wat leidt tot verwoestende aanvallen, zoals het volledig compromitteren van een server.

  Oxygis biedt geen functies voor het opnemen van bestanden op afstand.

- **Onveilige directe objectverwijzing:** Een directe objectverwijzing treedt op wanneer een ontwikkelaar een verwijzing naar een intern implementatieobject blootlegt, zoals een bestand, map, databaserecord of sleutel, in de vorm van een URL of formulierparameter. Aanvallers kunnen deze verwijzingen manipuleren om ongeautoriseerde toegang tot andere objecten te krijgen.

  Toegangscontrole tot Oxygis is niet geïmplementeerd op het niveau van de gebruikersinterface, dus er is geen risico op het blootleggen van verwijzingen naar interne objecten in URLs. Aanvallers kunnen de toegangscontrolelaag niet omzeilen door deze referenties te manipuleren, omdat elk verzoek altijd door de validatielaag voor gegevenstoegang moet.

- **Onveilige cryptografische opslag:** Webapplicaties maken zelden op de juiste manier gebruik van cryptografische functies om gegevens en referenties te beschermen. Aanvallers gebruiken zwak beveiligde gegevens om identiteitsdiefstal en andere misdaden, zoals creditcardfraude, te plegen.

  Oxygis gebruikt een standaard veilige hash voor gebruikerswachtwoorden (standaard PKFDB2 + SHA-512, met key stretching) om opgeslagen wachtwoorden te beschermen. Het is ook mogelijk om externe authenticatiesystemen te gebruiken om te voorkomen dat gebruikerswachtwoorden lokaal worden opgeslagen.

- **Onveilige communicatie :** Applicaties slagen er vaak niet in om netwerkverkeer te versleutelen wanneer het nodig is om gevoelige communicatie te beschermen.

  Oxygis werkt met HTTPS.

Partners SRL
België : Eikelenbergstraat, 20, 1700 Dilbeek - België- Tel: +32 (0)2 736 10 17 - BTW : BE 0872.350.989
Frankrijk : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - BTW: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

- **Gebrek aan URL-toegangsbeperking:** Vaak beschermt een applicatie gevoelige functionaliteit alleen door te voorkomen dat links of URL's worden weergegeven aan onbevoegde gebruikers. Aanvallers kunnen deze zwakke plek gebruiken om toegang te krijgen en ongeautoriseerde bewerkingen uit te voeren door deze URL's direct te openen.

  De toegangscontrole van Oxygis is niet geïmplementeerd op het niveau van de gebruikersinterface en de beveiliging is niet afhankelijk van het verbergen van speciale URLs. Aanvallers kunnen de toegangscontrolelaag niet omzeilen door een URL te hergebruiken of te manipuleren, omdat elk verzoek door de validatielaag voor gegevenstoegang moet. In de zeldzame gevallen waarin een URL niet-geauthenticeerde toegang biedt tot gevoelige gegevens, zoals de speciale URL's die klanten gebruiken om een bestelling te bevestigen, worden deze URL's digitaal ondertekend met unieke tokens en alleen per e-mail verzonden naar de beoogde ontvanger.

IV.Kwetsbaarheden in de beveiliging melden

Als u een beveiligingskwetsbaarheid wilt melden, meld dit dan zo snel mogelijk aan onze Helpdesk. Deze meldingen worden met de hoogste prioriteit behandeld, het probleem wordt onmiddellijk beoordeeld en opgelost door het Oxygis-beveiligingsteam, in samenwerking met de melder, en vervolgens op verantwoorde wijze bekendgemaakt aan de klanten en gebruikers van Oxygis.

Update en contact

Dit document wordt regelmatig bijgewerkt om ontwikkelingen in onze veiligheidspraktijken weer te geven. Als je vragen hebt of meer wilt weten, neem dan contact met ons op via info@oxygis.eu.

Gerelateerde documenten

- Privacybeleid
- Beleid verantwoordelijke informatie
- Service Level Agreement (SLA)
- Abonnementsovereenkomst

Aanvullende informatie over veiligheid

De cloudinfrastructuur die Oxygis gebruikt, is gebaseerd op Microsoft Azure-datacenters die ISO 27001 en SOC 2 gecertificeerd zijn en voldoen aan de beveiligingsstandaarden van de sector. Toegang tot productieomgevingen is strikt beperkt tot geautoriseerde leden van het technische team, die allemaal onder een interne vertrouwelijkheidsovereenkomst vallen. Toegangslogboeken worden bewaard voor analyse in het geval van een incident.

Partners SRL
België : Eikelenbergstraat, 20, 1700 Dilbeek - België- Tel: +32 (0)2 736 10 17 - BTW : BE 0872.350.989
Frankrijk : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - BTW: FR 13 811593730
www.oxygis.eu - info@oxygis.eu

Veiligheidstests

Oxygis voert regelmatig beveiligingstests uit, waaronder geautomatiseerde kwetsbaarheidsscans op zijn productieomgevingen, om minimale blootstelling aan bekende risico's te garanderen.

Authenticatie en toegangsbeheer

Oxygis adviseert het gebruik van sterke wachtwoorden en twee-factor authenticatie (2FA) voor toegang tot zijn platforms, indien beschikbaar. Gebruikersrollen maken een nauwkeurig beheer van toegangsrechten tot functies en gegevens mogelijk.

Partners SRL
België : Eikelenbergstraat, 20, 1700 Dilbeek - België- Tel: +32 (0)2 736 10 17 - BTW : BE 0872.350.989
Frankrijk : 130, Boulevard de la Liberté - 59800 Lille - Tel : +33 (0)3 20 13 79 44 - SIREN: 811593730 - BTW: FR 13 811593730
www.oxygis.eu - info@oxygis.eu