VISMA | visionplanner

Cloud security

Visionplanner gaat zeer zorgvuldig om met uw gegevens. Om dit te realiseren hebben we gekozen voor het veilige Microsoft Windows Azure platform. Door middel van dit Cloud platform bieden wij onze software aan onze partners en hun klanten.
Daarbij zijn beveiligingsmaatregelen geïmplementeerd op verschillende niveaus:

Datacenter **Database** **Applicatie** **Toegang tot klantdata** **Auditing**

Data-center beveiliging

Windows Azure wordt uitgevoerd in datacenters die door Microsoft Azure Global Infrastructure worden beheerd en geëxploiteerd. Deze geografisch verspreide datacenters voldoen aan de belangrijkste industrienormen voor beveiliging en betrouwbaarheid, zoals ISO/IEC 27001:2005. Ze worden beheerd en bewaakt door Microsoft-personeel dat jarenlange ervaring heeft met het 24 uur per dag, zeven dagen per week leveren van de grootste online services ter wereld.

Het datacenter van Microsoft wat wij gebruiken staat in de regio West Europa en heeft:

- Fysieke beveiliging
- Bescherming tegen DDOS aanvallen
- Uitwijkmogelijkheden

Naast het beveiligingsbeleid voor datacenters, netwerken en personeel gelden er voor Windows Azure diverse beveiligingsregels op de toepassings- en platform niveaus voor een nog uitgebreidere beveiliging voor ontwikkelaars van toepassingen en service beheerders.

Een totaaloverzicht van de beveiligingen op het Azure platform

Lees je hier

Toegang door Visionplanner employees naar de Azure datacenters is beschermd door middel van VPN access.

Database Beveiliging

Data opslag beveiliging
De database van Visionplanner waarin alle cijfers, dossiers en configuraties zijn opgeslagen, is 3-voudig gerepliceerd, waardoor de kans op fysieke corruptie nagenoeg nihil is. Alle wijzigingen worden continue opgeslagen in een back-up. Bij calamiteiten kan Visionplanner tot 30 dagen alle wijzigingen van alle kantoren ongedaan maken.
Dit is alleen voor echte calamiteiten, dit mechaniek kan niet gebruikt worden voor individuele kantoren of dossiers.
Om disaster recovery te ondersteunen wordt er een schaduw database bijgehouden in een andere regio. Deze database kan in noodgevallen gebruikt worden om een uitwijk omgeving op te zetten waarmee de kantoren en gebruikers weer verder kunnen.

Toegang
Binnen Visionplanner kunnen slechts enkele medewerkers de database beheren.
Het is voor kantoorgebruikers en ondernemers niet mogelijk om data te benaderen van andere kantoren dan die waarvoor de gebruiker is aangemeld en geautoriseerd.

Applicatiebeveiliging

De verbinding tussen de applicatieservers en de Internetbrowser van de gebruiker wordt versleuteld via een crypto-sleutel en met behulp van een SSL-certificaat (Class 3 EV SSL-certificaat). Visionplanner heeft onder meer de volgende security maatregelen ingebouwd:

- Alle communicatie tussen de Internetbrowser en de server is encrypted (256-bits) en de beveiligde SSL/TLS1.2 verbinding is door Symantec (voorheen Verisign) gecertificeerd (Class 3 EV SSL-certificaat). Al het verkeer met de webservice is beveiligd en wordt in een HTTPS-omgeving afgehandeld. Inloggen en werken in Visionplanner kan alleen met een beveiligde verbinding.

- Voor het aanmelden biedt Visionplanner meerdere opties:

    0 Bestaande login/passwords (wordt begin 2022 uitgefaseerd)
    0 Azure AD B2C local accounts
    0 De eigen Kantoor Authenticatie kan gebruikt worden. Hierbij bepaald het Kantoor zelf het niveau van beveiliging en door middel van SSO worden de “credentials” gebruikt binnen Visionplanner. Als Multi Factor Authentication (MFA) standaard is voor het kantoor, dan zal dit mechaniek ook worden gebruikt bij de toegang tot Visionplanner Cloud. De volgende opties worden ondersteund:

        * Microsoft Business accounts (Azure AD based)
        * Google accounts
        * Visma Connect accounts
        * Eigen IDP gebaseerd op OpenID (Azure AD B2C, Okta)

- Voor de door Visionplanner beheerde accounts geldt:

    0 Voor de In de aanmeldpagina is ‘brute force protection’ ingebouwd, zodat wachtwoorden niet oneindig geprobeerd kunnen worden.
    0 Alleen ‘sterke’ wachtwoorden zijn toegestaan.
    0 Wachtwoorden worden nooit op het scherm getoond, worden nooit vanaf de server aan de internet browser doorgegeven en worden nooit per e-mail verzonden.
    0 Alleen de gebruiker zelf kan zijn eigen wachtwoord instellen. Medewerkers van Visionplanner of applicatiebeheerders bij de klant kunnen dit niet voor anderen doen.

- Als een aangemelde gebruiker 20 minuten niet actief is met Visionplanner Cloud, wordt de Visionplanner Cloud sessie geblokkeerd en moet de gebruiker zich opnieuw authenticeren.

- Visionplanner Cloud is beveiligd tegen en getest op OWASP beveiligingsrisico's zoals Cross Site Scripting, SQL-injection, Insecure Direct Object References, Cross-Site Request Forgery (CSRF).

- Data van cliënten van een accountantskantoor is alleen toegankelijk voor medewerkers die aan dat kantoor gekoppeld. Medewerkers zijn altijd verbonden aan maximaal een kantoor.

Toegang tot klantdata

Visionplanner wordt ontwikkeld in een OTAP-omgeving (Ontwikkeling, Test, Acceptatie, Productie) met strikte scheiding van applicatiecode en data voor deze verschillende fasen. Ontwikkel- en testomgevingen hebben geen toegang tot de data van de productie-omgeving.

Een beperkt aantal ontwikkelaars heeft toegang tot de database van de productie-omgeving voor onderhoud en het oplossen van storingen. Als medewerkers problemen moeten oplossen naar aanleiding van een melding, dan is de standaard procedure dat deze medewerker door een beheerder van het kantoor wordt uitgenodigd in de kantooromgeving.
De medewerker zal proberen het probleem op te lossen. Als dit niet lukt wordt de oorzaak van het probleem geanalyseerd en wordt het betreffende probleem gereproduceerd op een van de development omgevingen en daar vervolgens opgelost. Als deze aanpak ook niet lukt, dan wordt er gebruik gemaakt van de database toegang van enkele ontwikkelaars en wordt er in de database gekeken of daar de oorzaak kan worden gevonden.
Als laatste redmiddel wordt er door de ontwikkelaar een debug-sessie opgezet met de betreffende administratie Algemeen gesteld, medewerkers van Visionplanner hebben geen toegang tot de data van cliënten, tenzij een Visionplanner medewerker expliciet in de medewerkerslijst van het kantoor wordt opgenomen.

Het is belangrijk dat deze toevoeging ongedaan wordt gemaakt als het incident afgehandeld is. Hiervan ligt de verantwoordelijkheid bij de betreffende beheerder van het kantoor. Deze accounts worden na 31 dagen (als niet gebruikt zijn), automatisch uitgezet. Visionplanner employees zullen nooit om inlog credentials van gebruikers vragen.

Auditing

Visionplanner logt het inloggen en aanmelden bij een administratie daarnaast ook al de web service aanroepen die naar de server komen. Deze informatie wordt gebruikt om problemen te detecteren. Daarbij worden geen cijfers gelogd die inzage in de financiële situatie van de klant zouden kunnen geven.

Periodiek worden onze interne procedures, applicatie kwaliteit en security maatregelen door een externe partij geaudit om te borgen dat onze applicatie nog voldoet aan de meest recente beveiligingseisen. De Visionplanner Cloud software wordt minimaal een keer per jaar getest om mogelijke penetratie gebreken te vinden en op te lossen. Dit wordt door het Visma Security team uitgevoerd.

Daarnaast nemen we deel aan het Visma Security programma, dit betekent dat Visionplanner moet voldoen aan de volgende zaken:

- Penetratietest (MAVA)
- Source code scanning op security problemen
- Dependency validatie op mogelijk gebruik van niet betrouwbare componenten
- Security Assessment waarbij veel details geanalyseerd worden. De security van de software en alle gerelateerde zaken worden aangescherpt onder begeleiding van het Visma Security team (https://www.visma.com/trust-centre/). Visma heeft veel expertise op het gebied van applicatie beveiliging. Deze expertise wordt gebruikt om de beveiliging van alle Visma producten te borgen en op een hoger niveau te krijgen.

Availability

Visionplanner monitort de “uptime” en “downtime” over een rollend jaar waarbij twee KPI’s worden berekend, namelijk de “uptime” gemeten over 24/7 en de “uptime” gemeten gedurende kantooruren.

- 24 uur / 7 dagen: uptime is > 99.9 %

- 9 uur / 5 werkdagen (ma-vr) is > 99.9 %

VISMA | visionplanner