perflectie
Mastering Change

Beveiligingsbeleid

Online platform Perflectie

2018

Beveiligingsbeleid Perflectie

Versiebeheer

Naam	Functie	Datum	Versie
Dimitri Tholen	Software Architect	12 december 2014	1.0
Dimitri Tholen	Software Architect	10 februari 2015	1.1
Dimitri Tholen	Software Architect	18 februari 2015	1.2
Serge Bekenkamp	Lead developer	2 januari 2017	1.3
Sander ten Kate	Partner	17 april 2018	1.4

1. Introductie

Binnen Perflectie wordt zeer veel waarde gehecht aan de bescherming van persoonsgegevens. Dit uit zich in de naleving van de privacy wet- en regelgeving. Naast deze vastgestelde regels hanteert de IT- en Ontwikkelafdeling een set eigen procedures om de veiligheid van de persoonsgegevens en de stabiliteit van de applicatie te waarborgen.

2. Technische documentatie

Ter ondersteuning van de ontwikkeling van Perflectie wordt er gebruik gemaakt van diverse technische documenten, zoals bijvoorbeeld schema's, diagrammen en 'wireframes'.

Deze documenten worden beschikbaar gesteld aan de ontwikkelaars en het IT management via de dienst Google Drive en/of de Source Control server.

Technische documentatie bevat verder geen gevoelige informatie.

3. Server

Perflectie draait op een Virtual Private Server van TransIP. Het beheer van de server is in handen van de server administrator van Perflectie. Medewerkers van TransIP hebben geen toegang tot de operationele zijde van Perflectie.

Perflectie behoudt het recht om medewerkers van TransIP toegang tot de server te verlenen indien zij dit nodig acht vanuit een technische behoefte.

3.1 Programmatuur

De server draait op Windows Server 2012 met uiterst geringe features. Vrijwel alle programmatuur is onderdeel van het Microsoft server platform, zoals Internet Information Manager en Server Manager.

3.2 Updates

De server wordt automatisch voorzien van de laatste updates.

3.3 Datacentrum

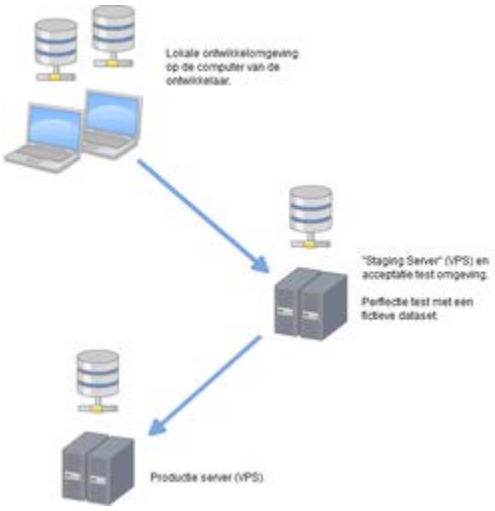
Het datacentrum is in handen van The Datacenter Group te Amsterdam. Het datacentrum heeft 24/7 on-site bewaking, biometrische identificatie en een HD CCTV netwerk. Het datacentrum is ISO 9001, ISO 27001 en ISO 14001 gecertificeerd. Daarmee zijn kwaliteitsmanagement, beveiliging en milieumanagement optimaal gewaarborgd.

3.4 Toegankelijkheid

Bij Perflectie vinden wij de privacy van onze gebruikers erg belangrijk. We hebben daarom verschillende maatregelen genomen om de toegankelijkheid tot databases en servers te beperken. Het datacentrum is onbereikbaar voor onbevoegden. De server is via een Remote Desktop verbinding beperkt beschikbaar. Uitsluitend de lead developer heeft toegang tot de ongepseudonimseerde app server met schrijfrechten. Overige developers hebben slechts toegang tot gepseudonomiseerde databases. Zij hebben schrijfrechten op gepseudonimseerde databases. Analisten hebben slechts lees rechten tot gepseudonomiseerde databases.

4. OTAP

Perflectie maakt gebruik van de een Ontwikkel-, Test- en Productie omgeving. Elk van deze omgevingen draait op een aparte server.



5. Database

Perflectie maakt gebruik van een instantie van SQL Server 2012 Express. De database server wordt naast Perflectie ook gebruikt voor andere applicaties en/of doeleinden. Naast de Perflectie applicatie database host de server tevens de Perflectie error logging database.

5.1 Toegankelijkheid

De database server wordt beheerd door de server administrator. Naast de server administrator heeft de database administrator volledige toegang tot de database server. De ontwikkelaars van Perflectie hebben uitsluitend leesrechten op een gepseudonomiseerde productie database.

5.2 Back-up

Er wordt elke dag om 01:00 een back-up gemaakt van de productie database.

De back-ups worden veilig opgeslagen op één of meerdere externe dragers, zoals externe schijven en beveiligde Cloud Storage diensten.

Back-ups worden na 60 dagen na aanmaken automatisch verwijderd van de Cloud Storage dienst.

6. Applicatie

6.1 Logging

Perflectie hanteert een strict error logging beleid. De logs worden opgeslagen in een aparte SQL database. Het e-mailadres van de gebruiker die een error veroorzaakt wordt hierbij opgeslagen.

6.2 Encryptie

Perflectie maakt gebruik van de encryptie en hashing functionaliteit van het ontwikkelplatform.

Op het moment van schrijven bestaat het hashing algoritme uit een SHA1 versleutelde “key” welke is gegenereerd door een PBKDF2 functie.

Alle wachtwoorden worden versleuteld middels deze methode.

6.3 Foutafhandeling

Het ontwikkelteam doet er alles aan om fouten in de applicatie op te vangen en af te handelen. Mocht er toch onverhoopt een fout de eindgebruiker bereiken, dan treedt er een mechanisme in werking die de technische details van de desbetreffende fout verbergt.

Deze details zijn achteraf op te halen door ontwikkelaars van Perflectie.

6.4 Token

Perflectie maakt gebruik van cookies om gebruikers bij het inloggen te onthouden. Er wordt een cookie met authenticatie teruggestuurd wanneer een gebruiker succesvol inlogt met een e-mailadres en wachtwoord waaraan een gebruiker is gekoppeld. De cookie wordt voor 30 dagen opgeslagen in de browser. Na deze 30 dagen zal de gebruiker opnieuw moeten inloggen.

6.5 Authorizatie

De cookie in sectie 6.4 verwijst naar een sectie aan 'claims'. Perflectie maakt gebruik van een Claims-based Identity model. Een claim kan bijvoorbeeld een rol binnen Perflectie zijn.

6.6 Rollen

Een gebruiker van Perflectie krijgt op basis van zijn of haar rol toegang tot afgeschermde delen van de applicatie. Er worden geen rechten gekoppeld aan individuele gebruikers. Hiermee voorkomt Perflectie dat één gebruiker ongemerkt meer rechten ontvangt dan zijn of haar bevoegdheid voorschrijft.

7. Subverwerkers

Perflectie werkt uitsluitend met subverwerkers binnen de EER of, als zij niet binnen de EER vallen, met een Prviacy Shield certification.

Een compleet overzicht van subverwerkers en tot welke gegevens zij toegang hebben, is terug te vinden in de Privacy Verklaring van Perflectie.nl

8. Broncode

De broncode van Perflectie bestaat deels uit maatwerk en deels uit voorgeprogrammeerde code van het applicatie framework, welke de basis vormt van de Perflectie applicatie.

Perflectie maakt in de back-end gebruik van ASP.NET MVC en Web API van Microsoft.

8.1 Git

Perflectie maakt gebruik van een versiebeheer systeem genaamd Git. Git is een gedistribueerde versiebeheersysteem, waarbij – in tegenstelling tot andere versiebeheer systemen – niet slechts de wijzigingen worden gedownload van de server, maar juist een complete kopie van de broncode (de ‘repository’), inclusief alle wijzigingen van alle teamleden.

Op deze manier is de code altijd veilig, want bij het uitvallen van één systeem kan één van de andere systemen de distributie zonder dataverlies herstellen.

8.2 Cloud

De Git repository van Perflectie wordt gehuisvest door Github in de cloud.

8.3 Toegankelijkheid

De Git repository is alleen toegankelijk het IT-team van Perflectie. Er is per ontwikkelaar een account nodig met de bijbehorende lees- en schrijfrechten.

9. Continuïteitsplanning

Bij Perflectie beperken we de ‘downtime’ van het online platform. Er wordt uitsluitend gereleased op 'rustige' momenten, tenzij er vanwege een kritisch technisch mankement een hotfix gedaan moet worden.