**Beveiligingsbeleid TrainStation**

## 1. Introductie

Binnen TrainStation wordt zeer veel waarde gehecht aan de bescherming van persoonsgegevens. Dit uit zich in de conformering aan en naleving van de Wet bescherming persoonsgegevens (Wbp) en de Europese Algemene Verordening Gegevensbescherming (AVG). TrainStation is daarom ook de trotse eigenaar van een MYOBI Privacy Seal.
Naast deze vastgestelde regels hanteert de IT- en Ontwikkelafdeling van TrainStation een set eigen procedures om de veiligheid van de persoonsgegevens en de stabiliteit van de applicatie te waarborgen. Deze procedures zijn hieronder beschreven.

## 2. Technische documentatie

Ter ondersteuning van de ontwikkeling van TrainStation wordt er gebruik gemaakt van diverse technische documenten, zoals bijvoorbeeld schema's en diagrammen. Deze documenten worden beschikbaar gesteld aan de ontwikkelaars en het IT management via de dienst Google Drive. De technische documentatie bevat verder geen persoonsgevoelige informatie.

## 3. Server

TrainStation draait op een Virtual Private Server (VPS) van Pocos [1]. Het beheer van de server is in handen van TrainStation. Medewerkers van Pocos hebben geen toegang tot de operationele zijde van TrainStation.
TrainStation behoudt het recht om medewerkers van Pocos toegang tot de server te verlenen indien zij dit nodig acht vanuit een technische behoefte.

### *3.1 Programmatuur*

De server draait op een Linux besturingssysteem met Debian als distributie.

### *3.2 Updates*

De server wordt handmatig voorzien van de laatste updates.

### *3.3 Datacentrum*

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*

Het datacentrum is onbereikbaar voor onbevoegden. De server is via een SSH verbinding beschikbaar voor de medewerkers van de IT- en Ontwikkelafdeling van TrainStation.

## 4. OTAP

TrainStation maakt gebruik van de een Ontwikkel-, Test-, Acceptatie- en Productie omgeving. De ontwikkelomgeving staat op een andere server dan de overige omgevingen.

## 5. Database

TrainStation maakt gebruik van een instantie van MariaDB. De database server wordt niet gebruikt voor andere applicaties en/of doeleinden.

### *5.1 Toegankelijkheid*

De database server wordt beheerd door de IT- en Ontwikkelafdeling van TrainStation, die volledige toegang heeft tot de database server.

### *5.2 Back-up*

Er wordt iedere dag een backup (herstelpunt) per database gemaakt op de productieomgeving, welke 30 dagen bewaard blijft. De eerste backup van de maand wordt 3 maanden bewaard.

### *5.3 Afscherming*

Iedere klant van TrainStation heeft een eigen database. Hierdoor is het onmogelijk dat klantspecifieke informatie beschikbaar wordt voor andere klanten. Verder zal in het geval van een virus of gekraakt gebruikersaccount alleen de database van het betreffende klant worden aangevallen. Hierbij zullen alle gegevens in deze database gecompromitteerd zijn.

## 6. Applicatie

### *6.1 Logging*

TrainStation hanteert een strict error logging beleid. De logs worden opgeslagen op de server. Daarnaast wordt de IT- en Ontwikkelafdeling automatisch per mail op de hoogte gesteld bij het optreden van een error.

### *6.2 Encryptie*

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

Op het moment van schrijven bestaat het hashing algoritme uit een SHA1 [2] en Salt [3] versleutelde “key”. 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 gebruiker bereiken, dan treedt er een mechanisme in werking die de technische details van de desbetreffende fout verbergt voor de gebruiker, maar wel de ontwikkelaars van TrainStation op de hoogte stelt van de fout, inclusief details.

### *6.4 Cookies*

TrainStation gebruikt alleen technische en functionele cookies. En analytische cookies die geen inbreuk maken op de privacy van de gebruiker. Een cookie is een klein tekstbestand dat bij het eerste bezoek aan deze website wordt opgeslagen op

de computer, tablet of smartphone van de gebruiker. De cookies die wij gebruiken zijn noodzakelijk voor de technische werking van de website en het gebruiksgemak.

### *6.5 Rollen*

Een gebruiker van TrainStation 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 TrainStation dat één gebruiker ongemerkt meer rechten ontvangt dan zijn of haar bevoegdheid voorschrijft. Het toekennen van gebruikersrechten is geheel in het beheer van TrainStation, tenzij anders bepaald.

## 7. Broncode

De broncode van TrainStation bestaat deels uit maatwerk en deels uit voorgeprogrammeerde code van het applicatie framework, welke de basis vormt van de TrainStation applicatie.
TrainStation maakt in de front- en back-end gebruik van PHP MVC op basis van Zend Framework. Op het moment van schrijven is er geen Escrow-overeenkomst vastgelegd.

### *7.1 Git*

TrainStation 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.

### *7.2 Cloud*

De Git repository van TrainStation wordt gehuisvest door Bitbucket. Hier staat uitsluitend code opgeslagen en dus geen gebruikersdata.

### *7.3 Toegankelijkheid*

De Git repository is alleen toegankelijk voor de ontwikkelaars van TrainStation. Er is per ontwikkelaar een account nodig met de bijbehorende lees- en schrijfrechten.

## 8. Continuïteitsplanning

Er kan altijd iets misgaan met de server, we doen er daarom alles aan om de ‘downtime’ te beperken en de data van de applicatie veilig te stellen, zoals:

### *8.1 Testing*

Om te voorkomen dat er door een aanpassing in de applicatie onderdelen van het systeem niet meer naar behoren werken, hanteren we een tweetal tests:
- Unit tests: hiermee testen we belangrijke stukken geprogrammeerde code, waarbij een bepaalde invoer altijd hetzelfde resultaat (uitvoer) moet hebben.
- Selenium tests: hiermee bootsen we gebruikershandelingen na door kliks en toetsaanslagen te simuleren in een webbrowser. Daarbij controleren we of de juiste informatie op het scherm wordt getoond.

Bij beide tests kan echte data gebruikt worden, deze blijft echter anoniem.

### *8.2 Disaster Recovery*

TrainStation heeft een efficiënt ‘rampenplan’ op de plank liggen. Bij ernstig falen van de server kan TrainStation binnen zeer korte tijd weer in de lucht zijn.
Het platform kan in de regel binnen de tijdsduur van 1 uur weer volledig operationeel zijn. Bij deze berekening wordt uitgegaan van het correct functioneren van de diensten van de domein registrar en volledige toegang tot de DNS van TrainStation.nl. Mocht deze toegang niet kunnen worden verleend, dan zal TrainStation tijdelijk worden opgezet onder een andere domeinnaam totdat de domein registrar weer toegang kan verlenen tot de DNS van TrainStation.nl.

[1] https://www.pocos.nl
[2] https://nl.wikipedia.org/wiki/SHA-familie
[3] https://nl.wikipedia.org/wiki/Salt_(cryptografie)