Fitale
Meerwaarde in zicht

SAFETY & QUALITY FITALE ADVIESSCAN PORTAL BY FITALE

Versie: 13 mei 2020

Fitale Schepenenstraat14 Geldrop

Fitale
Postbus 40
5580 AA Waalre
Nederland

+31 (0)40 - 304 15 16
welkom@fitale.nl
fitale.nl

KVK: 60184868
IBAN: NL97 RABO 0155 9195 04

1. Beveiliging en kwaliteitsborging van Fitale

Hoge kwaliteit en veiligheid zijn cruciale pijlers van de applicatie. Dit document licht toe hoe dit geborgd is. Hiervoor hanteren we het BIV-model, dit staat voor: Beschikbaarheid, Integriteit en Vertrouwelijkheid. Dit model wordt ook gehanteerd binnen de ISO 27001 certificering, volgens welke standaarden de applicatieontwikkeling plaatsvindt.

BIV: Beschikbaarheid

De applicatie moet altijd beschikbaar zijn voor de gebruikers. Dit borgen we met de volgende maatregelen:

- **Hardware, server & applicatiemonitoring**: 24/7 worden de servers gelogd door de applicatie Grafana. Hierdoor worden incidenten worden hierdoor direct gedetecteerd en opgepakt.
- **Centrale logging**: Alle handelingen in de applicatie worden 30 dagen bijgehouden in Papertrail**.** Onregelmatigheden kunnen achteraf snel worden opgespoord en opgelost.
- **Onverwachte fouten (real-time)**: Indien er zich een fout voordoet in de applicatie wordt het ontwikkelteam direct geïnformeerd via Sentry**.** Hiermee worden incidenten gerapporteerd zonder dat de gebruiker dit zelf hoeft te doen of zelfs nog voordat de gebruiker ervan op de hoogte is.
- **SLA-hosting (99.99% uptime)**: Vanaf 217 locaties wereldwijd wordt met de applicatie Uptrends getest of de applicatie bereikbaar is. De beschikbaarheid van de servers is 99,99%, exclusief gepland onderhoud.
- **Configuratie webserver via versiebeheer**: Alle wijzigingen aan de servers worden gelogd in Ansible. Hiermee wordt geborgd dat er geen fouten kunnen ontstaan in de configuratie.
- **OTAP-straat**: Een applicatie wordt ontwikkeld in een OTAP-straat (Ontwikkel, Test, Acceptatie, Productie-Omgeving) via Puppet Pipelines. Binnen de OTAP-straat wordt de applicatie zowel automatisch als functioneel getest voordat deze op een productieomgeving terecht komt. Hierdoor komen er alleen geteste versies op een live omgeving.
- **Code-reviews**: Alle code die wordt geschreven wordt door minimaal twee developers nagekeken en verwerkt via Bitbucket**.**
- **Automatische tests voor iedere oplevering**: Bij het verschijnen van een nieuwe versie worden delen van de applicatie automatisch getest met Bitbucket & PHPUnit
- **Backups**: Er worden kopieën gemaakt van de laatste 7 nachten en 1 per week van de laatste 6 weken. Deze worden opgeslagen in een ander datacentrum dan waar de applicatie gehost wordt.

BIV: Integriteit

Om de integriteit te bewaken moeten we de informatie op een platform kunnen valideren op correctheid. We hanteren hiervoor de volgende maatregelen:

- Coding standaarden (PSR-12, PSR-4, eslint en stylelint): Alle code wordt geschreven volgens de internationaal geldende "**PSR-12**" norm. Hierdoor is code overdraagbaar binnen het ontwikkelteam.
- Static code analysis: Alle code wordt automatisch geanalyseerd door de applicatie **PHPStan.** Hiermee wordt geborgd dat code ook daadwerkelijk voldoet aan de eisen.

BIV: Vertrouwelijkheid

Om de vertrouwelijkheid te bewaken moeten we ervoor zorgen dat informatie op en van de applicatie niet in handen kan komen van derden. Hiervoor zijn de volgende maatregelen genomen:

- **Interne procedures/registratie en controle van toegang** tot live data (actieve controle door de CISO, de Chief Information Security Officer): Alle procedures zijn beschreven en geformaliseerd volgens de **ISO 27001** norm. Dit wordt jaarlijks door een externe partij geaudit.
- **Gegevensclassificatie CISO** (klasse 3 applicatie met gevoelige informatie): Vertrouwelijke informatie is alleen toegankelijk voor specifieke personen binnen het bedrijf. Ook dit is volgens de **ISO 27001** norm.
- **Penetratietesten (OWASP top-10)**: Bij elke nieuwe versie worden er penetratietesten uitgevoerd op het platform. Dit gebeurt met het programma Detectify**.** Ook wordt er getest op de wereldwijd meest voorkomende beveiligingslekken. De onafhankelijke beveiligingsorganisatie OWASP levert hier dagelijks updates voor: de OWASP lijst.
- **Toegang server via VPN**, SSH (public/private key) en IP whitelisting: Alle toegang tot servers van de applicatie gaat middels het beveiligde VPN-protocol.
- Er wordt gebruik gemaakt van een 2.048-bits sterke **SSL-verbinding**.

2. Achtergrond ontwikkelteam

Softwareontwikkeling en onderhoud wordt verzorgd door Way2Web Software. Way2Web ontwikkelt innovatieve maatwerk applicaties voor klanten die een beslissende stap voorwaarts willen zetten. Als leiders en trendsetters in hun branche, zoeken ze telkens weer naar nieuwe en slimmere oplossingen om het met next level software anders en beter te doen dan de rest.
Kwaliteit, veiligheid en bedrijfszekerheid staan centraal bij Way2Web. Zij maken zich ook sterk voor verdere professionalisering van de branche binnen Dutch Digital Agencies, de branchevereniging en kennisorganisatie van de beste digitale bureaus in ons land. Daarnaast zijn ze medeoprichter van de Dutch Laravel Foundation, het kennisinstituut voor Laravel-ontwikkelaars in Nederland.

Agile Scrum
Voor het beheersen van haar projecten hanteert Way2Web de ontwikkelmethode Agile Scrum. Dit is de meest efficiënte methode om software te ontwikkelen. Met deze methode hebben opdrachtgever en het ontwikkelteam nauw contact. Dit heeft een aantal grote voordelen:

- De opdrachtgever heeft invloed gedurende het gehele proces en kan dus snel bijsturen.
- Er zijn meerdere tussenopleveringen waarbij de applicatie getest kan worden op accurate werking.
- De opdrachtgever kan al tijdens het project de applicatie aanbieden aan haar testklanten. Dit zorgt ervoor dat er tijdens de ontwikkeling alle ruimte is om gebruik te maken van voortschrijdend inzicht.

3. Hosting applicatie

De producten, diensten, applicaties en data van derden zijn ondergebracht op servers die aan de hoogste veiligheidsnormen voldoen. De hosting van de fysieke apparatuur en de faciliteiten van het datacenter is in handen van experts die hierin uitblinken. Deze partners zijn geselecteerd op veiligheid, continuïteit, kennisniveau en apparatuur van wereldklasse. `

Kenmerken datacenter

BIT B.V.
KVK: 09090351
De werkprocessen zijn ISO 27001 en NEN7510 gecertificeerd.

Stroomvoorziening

Het datacenter beschikt over dubbele rechtstreekse aansluitingen op het verdeelstation van netbeheerder Nuon. De stroom- en noodstroomvoorziening zijn tot in de serverracks volledig dubbel uitgevoerd met in de serverruimte een aparte groepenkast, met per rack een aparte schakelautomaat. Dubbel uitgevoerde UPS-systemen nemen bij een stroomonderbreking met behulp van accu's de stroomvoorziening naadloos over. Zo kunnen de dieselaggregaten opstarten die voor minimaal 48 uur stroom leveren. Elke maand wordt een hele dag op aggregaatspanning gewerkt, zodat zeker wordt gesteld dat de aggregaten altijd bedrijfsklaar zijn.

Maatregelen tegen brand

De serverruimte is voorzien van twee onafhankelijke branddetectiesystemen, namelijk conventionele rookmelders aangevuld met een early warning laserdetectiesysteem dat al bij vier deeltjes rook per miljoen deeltjes lucht alarm slaat. De brandmeldcentrales zijn met een vaste verbinding aangesloten op de meldkamer van de brandweer. Ook worden de alarmmeldingen via een apart systeem gemeld aan een particuliere alarmcentrale. Afspraken met de plaatselijke brandweer garanderen een snel ingrijpen in noodgevallen, met minimale schade aan de apparatuur.
Daarnaast blaast een eigen gasblusinstallatie bij brand in hoog tempo een speciaal Argonite gasmengsel ($Ar+N^2$) in de serverruimte, waardoor het zuurstofgehalte daalt en een brand in de kiem smoort. Het blusgas is niet schadelijk voor de opgestelde apparatuur, noch voor de mensen die eventueel aanwezig zijn of voor het milieu.

Inbraakbeveiliging

Het datacenter is elektronisch en bouwkundig beveiligd volgens BORG klasse 4, de hoogst haalbare norm voor een normaal bedrijfspand. Zo wordt de serverruimte afgesloten met kluisdeuren en de zijn hekken en sloten van de hoogst mogelijke kwaliteit. De alarminstallaties zijn door middel van twee rechtstreekse en bewaakte verbindingen aangesloten op twee verschillende meldkamers. 's Nachts en in het weekend surveilleren twee onafhankelijke beveiligingsdiensten om een optimale veiligheid te garanderen.

Camerabeveiliging

Overal in het datacenter zijn camera's geplaatst: niet alleen in de serverruimtes, maar ook buiten de gebouwen, bij alle ingangen en in de kantoorruimtes. Bij een alarm- of brandmelding buiten kantooruren kan de op afstand dienstdoende medewerker direct zien wat er aan de hand is. Bij elke vorm van onraad wordt de surveillancedienst gealarmeerd. De beelden van de camera's worden geregistreerd en tijdelijk gearchiveerd als mogelijk onderzoeks- of bewijsmateriaal.

Toegangscontrole

Voor toegangscontrole wordt gebruik gemaakt van een combinatie van paslezers en biometrische controle via irisscanners. Dankzij de irisscanners krijgen ongeautoriseerde personen geen toegang tot het datacenter. Aan de hand van de logs van het toegangscontrolesysteem is altijd te achterhalen wie wanneer welke ruimte betreden heeft.

Natuurverschijnselen

Het datacenter is gesitueerd in Ede in een pand dat in 2009 is opgeleverd en speciaal is ontworpen en gebouwd om als datacenter te fungeren. De serverruimte bevindt zich op 10 meter boven NAP, waardoor problemen als gevolg van overstroming worden voorkomen.

Airconditioning

De koelinstallatie zorgt in combinatie met closed cold corridors voor optimale koeling van de apparatuur. De installatie is op alle punten, inclusief pompen en leidingwerk, dubbel uitgevoerd, zodat een optimaal klimaat in de serverruimte gegarandeerd is.

Milieu

Er zijn veel energiebesparende maatregelen genomen. Zo kan door toepassing van closed cold corridors een flink deel van de tijd met vrije koeling worden gewerkt en wordt door toepassing van ultrasoonbevochtigers 95% energie bespaard vergeleken met stoombevochtigers. Alle energie die wordt gebruikt is duurzaam opgewekt.

Netwerk

Vanuit het datacenter wordt door middel van een glasvezelring verbinding gemaakt met het internetknooppunt AMS-IX in Amsterdam. Dit betekent dat er twee geografisch gescheiden glasvezelverbindingen lopen die zowel in Ede als in Amsterdam op twee verschillende locaties uitkomen en onderling ook weer door glasvezel met elkaar zijn verbonden. Hierdoor is het netwerk nog nooit onderbroken geweest.

Werkprocessen

De werkwijze van de organisatie van het datacenter voldoet aan ISO 27001 en NEN 7510. Deze internationale norm stelt de strengst mogelijke eisen aan informatiebeveiliging. Men gebruikt hierbij het Information Security Management System (ISMS) dat is ontworpen om de adequate keuze te waarborgen van proportionele beveiligingsmaatregelen die de informatie beschermen en vertrouwen bieden aan belanghebbenden.

Kenmerken servers

Hostingpartner

Exonet B.V.
KvK: 09129344
De werkprocessen zijn ISO 9001, 27001 en NEN7510 gecertificeerd.

Platform

Het virtualisatie platform is gebaseerd op de beste combinatie van hardware en software die op de markt te verkrijgen is en elk onderdeel hiervan is volledig redundant uitgevoerd. De hardware is gebaseerd op een FlexPod, een door Cisco en NetApp gestandaardiseerde en gevalideerde omgeving, waardoor alle onderdelen optimaal met elkaar samenwerken.

Servers

De bladeservers van Cisco zijn voorzien van de laatste Intel Xeon processoren met minimaal 20 cores. De servers zijn redundant uitgevoerd, waardoor er bij problemen direct overgeschakeld kan worden op een andere server.

Opslagruimte

De opslag wordt verzorgd door enterprise opslagsystemen van NetApp. Deze systemen maken gebruik van een grote hoeveelheid snelle SAS-schijven, een flash cache en intelligente RAID-levels. Hierbij is alles redundant uitgevoerd, zodat elk onderdeel van het systeem mag uitvallen zonder dat dit een onderbreking tot gevolg heeft.

Firewall en toegang

Om ervoor te zorgen dat niemand zich onbedoeld toegang kan verschaffen tot de data op de servers zijn alle poorten afgesloten met een firewall. Alleen de noodzakelijke poorten zijn toegankelijk voor publieke IP-adressen en volledige toegang tot de servers is slechts mogelijk vanaf het kantoor van Exonet.

Back-up

Er wordt elke nacht een back-up gemaakt van alle data. De kopieën van de laatste 7 nachten en 1 per week van de laatste 6 weken worden bewaard. Deze worden opgeslagen in een ander datacenter, 500 meter verderop, dat aan dezelfde strenge veiligheidseisen voldoet.

Support

De servers worden met monitoringsoftware continu in de gaten gehouden. Mochten er indicaties zijn van (toekomstige) problemen dan wordt hiervan automatisch, per sms, melding van gemaakt zodat meteen kan worden ingegrepen. Ook is de storingsdienst 24 per dag 7 dagen bereikbaar voor het

geval zich calamiteiten voordoen. De gegarandeerde responsetijd op een storing is 4 uur, maar in de praktijk wordt er direct actie ondernomen.

VPN

Servers zijn alleen bereikbaar via een sterk versleutelde VPN-verbinding. Exonet maakt hiervoor gebruik van een Fortinet Fortigate firewalling cluster.

Software updates

Exonet heeft processen ingericht om dagelijks op de hoogte te zijn van beveiligingslekken in alle hosting-softwarecomponenten. Op deze manier kan adequaat worden ingegrepen en worden patches geautomatiseerd uitgerold nadat deze zijn getest.