Databescherming en technische details

Software

- Historisch gezien kunnen we een uptime garanderen van de VrijeDagen applicatie van minimaal 99.5%. Voor een cloudapplicatie is dat relatief hoog.
- Updates en bugfixes worden dagelijks via Continuous integration doorgevoerd op het live systeem waardoor er geen tot nauwelijks down-time ontstaat.
- De applicatie is ontwikkeld in ASP.NET. De ontwikkeling wordt door eigen programmeurs gedaan en dat is altijd zo geweest.
- Ons team werkt volgens het Agile programmeer principe.
- Front-end maakt de applicatie onder andere gebruik van JavaScript
- Back-end is de applicatie voornamelijk in C# geschreven
- Gebruikers die inloggen maken gebruik van een AES 256 encryptie methodiek. Wat betekent dat ze verplicht zijn om een sterk wachtwoord te gebruiken. Optioneel voor gebruikers is het mogelijk om in te loggen via Oauth of 2FA.
- Ook wordt alle data versleuteld verzonden volgens de AES 256 encryptie methodiek
- De applicatie websites zelf zijn weer SHA 256 en TLS 1.2 gecertificeerd. Dus tussen de applicatie, de servers en de databases wordt alle verzonden data gecontroleerd op echtheid volgens de HTTPS, SHA256 en TLS 1.2 methodiek.
- De sourcecode ligt opgeslagen op servers van Microsoft Devops
- Er wordt OpenIDconnect met OAuth AccessTokens voor de API's en JWT Tokens als basis authenticatie gehanteerd. De wachtwoorden worden AES encryptie opgeslagen. De tokens worden getekend met een digitaal certificaat x.509 RSA algoritme.
- Iedere klant heeft een eigen database en website op een gedeelde webserver welke IIS draait.
- De applicatie wordt via SSL benaderd.
- We werken met Reverse Proxy servers voor het flexibel verwerken van adressering in ons netwerk (oa bij calamiteiten).
- Connecties van en naar het datacenter, dus niet naar een website, doet ons personeel met een VPN verbinding.
- De 2FA (two factor authentification) van MobilePass van ons personeel zorgt ervoor dat inlognamen en wachtwoorden ook versleuteld over het internet verzonden worden.
- Ook 'in rust' is alle data op de Azure servers alleen versleuteld beschikbaar.
- De software op onze (lokale) machines worden automatisch gecontroleerd door de software registratie tool Solarwinds en ook nog eens maandelijks door Microsoft SPLA. Tevens installeren wij uit voorzorg op alle machines Bitdefender en Cisco AMP Solutions.
- Via de dienst Solarwinds RMM worden met regelmaat penetratietests uitgevoerd

Hardware

- Onze software draait op onze eigen servers en wordt gehost in een datacenter in Rotterdam (http://www.i3d.nl/) Dit datacenter heeft een toegangscontrole systeem voor bij de voordeur en naar de ruimte waar de servers staan. Het toegangscontrole systeem wordt ondersteund door de aanwezigheid van veiligheidspersoneel (24 uur per dag) en videobewaking.
- Onze systeembeheerders dienen zich eerst aan te melden alvorens het biometrische systeem de toegang zal verlenen.
- Vervolgens is ons rack fysiek beveiligd middels een slot voor de laatste toegang. Dit slot kan alleen geopend worden door eigen, geautoriseerd personeel.
- De brandveiligheid in dit datacenter is voorzien door een verminderde zuurstof mengsel waarbij mensen in de betreffende ruimte wel gewoon kunnen ademhalen, maar vuur niet kan ontstaan.
- Er liggen vanuit het datacenter drie verschillende dataverbindingen, elk vanaf een hoek van het pand naar een andere netwerk knooppunt. Hierdoor is het welhaast onmogelijk om data uitval vanuit het datacenter te hebben.

- De productie en webservers in het datacenter zijn geplaatst achter een Cisco ASA 5508-X met:
  - IPS (Intrusion Prevention System) tegen DDOS aanvallen)
  - AMP (AntiMalware Protectie)
  - URL (Filtering van verkeer van en naar de servers)
- De Webservers (als enige in de DMZ) zijn vervolgens pas bereikbaar na een Proxy server
  - Extra veiligheid
  - Load balancing van de Site's
- Al onze computersystemen en onze netwerk componenten zijn dubbel uitgevoerd. (Redundant).
- De website wordt middels loadbalancing verdeeld over meerdere webservers die op hun beurt verbinding maken naar het i-SCSI harddisk cabinet
- Er wordt gewerkt op HP bladeservers (met 24x7, 4uur support contract) in een VMWare ESX omgeving met Acronis backup procedure.
- Voor backup, redundancy, en onderhoud word er een Cisco ASA 5520 ingezet. Beide firewalls worden gemonitord in een FMC, DUO (2FA) & Gemalto
- Vrijwel alle onderdelen staan minimaal dubbel geïmplementeerd.

Backups

- De databases staan in MSSQL 2016. De individuele databases worden dagelijks ook nog eens on-line gebackuped (dit gebeurt dus off-site).
- Database backups worden incrementeel gemaakt op separate schijven van de database files, dit geldt elk uur voor de logfiles en elke dag voor de database.
- De schijven van de servers worden dagelijks gebackupped naar online backup faciliteit.
- De VM machines worden volledig gebackupped ook naar online backup faciliteit.
  We werken met virtual machines die live kunnen worden gemigreerd tussen storage faciliteiten. Het verlies van een enkele schijf zal geen gevolgen hebben voor de service.
- Elke klant heeft een eigen database met de mogelijkheid dat deze wordt teruggeplaatst dan wel in een beschermde omgeving wordt geplaatst voor controle of onderzoek.
- Het fysieke adres voor online backups betreffen de datacenters van Equinix te Amsterdam

Herstel

- RTO (Recovery Time Objective); is 5 uur na normaal verlies van werkende machines. 24 uur na catastrofaal verlies van volledige infrastructuur.
- RPO (Recovery Point Objective); is tot maximaal het hele uur voor verlies van werkende machines.
- De fysieke adressen voor datarecovery (DR) betreffen:

Compete IT Solutions	**&**	**Microsoft Azure**
Algerastraat 7		Western Europa
3125 BS		Middelmeer
Schiedam		Noord-Holland

Wie

- Compete IT Solutions BV is leverancier van het product www.vrijedagen.nl
- Wij zijn ISO/IEC 27001:2013 (certificaat nr. ISC127) gecertificeerd
- Compete zelf bestaat al sinds 1989
- Vrijedagen de applicatie bestaat sinds 2005
- Als code van ethiek en professioneel gedrag volgen wij de AVG/GDPR regels, het bedrijfs-regelement en geheimhoudingsverklaring nauwlettend.
- Om veiligheid te kunnen blijven garanderen wordt de organisatie met regelmaat door auditors (extern en intern) doorgelicht. De resultaten hiervan worden beschikbaar gesteld aan het management team van Compete IT Solutions BV.
- Van alle medewerkers wordt de achtergrond gescreend tijdens de sollicitatieprocedure. Hierbij wordt onder andere gelet op het opleidingsniveau en gedrag (VOG).
- Alle medewerkers hebben een geheimhoudingsverklaring en het bedrijfs-regelement ondertekend. Ook zijn zij verplicht om sterke wachtwoorden te gebruiken, welke zij regelmatig moeten aanpassen.
- Onze netwerkbeheerders zijn CCNA gecertificeerd

Handtekening:

P.J.J. vd Water

Compete IT Solutions