INF2A

Onderzoeksverslag

NHL STENDEN hogeschool

StemApp

Gemeente Almelo

gemeente Molenwaard

gemeente Hollands Kroon

Gemeente Emmen

gemeente lingewaard

Interior of a data center (Manuel - Pexels.com)

Stenden hogeschool Emmen (Richard Broekhuijzen)

Opdrachtgevers:

Dhr. Jan-Willem Bos
(gemeente Emmen)
Dhr. Patrick Jonkman
(gemeente Almelo)

Projectgroep:

Fekke Fekkes	Fekke.Fekkes@student.stenden.com
Niels Stevens	Niels.Stevens@student.stenden.com
Ernst-Jan Bakker	Ernst-Jan.Bakker@student.stenden.com
Jimmy Habing	Jimmy.Habing@student.stenden.com
Niels van Wijk	Niels.van.Wijk@student.stenden.com
Kevin Hekman	Kevin.Hekman@student.stenden.com
Justin Heidotting	Justin.Heidotting@student.stenden.com

NHL STENDEN hogeschool

In samenwerking met:

FORUS

Versiebeheer

Versie	Status	Auteur(s)	Reden van uitgave / verandering
0.1	Concept	INF2A	Concept versie/opbouw van alle hoofdstukken
0.2	Copyright vrije afbeeldingen ingevoegd	Fekke Fekkes	Cover foto's waren nog leeg.
1.0	Alle hoofdstukken zijn ingevuld	INF2A	Eerste versie document, zonder feedback.

Verklarende woordenlijst

Node - "Een node is in een computer netwerk een connectie punt (server) die data kan ontvangen, aanmaken, opslaan of verzenden" (TechTarget, Rouse, & Gerwig, 2016).

PhoneGap – Officiële naam "PhoneGap Cordova", is een programma waarmee Apps geschreven kunnen worden in CSS,HTML5 en JavaScript. Omdat apps geschreven worden in programmeertalen waaruit webpagina's ook bestaan kan een app makkelijk gereleased worden op zowel Android als Apple iOS (Adobe Systems Inc., z.d.).

Quorum- Dit is software die er voor zorgt dat er snel een private transactie kan worden gedaan binnen een toegestane groep van bekende deelnemers (J.P. Morgan, z.d.).

Minen – "Een proces van gegevens vastleggen in een blockchain met behulp van rekenkracht van computers" (Cointelegraph, z.d.) .

Consensys- Consensys is een bedrijf die gespecialiseerd is in het bouwen, adviseren en faciliteren van gedecentraliseerde applicaties op de Ethereum blockchain (ConsenSys, z.d.).

VM's- "Een Virtual Machine (VM) is een besturingssysteem (operatingsystem, OS) of applicatie-omgeving die geïnstalleerd is op software die specifieke hardware imiteert. Virtual Machines zijn zo ingericht dat de eindgebruiker van de applicatie of het besturingssysteem op dezelfde manier kan blijven werken als hij gewend is" (Marqit, z.d.).

load balancing- "Load balancing verdeelt de hoeveelheid werk waar een computer mee te maken heeft over twee of meer computers, zodat meer werk kan worden gedaan binnen dezelfde hoeveelheid tijd en in het algemeen, alle gebruikers sneller bediend kunnen worden. Load balancing kan worden uitgevoerd door hardware, software of een combinatie van beiden" (Marqit, z.d.).

API- "Een API is een set aan definities waarmee softwareprogramma's onderling kunnen communiceren. Het dient als een interface tussen verschillende softwareapplicaties waardoor de gebruikte code automatisch elkaar toegang tot informatie en/of functionaliteit geeft, zonder dat ontwikkelaars hoeven te weten hoe het andere programma exact werkt" (Computerworld & V Tuil, z.d.).

(MS)(My)SQL – "SQL (spreek uit S-Q-L of Sequel) staat voor Structured Query Language en is wereldwijd de meest populaire (vraag)taal om relationele databases mee aan te sturen"(Computerworld & V Tuil, z.d.).

SQL injectie(s) – "Een SQL-injectie (of SQLi) is een methode om een op SQL-gebaseerde database via internet te kraken. De hacker test in zo'n geval vooraf of de database van de website vatbaar is voor een SQL-injectie door verschillende queries via zijn browser op de database los te laten. Als de hacker beet heeft (en de database dus kwetsbaar is), kan de hacker uiteindelijk de backend database in zijn geheel overnemen" (Computerworld & V Tuil, z.d.).

Samenvatting

Het doel van het onderzoek is om een overzicht te krijgen over hoe de StemApp opgezet is en wat er voor nodig voor is om de app om met zo min mogelijk fouten/storingen draaiend te krijgen voor de pilot die gehouden gaat worden over een gemeentelijk besluit. In dit document zijn de resultaten van dit onderzoek te vinden. Aan de hand van deze resultaten zal de projectgroep een advies uitbrengen over wat volgens de projectgroep de beste oplossing is.

De hoofdvraag van dit onderzoek is:

> ***"Hoe richt men een omgeving in met betrekking tot blockchain, die geschikt is om te gebruiken voor het houden van een pilot in een wijk of dorp in de gemeente Emmen, waarbij gestemd kan worden over een lokaal besluit?"***

Om antwoord te geven op deze hoofdvraag zijn er een aantal deelvragen opgesteld door de projectgroep.

- *Hoe werkt de StemApp?*
- *Wat is de schaalbaarheid van de StemApp?*
- *Welke resources zijn er nodig om de StemApp te kunnen gebruiken en hier een test mee uit te kunnen voeren?*
- *Moet de omgeving in de cloud of lokaal gaan draaien?*
- *Hoe is de security geregeld in de StemApp-omgeving?*

De antwoorden op deze vragen zijn mogelijk niet meer up-to-date of van toepassing wanneer de app daadwerkelijk in productie wordt gebracht door de gemeenten. De projectgroep heeft alleen rekening gehouden met de pilot die gedaan gaat worden in een wijk of dorp in de gemeente Emmen tussen juni en september 2018.

Voor dit onderzoek heeft de projectgroep gesprekken gevoerd met diverse partijen. Zo is er een afvaardiging van de projectgroep naar Den Haag toe gereisd om daar met de toenmalige app bouwer (Milvum) te praten. Tijdens dit gesprek is door Milvum een broncode overhandigd die de projectgroep kon gebruiken voor het onderzoek. Vanwege enige problemen met deze opgeleverde broncode en "conflicten" tussen de opdrachtgevers en Milvum hebben de opdrachtgevers besloten om verder te gaan met Stichting Forus uit Groningen. Dit heeft voor de projectgroep het gevolg dat niet voor de deadline van dit document geen werkende "testomgeving" gedraaid kon worden. Alle antwoorden op de onderzoeksvragen zijn gebaseerd op literatuuronderzoek, eigen kennis en interviews met diverse partijen en experts.

Inhoudsopgave

Inhoud

Inleiding

Het doel van het onderzoek is om een overzicht te krijgen over hoe de StemApp opgezet is en wat er voor nodig voor is om de app om met zo min mogelijk fouten/storingen draaiend te krijgen voor de pilot die gehouden gaat worden over een gemeentelijk besluit. In dit document zijn de resultaten van dit onderzoek te vinden. Aan de hand van deze resultaten zal de projectgroep een advies uitbrengen over wat volgens de projectgroep de beste oplossing is.

De hoofdvraag van dit onderzoek is:

> ***"Hoe richt men een omgeving in met betrekking tot blockchain, die geschikt is om te gebruiken voor het houden van een pilot in een wijk of dorp in de gemeente Emmen, waarbij gestemd kan worden over een lokaal besluit?"***

Om antwoord te geven op deze hoofdvraag zijn er een aantal deelvragen opgesteld door de projectgroep.

- Hoe werkt de StemApp?
- Wat is de schaalbaarheid van de StemApp?
- Welke resources zijn er nodig om de StemApp te kunnen gebruiken en hier een test mee uit te kunnen voeren?
- Moet de omgeving in de Cloud of lokaal gaan draaien?
- Hoe is de security geregeld in de StemApp-omgeving?

De antwoorden op deze vragen zijn mogelijk niet meer up-to-date of van toepassing wanneer de app daadwerkelijk in productie wordt gebracht door de gemeenten. De projectgroep heeft alleen rekening gehouden met de pilot die gedaan gaat worden in een wijk of dorp in Emmen tussen juni en september 2018.

Voor dit onderzoek heeft de projectgroep gesprekken gevoerd met diverse partijen. Zo is er een afvaardiging van de projectgroep naar Den Haag toe gereisd om daar met de toenmalige app bouwer (Milvum) te praten. Tijdens dit gesprek is door Milvum een broncode overhandigd die de projectgroep kon gebruiken voor het onderzoek. Vanwege enige problemen met deze opgeleverde broncode en "conflicten" tussen de opdrachtgevers en Milvum hebben de opdrachtgevers besloten om verder te gaan met Stichting Forus uit Groningen. Dit heeft voor de projectgroep het gevolg dat niet voor de deadline van dit document geen werkende "testomgeving" gedraaid kon worden. Alle antwoorden op de onderzoeksvragen zijn gebaseerd op literatuuronderzoek, eigen kennis en interviews met diverse partijen en experts.

Onderzoeksopzet

Dit hoofdstuk van het onderzoeksverslag beschrijft de algehele opzet van het onderzoek. De onderwerpen onderzoek, dataverzameling en analysemethoden komen hierin aan bod.

Onderzoek

Tijdens het onderzoek zijn er twee onderzoeksmethoden toegepast. Namelijk deskresearch en kwalitatief onderzoek Deze methoden worden hieronder beschreven om zo een duidelijker beeld te geven bij hun betekenis.

- Deskresearch: onderzoeksmethode waarbij er gebruik gemaakt wordt van bestaande gegevens. Hierbij gebruiken de onderzoekers gegevens en data van literatuur en bestaande onderzoeken om standpunten en stellingen te onderbouwen.
- Kwalitatief onderzoek: onderzoeksmethode die zich meer richt op beschrijvingen en interpretaties, deze worden meestal weergegeven in woorden.

Dataverzameling

De data/gegevens die verzameld wordt komt voornamelijk voort uit deskresearch. Tijdens dit proces halen de onderzoekers informatie uit bronnen zowel online als offline. Hieronder vallen ook de notulen die de projectgroep gemaakt heeft tijdens meerdere afspraken en interviews met de opdrachtgevers en externe partijen.

Alle verzamelde data wordt vervolgens omgezet naar bruikbare gegevens en resultaten. Deze worden uiteindelijk verwerkt in dit onderzoeksverslag.

Analysemethoden

De vergaarde data wordt middels interpretatie verder in het rapport verwerkt en gebruikt. Bij deze methode komt dus de projectgroep tot de resultaten en een conclusie.

Resultaten

In dit hoofdstuk zijn de resultaten van het onderzoek te vinden. De resultaten zijn de uitkomsten van de onderzoeksvragen die in de inleiding van dit document te vinden zijn. Dit hoofdstuk bevat alleen de bevindingen van de onderzoeken die gedaan zijn. In het hoofdstuk Conclusie/Advies is het advies te vinden die gevormd is aan de hand van de resultaten die in dit hoofdstuk te vinden zijn.

Werking van de StemApp

Van de StemApp zijn er nu inmiddels twee versies, één versie is gebouwd door Milvum, en er is een versie gebouwd door Forus. De vormgeving van deze twee apps is momenteel (bijna) identiek. Echter zijn de infrastructuur en de werking van deze twee apps zijn verschillend. In overleg met de opdrachtgevers zal er alleen gefocust worden op de versie die gebouwd is door Forus. Het gevolg hiervan is dat de versie waarmee gewerkt gaat worden nog in ontwikkeling is door Stichting Forus. Hierdoor is de projectgroep niet in staat om voor de gestelde deadline van dit document de volledige werking van de StemApp te weten of te testen. Wat wel bekend is staat hieronder beschreven.

Blockchain

De StemApp moet uiteindelijk gebruik gaan maken van de Ethereum blockchain. De reden waarom Ethereum gekozen is omdat door middel van smartcontracts gedecentraliseerde applicaties gebouwd kunnen worden. Dit is voor de toepassing van de StemApp een ideale uitkomst. De StemApp mag namelijk niet afhankelijk zijn van één partij of persoon omdat deze partij of persoon de uitslag van een verkiezing of stemming zou kunnen veranderen.

Omdat de techniek nog niet ver genoeg is om veilig en anoniem te kunnen stemmen is er in overleg met stichting Forus gekozen om tijdens de pilot gebruik te maken van een ”traditionele omgeving” met een SQL database.

In de 1e fase van dit project wordt er een pilot gehouden. Deze pilot wordt gebruikt als test voor de front-end en functionaliteiten van de StemApp. Na de pilot wordt het onderzoek voor een back-end dat op de Ethereum blockchain draait in gang gezet. Stichting Forus gaat dan onderzoek doen naar het gebruik van Quorum van JP Morgan en onderzoeken of er een node gedraaid kan worden bij het bedrijf ConsenSys.

Pilot

Voor de pilot zal zoals eerder genoemd is gebruik gemaakt gaan worden van een ”traditionele omgeving”. Deze ”traditionele omgeving” zal gebruik maken van een standaard SQL database en NodeJS. De StemApp die tijdens de pilot gebruikt gaat worden is geschreven in het programma PhoneGap zodat deze zowel op Android devices kan draaien als Apple devices. De StemApp wordt tijdens deze pilot dan voornamelijk getest op functionaliteit, vormgeving en er wordt gekeken of er genoeg animo voor is. Verder kan er voor gekozen worden om de stemgerechtigden te laten inloggen op de StemApp doormiddel van de Me-App van Stichting Forus.

De stelling die gebruikt gaat worden bij de pilot kan worden beheerd via een dashboard die te bereiken is op een website. Ook op deze dashboard kan de mogelijkheid worden toegev oegd om in te loggen met de Me-App van stichting Forus.

Me-App

Stichting Forus is bezig met het ontwikkelen van de Me-App. Met deze app kan een gebruiker zijn/haar eigen digitale identiteit beheren. Deze app zou ook gebruikt kunnen worden tijdens de pilot. De gebruikers of beheerders van de StemApp kunnen met behulp van de Me-App de eigen identiteit verifiëren waardoor gebruikers toegang kunnen krijgen tot een stelling en beheerders toegang kunnen krijgen tot het beheerportaal van de StemApp.

Schaalbaarheid

Om een goed beeld te kunnen krijgen over de schaalbaarheid van het systeem wordt er onderzocht wat er benodigd is om het initiële systeem te kunnen laten draaien en hoeveel mensen hier dan gebruik van kunnen maken. Door middel van het trekken van een basislijn kan er gekeken worden wat voor resources het systeem nodig is en wanneer het moet worden uitgebreid voor bijvoorbeeld piektijden.

Basislijn

Wanneer het systeem opgezet wordt moet er een basislijn getrokken worden voor het aantal gebruikers die gebruik gaan maken van het systeem. Om deze initiële setup goed in beeld te kunnen krijgen is er naar aanleiding van het gesprek met Stichting Forus gebleken dat men voor 80 gezinnen 3 nodes (servers / vm's) nodig is.

Uitbreidingsmogelijkheden / Doorontwikkeling

Door middel van het toevoegen van bovengenoemde "nodes" is het mogelijk om het draagvlak van het aantal gebruikers te vergroten. Hiervoor is technische kennis van het bestaande systeem nodig en moet er een manier zijn voor het "load balancing" van alle stemmen die binnen gaan komen, tevens is het maar op een bepaald aantal dagen dat er pieken van gebruikersinteractie voor zullen / kunnen komen. Hierna is het niet cruciaal dat alle "nodes" op volle capaciteit blijven opereren. Pas wanneer er weer gestemd gaat worden kan men de "nodes" weer op volle vermogen zetten waardoor het systeem de hoeveelheid stemmen zonder problemen zou kunnen verwerken.

Tevens is het mogelijk om de app in een later stadium toe te voegen binnen het "echte net", dit betekent dat de app toegevoegd wordt aan de public Ethereum blockchain. Dit is alleen mogelijk wanneer de ethereum blockchain draait binnen Quorum, en voor het "echte net" wordt dan gebruikt gemaakt van een "node" via ConsenSys, hier word na de pilot in de 2e fase van het project aan gewerkt samen met stichting Forus.

Resources

Voor het project StemApp zijn er bepaalde resources nodig om een test te kunnen doen met de applicatie. De volgende onderzoeksvraag is opgesteld: Welke resources zijn er nodig om de StemApp te kunnen gebruiken om hier een test mee uit te kunnen voeren? Hiervoor is onderzoek gedaan en in dit hoofdstuk worden de resultaten benoemd.

Voor het onderzoek dat de projectgroep heeft uitgevoerd zijn twee partijen betrokken deze zijn al eerder benoemd in de voorgaande hoofdstukken (Milvum en Stichting Forus). Na vragen te hebben gesteld aan de ontwikkelaars van de originele StemApp (Milvum) over hoe de pilot is uitgevoerd was er weinig bekend over van welke resources hiervoor gebruikt zijn, alleen dat hier een standaard server van TransIP gebruikt is.

Kindpakket gemeente Zuidhorn

Na een gesprek te hebben gehad met de Stichting Forus is er meer bekend geworden over een omgeving die gebruikt kan worden. Op basis van een soortgelijke app die ook werkt met Blockchain voor het kindpakket in Zuidhorn zijn er vragen gesteld over hoe dit systeem precies werkt en wat er voor nodig is om deze te kunnen draaien. Hier zijn de volgende resultaten uit gekomen.

De servers zijn op de volgende manier ingericht:

Server 1: Front-end server
Server 2: Traditionele back-end server
Server 3: Ethereum node met eigen geschreven API

De specificaties van de servers zijn als volgt:

- 1 intel Xeon core
- 1 Gigabyte RAM
- 50 Gigabyte opslag

Als besturingssysteem wordt er gebruik gemaakt van een Linux distro.

Server 1:
Op server 1 wordt de front-end van het systeem gedraaid. Dit houdt onder andere in dat de website op die server gehost wordt.

Server 2:
Op server 2 wordt de traditionele back-end server gehost. Daar staat een SQL server op die gegevens opslaat voor het kindpakket.

Server 3:
Op server 3 wordt de Ethereum node gehost met een eigen geschreven API. Deze API communiceert met het systeem. De Ethereum node staat op dit moment private. Dit betekend dat transacties niet openbaar zijn er dus niet van buitenaf gecontroleerd kunnen worden. Het betekent wel dat de node niet tegen andere nodes hoeft te “racen”, wat dus betekent dat er geen grote rekenkracht nodig is om te minen.

Stichting Forus gaat bij het uitbreiden en schaalbaar maken van het kindpakket de Front-end en traditionele back-end in de cloud laten draaien. Voor de blockchain kant wordt er gekeken naar een andere oplossing. Er wordt door Forus onderzocht over het gebruik van Quorum zoals dit ook bij de StemApp onderzocht wordt.

De app die gemeente Zuidhorn gebruikt werkt deels nog met een traditioneel ingerichte omgeving die naast een blockchain omgeving draait. De drie servers die voor het kindpakket zijn inricht zijn allemaal vrij klein dit betekent 1 core en 1 GB ram. De servers draaien bij TransIP. Op de eerste server draait de traditionele back-end, op de tweede de front-end en de derde server wordt gebruikt als Ethereum node.

Er zijn nu tachtig gezinnen die gebruik maken van het kindpakket. Het systeem heeft met de resources die er nu worden gebruikt bij het kindpakket geen enkel probleem om het gebruik van alle tachtig gezinnen tegelijkertijd aan te kunnen. Door gekeken te hebben naar de resources die Forus heeft gebruikt voor het draaien van het kindpakket kunnen de resources van de StemApp hierop worden gebaseerd.

De omgeving van het kindpakket wordt als basislijn gebruikt bij het opzetten van de pilot omgeving. Aan de hand van de grote van de pilot kunnen de resources hierop worden afgestemd.

Cloud of lokaal?

Voor de StemApp moet er de keuze worden gemaakt of deze in de cloud of lokaal moet worden gedraaid. Hiervoor is de volgende onderzoeksvraag opgesteld: *Moet de omgeving in de cloud of lokaal gaan draaien?* in dit hoofdstuk zullen de resultaten van het onderzoek worden benoemd.

Cloud

Om te weten of het systeem achter de StemApp in de cloud of lokaal moet draaien is er informatie gevraagd aan Forus. Volgens een gesprek met (Forus, 2018) heeft het kindpakket wat zij ontwikkeld hebben de beschikking over een 3 tal servers. Met deze servers kunnen er 80 gezinnen gebruik maken van het systeem zonder problemen. Het huidige systeem kan 80 transacties per seconde aan(Forus, 2018). En de transacties die richting de ethereum node gaan worden op dit moment in een wachtrij gezet.
Forus gebruikt drie servers in een cloudomgeving. Deze drie servers zijn bij TransIP gehost.

Volgens (Valley, 2016) biedt de cloud veel mogelijkheden tot opschaling doordat er de mogelijkheid is om een andere server te kiezen bij de cloud provider die bijvoorbeeld meer capaciteit heeft en meer rekenkracht. Wanneer dat het na het draaien van een test niet genoeg rekenkracht of capaciteit is het belangrijk dat dit makkelijk kan worden opgeschaald om zo een succesvolle pilot uit te voeren.
De cloud neemt verder geen ruimte in beslag, zo hoeven er geen eigen servers worden aangeschaft. er hoeft ook niet gedacht te worden aan extra stroom die er nodig zou zijn voor fysieke servers.

Verder is er een grote afhankelijkheid van de cloudprovider zo is de hardware en infrastructuur niet in eigen beheer, er kan bijvoorbeeld de mogelijkheid ontstaan dat de cloud provider later stadium niet geschikt blijkt voor de app. Wanneer dit gebeurt moet er wel goed onderzocht zijn of de data die in de cloud staat gemakkelijk terug te krijgen is, anders gaat dit verloren bij de cloudprovider.
Omdat de uiteindelijke pilot al vrij snel zal moeten plaatsvinden zou de cloud ook een goede oplossing zijn, omdat er hier volgens Valley al binnen een aantal weken de applicatie live kan zijn en gebruikt kan worden.

Lokaal

Om te onderzoeken of er misschien voor de pilot toch beter lokale servers gebruikt kunnen worden is er gekeken naar een blogpost online deze gaat over de redenen om beter niet voor de cloud te kiezen.

De eerste en gelijk het meest belangrijkste punt van het lokaal draaien van de StemApp is dat er volgens (Valley, 2016) *"De belangrijkste redenen om workloads in het datacenter te houden hebben te maken met zorgen over de data. Specifieke aandachtspunten zijn: informatiebeveiliging, data privacy c.q. wet- en regelgeving en bedrijfsbeleid."* Omdat de StemApp gebruik wordt gemaakt van belangrijke en privacygevoelige informatie van mensen zou er voor de pilot een keuze kunnen worden gemaakt voor lokaal.

Als de omgeving in de cloud draait worden er wel hogere kosten gevraagd wanneer er meer resources nodig zijn. Als de omgeving lokaal gedraaid gaat worden dient er een stabiele snelle verbindinding aanwezig te zijn en moeten de benodigde resources ook aanwezig zijn. Het upgraden van lokale resources is tevens ook arbeidsintensiever. Er moet dan vaak een ICT dienst gevraagd worden om meer resources toe te wijzen, voor het fysiek toevoegen van resources dient er nieuwe hardware te worden aangeschaft en ook dit moet door de betreffende ICT dienst gedaan worden.

Security

In dit hoofdstuk wordt antwoord gegeven op de volgende onderzoeksvraag: "*Hoe is de security geregeld in de StemApp-omgeving?*". In bepaalde onderdelen wordt ook naar de Me-App gerefereerd, omdat dit de centrale applicatie is waaraan de StemApp verbonden is. De focus ligt op de mogelijkheden die relevant geacht worden voor de pilot richting het einde van periode 4, wanneer de StemApp getest zal worden in een wijk of dorp in de gemeente Emmen.

Doordat er op het moment van de pilot nog geen werkende blockchain omgeving is wordt er gebruik gemaakt van een SQL database voor de back-end van de applicatie. Dit heeft de maken met het feit dat de technologie van Ethereum op dit moment nog niet ver genoeg is om het geheel naar wens te kunnen laten functioneren. Wanneer dit wel het geval is kan de database worden vervangen voor een back-end dat op de blockchain draait.

Het beveiligen van een SQL database/server kan op verschillende manieren volgens UC Berkeley (Berkeley University of California, z.d.) en UPGuard (UpGuard, Inc., 2017):

- Indien er wachtwoorden worden gebruikt, kunnen deze gehasht (versleuteld) worden volgens PHP.net *(PHP Group, z.d.)*;
    - Dit houdt in dat het door de gebruiker ingevoerde wachtwoord omgezet wordt in een reeks willekeurige tekens. De gebruiker kan dan gewoon met zijn/haar normale wachtwoord inloggen, doordat er gekeken wordt of het door de gebruiker ingevoerde wachtwoord overeenkomt met de sleutel. Er zijn hiervoor verschillende algoritmen die ieder hun eigen manier van versleutelen hebben. Uit de broncode van de Me-App is gebleken dat er hier gebruik wordt gemaakt van het Blowfish algoritme. Deze versleuteld het wachtwoord achter een reeks van 60 tekens.

- Verwijder onnodige features van je DB server;
    - MSSQL en MySQL hebben veel extra features die je waarschijnlijk niet zult gebruiken. Iedere feature die je verwijderd (of niet installeert) is één potentiële ingang minder voor mensen met kwade bedoelingen. Mocht je toch iets willen testen is het handig om dit op een test-/ontwikkelomgeving te gaan doen.

- De database versie up-to-date houden;
    - Voor zowel MSSQL als MySQL worden regelmatig (security) patches gereleased. Deze patches bevatten regelmatig fixes tegen kwetsbaarheden die bekend zijn. Het is aan te raden om deze security patches tijdig te installeren.

- Bescherming tegen SQL injecties. Dit is het plaatsen van SQL queries op plekken waar enkel data hoort;
    - Gebruik maken van Prepared Statements. Dit zijn SQL queries die als het ware klaar staan om uitgevoerd te worden indien de parameters kloppen. Deze parameters zijn placeholders voor de invoer van de gebruiker. De invoer wordt gebonden aan een variabele en wordt per definitie niet door de database uitgevoerd;

    - String escaping. Dit is het vervangen van tekens met een bepaalde betekenis in een programmeertaal door andere tekens die geen speciale betekenis in deze programmeertaal hebben. Dit gebeurt vaak door er een “\” voor te zetten;

    - Gebruik maken van Stored Procedures. Deze methode lijkt behoorlijk op prepared statements. Het is een samenvoeging van enkele SQL statements die je tegelijkertijd aanroept met de naam van de stored procedure. Ook hier wordt gebruik gemaakt van parameters waarin de invoer van de gebruiker komt.

- Gebruik maken van data encryptie;
    - Dit is het versleutelen van de data die in je database staat / komt te staan. De data is vrijwel nutteloos wanneer de toetreder niet beschikt over de sleutel of het wachtwoord.

- Back-ups maken en beschermen;
    - Het maken van back-ups is uiteraard erg handig, maar soms wordt er vergeten dat ook hier een potentieel lek is. De back-up kan eventueel geëncrypt worden of er kunnen restricties op de toegankelijkheid gelegd worden.

- Restricties op de toegankelijkheid en permissies zetten;
    - Dit zorgt ervoor dat enkel bepaalde mensen en/of rollen toegang hebben tot (bepaalde onderdelen van) de database en hierin acties kunnen uitvoeren. Hoe streng deze restricties zijn is afhankelijk van hoe veilig de database dient te zijn.

- Database niet benaderbaar maken via het internet;
    - Door gebruik te maken van een SSH key (Secure Shell key) benader je de host via een shell in plaats van het internet. Hierdoor is het niet mogelijk om via het internet afgeluisterd te worden.

- Monitorings- en anti-spam tools installeren.
    - Er zijn verschillende tools te installeren voor je server die er voor zorgen dat je toezicht kan houden op bepaalde dingen of spam en andere onnodige zaken tegen kan gaan.

Ook de eindgebruiker zelf kan bij het gebruik van de Me-App de veiligheid waarborgen door:

- Het aanwijzen van Delegates binnen de Me-App;
    - Dit zijn personen die je als gebruiker kunt aanwijzen door ze een QR-code te laten scannen. Het scannen van deze code geeft deze personen de autoriteit om jouw identiteit te bevestigen wanneer je de toegang tot je wallet verliest (door het kwijtraken van je toestel bijvoorbeeld). Zo raak je nooit de toegang tot jouw wallet, de plek waar jouw bezittingen in staan, kwijt.
- Het bevestigen van de identiteit door “handtekeningen” verkrijgen.
    - Het idee van Forus is dat Me-App met een systeem gaat werken dat data vanuit andere omgevingen kan gebruiken. Één van deze omgevingen is DigiD. Door je persoonlijke gegevens (waarvan een aantal alleen jij hoort te weten) in te voeren, kan DigiD een bevestiging plaatsen. Op deze manier wordt bevestigd dat de wallet daadwerkelijk tot jou behoord en dat het niet iemand anders is die zich onder jouw naam registreert.

De applicatie waarborgt de veiligheid doordat het zich in een decentrale omgeving bevindt. Jouw identiteit en gegevens binnen de wallet komen op de blockchain terecht. Door de decentrale omgeving kijkt iedere gebruiker naar hetzelfde en is het ongezien veranderen van gegevens niet mogelijk.

Voor de server(s) heeft Stichting Forus de volgende mogelijke maatregelen aangegeven:

- Gebruik maken van een back-up server;
    - Wanneer de hoofdserver door hardware- of softwareproblemen uitvalt, is het de bedoeling dat een back-up server er voor zorgt dat de omgeving draaiende blijft. Het is aannemelijk dat de Me-App voortdurend zal draaien, terwijl de Stem-App enkel op nodige momenten zal draaien. Dit valt buiten de scope van het onderzoek, maar kan eventueel worden meegenomen in het besluit voor de pilot.

- De omgeving op de cloud draaien;
    - Stichting Forus heeft de projectgroep aangeraden om een of meerdere cloud server(s) van TransIP te gebruiken, Dit bedrijf heeft namelijk goede service en support. Daarnaast is een cloud server schaalbaar en biedt TransIP bescherming tegen DDoS aanvallen (zie bijlage 1).

Conclusie en advies

Dit hoofdstuk bevat de conclusie voor het gehele onderzoek. De hoofdvraag en de deelvragen worden herhaald en beantwoord. Daarnaast is er aan het eind nog een advies van de projectgroep te vinden.

Conclusie

Hieronder zijn alle deelvragen overzichtelijk opgesteld met het uiteindelijke onderzoeksresultaat. Daarna volgt er een slotstuk met de beantwoording van de hoofdvraag en de uiteindelijke conclusie bij deze hoofdvraag.

Deelvragen en hun resultaten:

- Hoe werkt de StemApp?
  - Resultaat: De huidige StemApp (Me-App) werkt op een “traditionele omgeving” waarbij er gebruik gemaakt wordt van een SQL database.
- Wat is de schaalbaarheid van de StemApp?
  - Resultaat: Door middel van het gebruik van een server node worden berekeningen doorgevoerd en wordt de data opgeslagen. De server zal zoveel resources gebruiken als deze nodig heeft.
- Welke resources zijn er nodig om de StemApp te kunnen gebruiken om hier een test mee uit te kunnen voeren?
  - Resultaat: Om een test uit te voeren met de huidige StemApp (Me-App) zouden er 2 servers (cloud of lokaal) beschikbaar moeten komen. Een voor de front-end(Website/app) en een voor de back-end (SQL-Server).
- Moet de omgeving in de cloud of lokaal gaan draaien?
  - Resultaat: Het meest gunstige scenario is dat de omgeving in de cloud gaat draaien, dit komt omdat er veel meer mogelijkheden zijn met betrekking op schaalbaarheid, een keerzijde hiervan is dat alles afhankelijk is van de cloud provider.
- Hoe is de security geregeld in de StemApp-omgeving?
  - Resultaat: Stichting Forus doet al aardig veel aan het beveiligen van de SQL server. Er nog kunnen nog een aantal dingen gedaan worden, maar desondanks is de database al behoorlijk veilig te noemen. De andere servers die eventueel gebruikt worden zijn voldoende veilig door het gebruik van een SSH authkey en een aantal handige applicaties.

Tot slot bevindt zich hieronder de hoofdvraag met de uiteindelijke conclusie:

Hoofdvraag: ***”Hoe richt men een omgeving in met betrekking tot blockchain, die geschikt is om te gebruiken voor het houden van een pilot in een wijk of dorp in de gemeente Emmen, waarbij gestemd kan worden over een lokaal besluit?”***

Conclusie: De omgeving kan voor de pilot het beste in de cloud gedraaid worden. De reden hiervan is dat dan de gehele omgeving schaalbaar kan worden gemaakt en er niet hoeft te worden omgekeken hardware onderhoud en het fysiek toevoegen van hardware. Wanneer er in een Cloud omgeving extra resources nodig zijn kan dat simpelweg via het beheerdersportaal van de Cloudprovider.

Advies

Met de gadegeslagen bronnen volgt het volgende advies:
Er wordt getracht de Me-App te gebruiken voor de beheerders zodat het voor de gebruikers makkelijker is en er maar één app voor de gebruiker benodigd is om te stemmen. De omgeving kan het beste in de cloud worden gedraaid zodat er veel meer mogelijkheden zijn om de applicatie schaalbaar te maken, tevens worden er op dit gebied passende veiligheidsmaatregelen getroffen omtrent de privacy van de burger. Binnen de SQL omgeving zullen er nog een paar beveiligingen moeten komen om te voorkomen dat valse data geïnjecteerd wordt.

Bijlages

Bijlage 1

DDoS bescherming van TransIP. (TransIP, z.d.)

Wanneer onze monitoringsystemen een DDoS-aanval (Distributed Denial of Service) detecteren van meerdere Gbit/s dan zullen wij automatisch je IP-adres 'nullrouten'. Dit geldt niet voor een DoS-aanval (Denial of Service), waarbij wij het aanvallende IP-adres blokkeren in onze firewall of bij aanvallen tot enkele Gbit/s omdat wij in dat geval dit nog automatisch kunnen filteren.
Dit kent echter limieten en in een dergelijke situatie zijn wij genoodzaakt het aangevallen IP-adres te nullrouten. Bij een 'nullroute' wordt je IP-adres gerouteerd naar een niet bestaand doel / route waardoor alle pakketjes bestemd voor dat IP 'gedropt' worden in plaats van op de server terecht komen.
Dit betekent wel dat dit IP-adres, zolang deze genullroute is, niet langer van buitenaf bereikbaar is. Dat is uiteraard vervelend voor 'legitieme' bezoekers, want deze kunnen geen websites of services op het betreffende IP meer bezoeken.

Wat kun je zelf doen om de risico's en impact van een DDoS te beperken?

- Draai (populaire) websites achter een oplossing zoals 'Cloudflare'. Dit zal het daadwerkelijke IP-adres van de website 'verbergen' via de nameservers van Cloudflare waardoor je server moeilijker aangevallen kan worden. Het biedt echter geen 100% garantie, omdat slimme aanvallers via een omweg soms alsnog het IP-adres kunnen achterhalen. Let er dan ook op dat je subdomeinen achter Cloudflare plaatst, zodat niet via een subdomein het daadwerkelijke IP-adres van een website achterhaald wordt.
- Draai je websites op een ander IP-adres dan het hoofd IP-adres van je VPS. Als je alle diensten op hetzelfde IP-adres draait dan zal je VPS meteen in zijn geheel niet meer bereikbaar zijn via IPv4, alleen nog via IPv6.
- Ook bij applicaties / services welke een grotere kans lopen om door kwaadwillende aangevallen te worden, zoals Minecraft-servers, IRC-servers en Teamspeak-servers, is het verstandig om dit op een extra IPv4-adres te draaien.
- Draai niet te veel websites op 1 IP-adres. Hoewel technisch gezien geen enkel probleem, neemt met elke website op het IP-adres de kans op een DDoS wel toe. Daarnaast is dit ook handig om de impact van blacklist-problematiek te verminderen wanneer een website bijvoorbeeld gehackt wordt en hier 'spam' vanaf verzonden wordt.

Bronnen

TechTarget, Rouse, M., & Gerwig, K. (2016, augustus). Network Node. Geraadpleegd van https://searchnetworking.techtarget.com/definition/node

Adobe Systems Inc.. (z.d.). About. Geraadpleegd van https://phonegap.com/about/

J.P. Morgan. (z.d.). Quorum. Geraadpleegd van https://www.jpmorgan.com/global/Quorum

Cointelegraph. (z.d.). What is Bitcoin Mining. Geraadpleegd van https://www.marqit.nl/wat-is-loadbalancing

ConsenSys. (z.d.). Geraadpleegd van https://new.consensys.net/

Computerworld, & V Tuil, K. (z.d.). Wat is een API? Geraadpleegd van http://computerworld.nl/development/74796-wat-is-een-api

Computerworld, & V Tuil, K. (z.d.). Wat is SQL? Geraadpleegd van http://computerworld.nl/development/73917-wat-is-sql

Computerworld, & V Tuil, K. (z.d.). Wat is een SQL injectie? Geraadpleegd van http://computerworld.nl/security/75015-wat-is-een-sql-injectie

Forus. (2018). *Code Review StemApp - Forus*. Geraadpleegd van https://drive.google.com/drive/folders/1FVGDBtRi-qEqNZlTFTtVDqc6V0PWTGBJ

Valley. (2016, 22 december). 8 REDENEN OM VOOR DE CLOUD TE KIEZEN [Blogpost]. Geraadpleegd op 30 maart 2018, van https://www.atvalley.nl/8-cloud-redenen/

Forus. (2018, 27 maart). [Antwoord op vragen] [Forumpost]. Geraadpleegd op 2 april 2018, van https://chat.forus.io/channel/questions

[Is een bedrijf/organisatie dat een API heeft ontwikkeld speciaal voor Ethereum blockchain en IPFS.]. (z.d.). Geraadpleegd op 2 februari 2018, van https://infura.io/

11 steps to secure SQL. (2017, 1 mei). Geraadpleegd op 3 april 2018, van https://goo.gl/qVrXHx

Database Hardening Best Practices | Information Security and Policy. (z.d.). Geraadpleegd op 3 april 2018, van https://goo.gl/5q98VK

PHP: password_hash - Manual. (z.d.). Geraadpleegd op 3 april 2018, van https://goo.gl/pui5gr

TransIP | Knowledge Base - Het beperken van de impact van een DDoS-aanval. (z.d.). Geraadpleegd op 3 april 2018, van https://www.transip.nl/knowledgebase/artikel/229-beperken-van-impact-van-een-ddos-aanval/