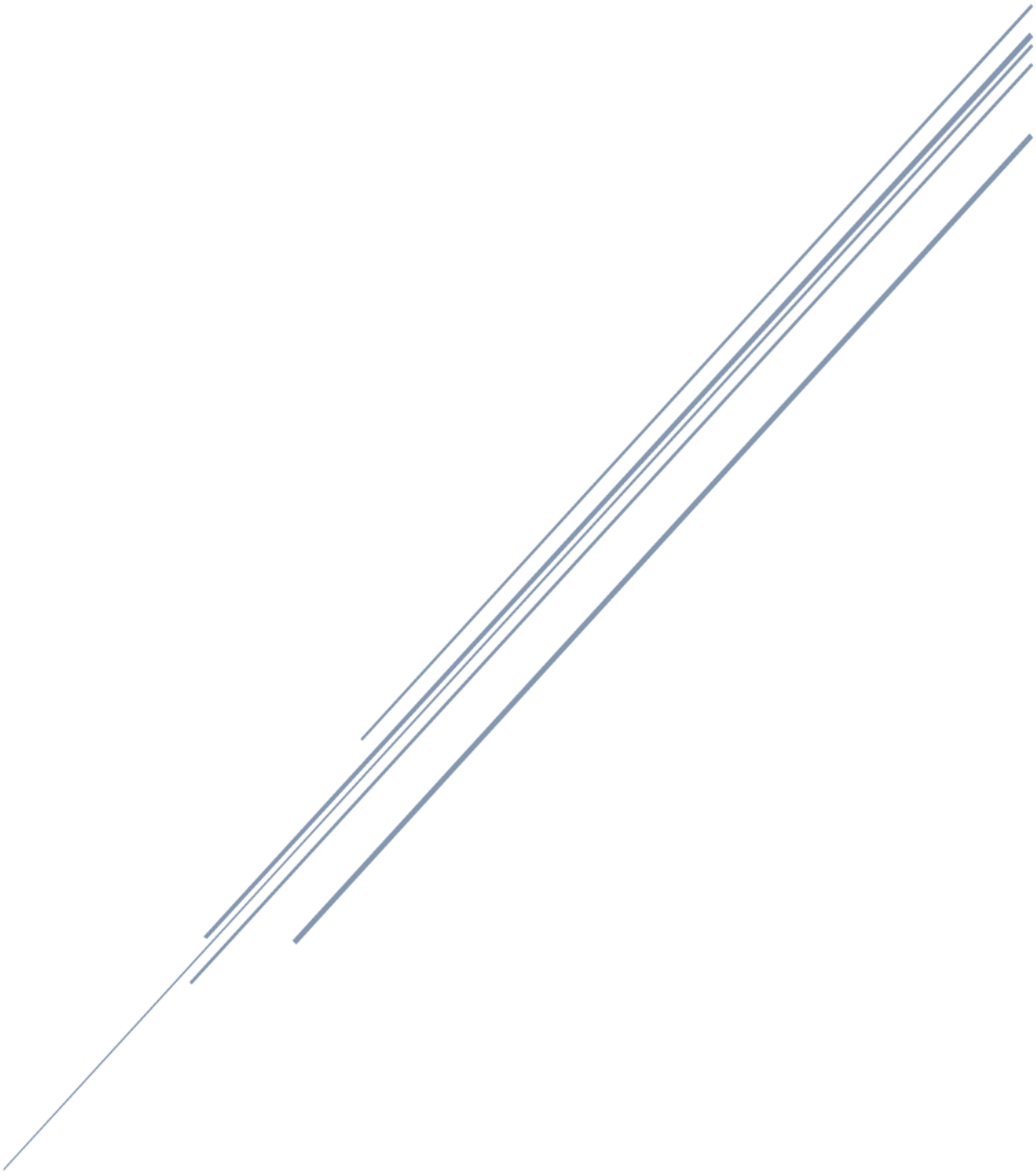
ADVIESRAPPORT

Adviezen voor de Sarea Applicatie



Hanzehogeschool Groningen

ITV-2F

Project IT-Security

16-04-2020

10.2.e. (10.2.e.

10.2.e. 10.2.e.

10.2.e. 10.2.e.

10.2.e. 10.2.e.)

Inhoudsopgave

1. Voorwoord

In de derde periode van ons tweede studiejaar aan de Hanzehogeschool te Groningen hebben wij een project gekregen waarbij de projectgroepen advies moeten geven aan echte bedrijven. Tijdens de Kick-off van het project kwam 10.2.e. vertellen over Sarea. Het verhaal van 10.2.e. en Sarea sprak ons erg aan waardoor Sarea ook in onze top 3 van opdrachtgevers kwam. Uiteindelijk kregen wij als groep Sarea toegekend. Dit betekende dat wij voor Sarea onderzoek mochten doen naar de veiligheid en alles daaromheen.

Voor ons als groep geeft het een goed gevoel dat wij advies mogen uitbrengen voor een idee die de maatschappij vooruit zal gaan helpen. Sarea zal ervoor zorgen dat met de middelen (Mobiele telefoon) die bijna ieder persoon heeft de zoekacties gecoördineerd verlopen, wat als positief gevolg heeft dat een vermist persoon waarschijnlijk eerder zal worden gevonden.

Wij willen voor dit project graag gebruik maken van de mogelijkheid om een aantal mensen bedanken, zonder hen zouden wij dit adviesrapport niet tot stand kunnen hebben laten komen.

Wij willen graag bedanken:

10.2.e., voor de kennis en vaardigheden die wij hebben opgedaan tijdens de practica van Beveiliging & Techniek.

10.2.e., voor de kennis die wij hebben opgedaan tijdens de hoorcolleges van Beveiliging & Techniek.

10.2.e., voor de kennis en vaardigheden die wij hebben opgedaan tijdens de hoorcolleges en de practica van Beveiliging & Organisatie.

10.2.e., voor de kennis en vaardigheden die wij hebben opgedaan tijdens de practica van de communicatieve onderdelen binnen het project en ook voor de aanbevelingen en feedback tijdens de tutorgesprekken van het project.

10.2.e. voor de aanbevelingen en feedback tijdens de tutorgesprekken van het project.

10.2.e., voor het beschikbaar stellen van documenten en toegang tot onderdelen van Sarea, de gespreken en de feedback op onze aangeleverde documenten.

Groningen, 16 april 2020

10.2.e., 10.2.e., 10.2.e. en 10.2.e.

2. Inleiding

Het is ieders grootste angst, een vermissing van een bekende of een geliefde. Bij een vermissing zijn de eerste uren cruciaal bij het terugvinden van een vermist persoon. Sarea is een project van het innovatiehuis politie die wil helpen met het snel opzetten van een zoektocht. In dit rapport wordt er gekeken naar mogelijke beveiligingsrisico's binnen de bestaande opzet van de Sarea applicatie.

Als eerste zal er gekeken worden naar de Stakeholders/Assets en interviewschema om concreet te krijgen wat er verwacht wordt binnen dit project. Hierna wordt er gekeken naar een risicoanalyse, hierin wordt gekeken naar de mogelijke risico's binnen de Sarea applicatie. Naar aanleiding van deze risicoanalyse wordt hierna een threat model gemaakt. Op basis van de risicoanalyse en threat model wordt een testplan en taakverdeling gemaakt.

Als laatste wordt gekeken naar de analyse van de verschillende onderdelen benoemt in het testplan. Er wordt onder andere gekeken naar veiligheidsrisico's binnen de GPS, databeveiliging, datacommunicatie, de organisatorische kant van de applicatie, de database en de authenticatie van de Sarea applicatie en infrastructuur.

3. Stakeholders/Assets & Interviewschema

3.1 Stakeholders

- Innovatiehuis politie

3.2 Assets

- Mobiele applicatie
- Website
- Database

3.3 Interviewschema

In dit onderdeel wordt er gekeken naar het opgestelde interview schema die gebruikt is voor het achterhalen van de requirements van dit project.

Hoofdthema

De concrete opdracht

Subthema: Sarea/Algemene informatie

- Wat is het specifieke doel voor Sarea? (Zorgen dat het doel van de applicatie duidelijk is zodat er beter gekeken kan worden naar de veiligheid van de key-aspects binnen het project)
- Op welke manier wordt dit bereikt?
    - Specifieke technieken?
- Is er al nagedacht over de veiligheid van de applicatie? (Welk werk is er al gedaan zodat er geen dubbel werk wordt verricht)
- Op welke manier zien jullie/zit u ons in deze opdracht? (Concreter beeld krijgen van de verwachtingen vanaf hun kant)
- Wanneer willen jullie/wilt u de applicatie live hebben? (Tijdsframe/deadline vraag)

Subthema: Sarea App

- Hoe krijgt een gebruiker toegang tot de app? (inloggen/registreren?)
- Wat voor informatie is er zichtbaar voor een gebruiker tijdens het gebruiken van de app?
- Waar wordt informatie opgeslagen?
- Wordt deze informatie beveiligd? (met encryptie?)
- Hoe wordt een locatie van een gebruiker verkregen? (GPS en/of mobiel netwerk)(Controle of locatie wel daadwerkelijk klopt)

Subthema: Classificatie van gegevens

- Welke gegevens van gebruikers verwachten jullie te gebruiken en in hoeverre moeten deze beschermd worden?
- Welke gegevens van de politie gebruiken jullie en hoe moeten deze beschermd worden?
- Zijn er al risico's voor de gebruikers data gevonden?
- Is er een beleidsdocument waarin het beleid staat omtrent de informatie die de app verzameld? (beleidsdocument)
- Hoe houdt de politie rekening met de rechten voor databescherming van de burger en hoe kan de burger aanspraak maken op AVG/GDPR?

Subthema: Organisatorisch

- Wie binnen de politie is verantwoordelijk voor Sarea?
- Wie binnen de politie heeft rechten tot het gebruik van Sarea?
- Hoe wordt er om gegaan met de gegevens van de gebruikers? (Hoe wordt het opgeslagen, is er back-up etc.)

- Zijn er verschillende rechten tot het gebruik van de app (Hebben er binnen de politie verschillende posities verschillende rechten?)
- Hoe maakt de politie gebruik van de app i.v.m. communicatie?

4. Risicoanalyse

Risicomatrix

Kans \ Potentiele consequenties	Niet significant	Klein	Redelijk	Groot	Enorm
Bijna zeker	Medium	Hoog	Erg hoog	Erg hoog	Erg hoog
Waarschijnlijk	Medium	Hoog	Hoog	Erg hoog	Erg hoog
Mogelijk	Laag	Medium	Hoog	Hoog	Erg hoog
Onwaarschijnlijk	Laag	Laag	Medium	Medium	Hoog
Zeldzaam	Laag	Laag	Laag	Laag	Medium

Legenda

Kans

- Bijna zeker: 1x per maand
- Waarschijnlijk: Tussen 1x per 3 maanden en 1x per maand
- Mogelijk: Tussen 1x per half jaar en 1x per drie maanden
- Onwaarschijnlijk: Tussen 1x per jaar en 1x per half jaar
- Zeldzaam: Minder dan 1x per jaar

Potentiele consequenties

- Enorm: Data kan uitlekken en de integriteit kan niet meer gewaarborgd worden.
- Groot: Werkzaamheden kunnen stilliggen of confidentiële data kan uitlekken.
- Redelijk: Het ondervinden van (tijdelijke) hinderingen in beperkte groepen.
- Klein: De dienst draait, maar mogelijk langzamer.
- Niet significant: Zowel de applicatie als de gebruikers ondervinden nauwelijks tot geen hinder.

GPS

Iemand kan doen alsof hij/zij ergens heeft gezocht terwijl dit niet zo is.

- Kans: Onwaarschijnlijk. Er zij weinig redenen om deze informatie te vervalsen.
- Consequenties: Groot. Niet integere gps-data kunnen de zoekers laten geloven dat ergens al gezocht is, terwijl dat niet zo is. Dit zou de zoekactie kunnen remmen of zelfs belemmeren
- Risico: Medium

Iemand kan ergens gezocht hebben, maar het laten lijken dat dit niet zo is geweest.

- Kans: Zeldzaam. Er is geen reden voor een kwaadwillige om dit te doen, want een kwaadwillende zal hoogstwaarschijnlijk niet meedoen aan een zoekactie.
- Consequenties: Klein, omdat er altijd nog de kans bestaat dat er met een spoor geknoeid kan worden.
- Risico: Laag

Er kunnen mogelijk GPS-jammers gebruikt worden om het signaal te verstoren.

- Kans: Zeldzaam, omdat dit duidelijke verstoring is en het makkelijk op te sporen valt, wat dit een zeer makkelijk traceerbare interruptie maakt.
- Consequenties: Groot, omdat de zoekactie tijdens de interruptie stilligt maar wel weer direct te hervatten valt.
- Risico: Laag

Databeveiliging

Als iemand ongewenste toegang heeft tot de database dan kan hij/zij data aanpassen.

- Kans: Mogelijk, omdat het motief voor een potentiele aanvaller erg hoog kan zijn terwijl de beveiliging moeilijk helemaal veilig te verklaren valt.
- Consequenties: Enorm omdat met deze toegang alle data van gebruikers, onderzoeken en meer aan te passen valt. Ook is deze breuk aan confidentialiteit een data lek.
- Risico: Erg hoog

Iemand met meer rechten op de backend zou informatie/data kunnen geven aan personen die hier geen rechten voor hebben.

- Kans: Waarschijnlijk, mensen die meer rechten krijgen zullen wel aardig gescreend kunnen worden, maar toch zijn mensen slecht in het verborgen houden van informatie. Hierdoor is intentioneel of niet intentioneel de kans zeker wel aanwezig.
- Consequenties: Groot, omdat weinig gebruikers toegang tot veel meer informatie hebben maar deze kan wel confidentieel zijn en gecategoriseerd worden als datalek.
- Risico: Erg hoog

Als de server een IO-bottleneck bereikt heeft zal de data minder goed beschikbaar zijn.

- Kans: Mogelijk wanneer de dienst erg veel gebruikt wordt. Ook bestaat een kleine kans dat een kwaadwillige dit intentioneel kan doen.
- Consequenties: Klein omdat dit het onderzoek een beetje kan vertragen maar het verder een lage impact heeft.
- Risico: Medium

Als een harde schijf van de database corrupt raakt dan is het systeem tijdelijk buiten dienst.

- Kans: Zeldzaam, wanneer de database op een goede array draait deze dan gewoon door kan, wanneer dit niet zo is de kans bijna zeker.
- Consequenties: Groot omdat alle data hierbij verdwijnt voor een korte of tijd of voor altijd en de dienst niet beschikbaar is.
- Risico: Laag/Erg hoog afhankelijk van de inrichting van de DB-server.

Datacommunicatie

Een gebruiker kan zich voordoen als een coördinator

- Kans: Mogelijk, door het onderscheppen van het token van een coördinator kan de aanvaller zich verifiëren als de coördinator.
- Consequenties: Groot. Als een aanvaller zich voordoet als een coördinator kan de aanvaller vervalste informatie goedkeuren en/of correcte informatie verwijderen/aanpassen.
- Risico: Hoog

Data kan onderweg onderschept worden en gewijzigd worden

- Kans: Mogelijk, omdat ondanks dat het motief van een kwaadwillige hiervoor groot kan zijn, deze aanval moeilijk uit te voeren is, echter is dit afhankelijk van de encryptie.
- Consequenties: Groot, omdat hiermee data kan lekken en gewijzigd kan worden.
- Risico: Hoog

Confidentiële data kan uitgelekt worden

- Kans: Mogelijk, omdat er veel scenario's met een kleinere kans zijn waar zich dit voor kan doen.
- Consequenties: Groot, omdat het lekken van confidentiële data een breuk aan vertrouwen is.
- Risico: Hoog

Communicatie van of naar de dienst kan geblokkeerd worden

- Kans: Mogelijk, omdat de aanval enigszins doenbaar is in het veld en hier af en toe wel een motief van een kwaadwillige voor te vinden kan zijn.
- Consequenties: Redelijk, omdat dit wel een impact kan hebben op 1 of meer zoekacties afhankelijk van hoeveel mensen hiervan last ondervinden ook al is fenomeen tijdelijk.
- Risico: Hoog

Iemand kan claimen tot de Sarea infrastructuur te behoren

- Kans: Zeldzaam. De kans dat iemand zich als infrastructuur voordoet is klein.
- Consequenties: Enorm. Mocht iemand zich als infrastructuur voor doen kan deze hier niet direct blijvende schade aanrichten. Wel kan iemand hier mogelijk informatie mee kunnen ontfutselen.
- Risico: Medium

Een gebruiker kan zich voordoen als een andere zoeker

- Kans: Zeldzaam. Mensen kunnen via een netwerk de gegevens van anderen onderscheppen, bekijken en wijzigen.
- Consequenties: Klein. Als de aanvaller inloggegevens of het token van een andere gebruiker kan onderscheppen kan deze zich voor doen als deze persoons of onjuiste informatie leveren aan zowel de gebruiker als de server.
- Risico: Laag

Organisatorisch

Een gebruiker kan een rol met te veel bevoegdheden bemachtigen

- Kans: Onwaarschijnlijk. Er zal hoogstwaarschijnlijk een goede screening proces vooraf het selecteren zitten van een coördinator.
- Consequenties: Enorm. Als een gebruiker bijvoorbeeld de rol krijgt van een coördinator dan kan de aanvaller bijvoorbeeld aanwijzingen verwijderen of aanpassen en dit heeft een grote impact op de zoektocht
- Risico: Erg Hoog.

Een coördinator kan een aanwijzing aanpassen of verwijderen

- Kans: Redelijk. Dit zou een coördinator niet snel doen, wel mogelijk een aanvaller die zich voordoet als coördinator. Wel is deze aanval heel makkelijk uit te voeren.
- Consequenties: Groot. Het aanpassen of verwijderen van een aanwijzing kan het onderzoek remmen of stopzetten
- Risico: Hoog

Een coördinator kan een foute aanwijzing goedkeuren

- Kans: Waarschijnlijk. Een aanvaller of coördinator krijgen waarschijnlijk veel aanwijzingen binnen en er is een grote kans dat niet alles even relevant is voor de zoektocht.
- Consequenties: Redelijk. Een foute aanwijzing zou de zoektocht even op een dwaalspoor kunnen brengen, maar is niet zo erg als het verwijderen van een aanwijzing.
- Risico: Hoog

Een coördinator kan gevoelige informatie lekken over aanwijzingen of andere gevoelige zaken.

- Kans: Mogelijk. Dit is mogelijk als de aanvaller bijvoorbeeld de rol krijgt van coördinator. Of als de coördinator
- Consequenties: Groot. Informatie van de zoektocht is hoogstens vertrouwelijk en specifieke dingen als aanwijzingen of gegevens over de vermiste mogen niet gelekt worden.
- Risico: Hoog

Een type gebruiker kan mogelijk meer permissies hebben dan benodigd

- Kans: Onwaarschijnlijk. Dit zou dan een fout in het design zijn en dit is niet iets wat snel onopgemerkt blijft.
- Consequenties: Groot. Dit is afhankelijk van de permissies die een gebruiker erbij krijgt, wordt de gebruiker bijvoorbeeld opeens een coördinator in het onderzoek dan veranderd de consequentie naar enorm.
- Risico: Medium

Een gebruiker kan zich voordoen als een gebruiker met andere rechten.

- Kans: Onwaarschijnlijk. Het voordoen als een gebruiker met andere rechten heeft in deze context niet zoveel zin, want de aanvaller schiet er niet veel mee op, aangezien hij niet deze extra rechten ook daadwerkelijk heeft.
- Consequenties: Klein. Er zijn mogelijk zoekers die in de spoof kunnen vallen, maar dit zullen hoogstwaarschijnlijk niet veel zijn. Dit is ook makkelijk te ontdekken
- Risico: Laag

Een coördinator kan gegevens inlezen van gebruikers waartoe hij niet bevoegd is

- Kans: Onwaarschijnlijk. De kans dat de coördinator inzicht krijgt in confidentiële gegevens van gebruikers is niet groot, ook aangezien gebruikers niet veel gevoelige gegevens invoeren.
- Consequenties: Klein. De gegevens die gebruikers invoeren zijn niet heel gevoelig.
- Risico: Laag

Database

Een aanvaller zou de backend kunnen spoofen om toegang te verkrijgen tot de database buiten de backend om.

- Kans: Mogelijk, hierbij geldt eigenlijk dezelfde reden als bij de ongewenste toegang tot de database. Het motief kan mogelijk erg hoog zijn, terwijl het wel goed beveiligd is.
- Consequenties: Enorm, omdat alle data uit de database verwerkt kan worden op allerlei verschillende wijzen, denk hierbij aan verwijderen, aanpassen of kopiëren.
- Risico: Erg hoog

Een aanvaller zou via een SQL-Injection bijvoorbeeld een update statement doen waardoor de data wordt aangepast en niet meer integer is.

- Kans: Mogelijk, een aanvaller zou data kunnen aanpassen waardoor de zoekers op een verkeerd spoor gezet worden. Echter, het moet wel lukken om de query uit te kunnen voeren.
- Consequenties: Afhankelijk van de data waarmee geknoeid wordt kunnen de consequenties variëren van redelijk tot en met enorm.
- Risico: hoog tot erg hoog

Logs zouden gemanipuleerd kunnen worden om toegang en wijzigingen te verbergen.

- Kans: Mogelijk. Hierbij geldt dezelfde kans als wanneer iemand data heeft gewijzigd, omdat de kans groot is dat een aanvaller zijn sporen wist als hij/zij toegang kan krijgen tot de logs.
- Consequenties: groot, er kan namelijk minder makkelijk worden nagetrokken wie wat, waar en wanneer heeft aangepast of verwijderd.
- Risico: Erg hoog

Een aanvaller zou via een SQL-Injection een select-statement kunnen uitvoeren en daarmee confidentiële informatie kunnen vrijgeven.

- Kans: Mogelijk, een aanvaller kan op deze manier vrij onopvallend data vrijgeven. Er wordt met een select-statement namelijk geen data aangepast, waardoor het niet erg opvalt dat er ongewenste acties hebben plaatsgevonden.
- Consequenties: groot, er kunnen niet vertrouwelijke gegevens gelekt worden, maar ook wachtwoorden. Het verschilt dus per wat er lekt, maar in het algemeen zijn de consequenties Hoog
- Risico: Erg hoog

Een database dump zou door kwaadwilligen gestolen kunnen worden.

- Kans: Mogelijk, een dump stelen valt minder op dan daadwerkelijk data aanpassen. Het is daarom voor een aanvaller een redelijk gunstige manier om aan gegevens te komen.
- Consequenties: Enorm, de gehele inhoud van een database kan hierdoor gestolen worden, inclusief wachtwoorden.
- Risico: Erg hoog

Wanneer iemand toegang krijgt tot de database kan hij/zij de data vrijgegeven.

- Kans: Mogelijk. Een aanvaller heeft vaak toegang nodig tot de database als hij/zij gegevens wil stelen en mogelijk aanpassen. Het is uiteraard wel afhankelijk van de beveiliging van de database hoe makkelijk dit gaat.
- Consequenties: Enorm, hiervoor geldt eigenlijk hetzelfde als bij de database dump. Er bestaat namelijk een grote kans dat wachtwoorden lekken als iemand toegang heeft tot de database. Bovendien kunnen rechten van andere gebruikers ontnomen worden.
- Risico: Erg hoog

Een aanvaller zou via bijvoorbeeld een SQL-Injection heel veel inserts (toevoegingen) kunnen doen aan de database waardoor deze overbelast raakt, en uiteindelijk een Denial of Service geeft.

- Kans: Waarschijnlijk. Een DDOS-aanval via SQL is niet moeilijk uit te voeren.
- Consequenties: Redelijk. Het tijdelijk niet online zijn van de database kan ervoor zorgen dat de zoekactie wordt vertraagd, maar de database is alleen tijdelijk niet beschikbaar.
- Risico: Hoog

Wanneer de database server direct te adresseren is, bestaat de kans op een traditionele (D)DoS aanval.

- Kans: Waarschijnlijk. Het opzetten van een DDOS aanval is een relatief simpel uit te voeren aanval.
- Consequenties: Redelijk. De server raakt overbelast en delen van, of de gehele dienst kan niet meer geleverd worden waardoor zoekacties potentieel vastlopen.
- Risico: Hoog

Wanneer iemand toegang heeft tot de database kan hij/zij deze verwijderen, waardoor grotendeels de hele service niet meer bruikbaar is.

- Kans: Mogelijk. Alhoewel het lastig kan zijn om toegang tot een database te krijgen is het voor aanvallers met een grote wil zeker niet onmogelijk.
- Consequenties: Enorm. Hierdoor raken alle zoekacties stil en zal de gehele database opnieuw ingericht moeten worden. Als de back-up niet is verwijderd dan zal deze terug moeten worden gezet, wat een tijdelijke Denial of service oplevert.
- Risico: Erg hoog

Een aanvaller zou via een SQL-Injection de database kunnen aanpassen of verwijderen en daarmee meer rechten krijgen dan die daadwerkelijk heeft.

- Kans: Mogelijk. Het uitvoeren van een SQL injection is niet moeilijk en zou makkelijk een database kunnen aanpassen.
- Consequenties: Enorm. Zowel het aanpassen van data als het verwijderen van de data kan een grote invloed hebben op de zoekactie.
- Risico: Erg hoog.

Een aanvaller zou via een SQL-Injection zichzelf rechten kunnen geven zoals de eigenaar van zoekacties

- Kans: Mogelijk. Als Sarea niet beschermt is tegen SQL injections dan is het vrij eenvoudig om een SQL-injection uit te kunnen voeren.
- Consequenties: Groot. Als een gebruiker zichzelf bepaalde rechten kan geven dan kan hij/zij op een gegeven moment ook rechten afnemen van andere gebruikers en mogelijk ook gegevens verwijderen afhankelijk van de rechten die de aanvaller zichzelf heeft gegeven.
- Risico: Hoog

Authenticatie

Een aanvaller kan een MITM-attack uitvoeren om het token van een andere gebruiker te bemachtigen en hiermee zijn eigen identiteit vervalsen.

- Kans: Mogelijk, het uitvoeren van een MITM-attack is niet heel moeilijk maar het is niet per definitie dat er bruikbare data uit wordt behaald.
- Consequenties: Redelijk, Mocht de aanvaller inloggegevens van een andere gebruiker kunnen bemachtigen kan deze gebruikt worden om valse informatie onder iemand anders naam te verschaffen of in het ergste geval goed te keuren als coördinator.
- Risico: Hoog

Een aanvaller kan de authenticatieserver overbelasten door hier vele requests naar te sturen.

- Kans: Waarschijnlijk. Een DDOS-aanval kan makkelijk opgezet worden.
- Consequenties: Redelijk. Een Denial Of Service door een DDOS naar de authenticatie server kan ervoor zorgen dat de dienst tijdelijk niet beschikbaar is maar zal geen blijvende schade veroorzaken.
- Risico: Medium

Een aanvaller kan de authenticatieserver overbelasten door alle connecties op te vragen met een Slow Loris attack.

- Kans: Mogelijk, het kost niet veel kracht om een Slow Loris attack uit te voeren. Maar er moet wel kennis zijn over de connecties die opgehouden worden en hoe groot de pool is.
- Consequenties: Redelijk. Een Denial Of Service door een Slow Loris naar de authenticatie server kan ervoor zorgen dat de dienst tijdelijk niet beschikbaar is maar zal geen blijvende schade veroorzaken.
- Risico: Laag

Door zich te authentiseren als een persoon met hogere rechten dan een aanvaller voorheen had kan deze zijn bevoegdheden uitbreiden.

- Kans: Mogelijk.
- Consequenties: Redelijk.
- Risico: Hoog.

5. Threat model

In dit hoofdstuk wordt er gekeken naar het threat model die gemaakt is met behulp van het STRIDE-model. In de volgende tabellen wordt per onderdeel gekeken welke mogelijke risico's er zijn.

Threat	Eigenschap	Definitie	Voorbeelden
Spoofing (Vervalsen)	Authenticatie	Je voordoen als iets of iemand anders dan jijzelf.	- Een aanvaller die wel is uitgenodigd voor een zoekactie zou zijn/haar GPS-data kunnen aanpassen zodat het lijkt alsof hij/zij al ergens heeft gezocht terwijl dit helemaal niet zo is.
Tampering (Knoeien met data)	Integriteit	Aanpassen van gegevens op de harde schijf, het netwerk, het geheugen of een andere entiteit.	- Het ongeautoriseerd verwijderen of aanpassen van aanwijzingen op de server. - Het aangeven van een aanwijzing die niet correct of integer is.
Repudiation (Verwerping)	Non-repudiability	Beweren dat je iets niet hebt gedaan of niet verantwoordelijk was. Dit kan eerlijk of oneerlijk zijn.	- Mensen die zeggen: "Ik heb deze aanwijzing niet aangeleverd." of "Ik heb daar wel of niet gezocht."
Information disclosure (Vrijgeven van informatie)	Confidentialiteit	Aanleveren van informatie aan iemand niet geautoriseerd voor deze informatie.	- Vindingen van een zoekactie die in te zien zijn door users die niet aangemeld zijn voor de bepaalde zoekactie of andere actoren van buitenaf - Een user die de inhoud kan lezen van de database of op een andere manier confidentiële data inziet. - Een coördinator die bepaalde gegevens die alleen zichtbaar zijn voor een coördinator deelt met 'gewone' gebruikers.
Denial of Service (Weigering van dienst)	Beschikbaarheid	Het crashen van een bepaalde service door het versturen van te veel aanvragen of pakketjes totdat de service het niet meer aankan en uiteindelijk crasht.	- Een aanvaller zou via bijvoorbeeld een SQL-Injection heel veel inserts (toevoegingen) kunnen doen aan de database waardoor deze overbelast raakt, en uiteindelijk een Denial of Service geeft. - Een aanvaller zou heel veel bevindingen of tips tegelijk kunnen sturen mogelijk in combinatie met een script die kan leiden tot een Denial of Service.

Elevation of Privilege (Uitbreiding van bevoegdheden)	Autorisatie	Permissies bemachtigen zonder de benodigde autorisatie.	- Een user zou de rol van coördinator kunnen innemen en zou meer rechten kunnen krijgen tijdens een zoekactie. - Een coördinator zou gevoelige informatie van users kunnen inzien

GPS

Threat	Risk
Spoofing (Vervalsen)	- Iemand kan doen alsof hij/zij ergens heeft gezocht terwijl dit niet zo is. - Iemand kan ergens gezocht hebben, maar het laten lijken dat dit niet zo is geweest.
Tampering (Knoeien met data)	- N.v.t
Repudiation (Verwerping)	- Iemand kan zeggen dat hij/zij ergens wel heeft gezocht terwijl dit niet zo is of andersom.
Information disclosure (Vrijgeven van informatie)	- N.v.t
Denial of Service (Weigering van dienst)	- Er kunnen mogelijk GPS jammers gebruikt kunnen worden om het signaal te verstoren.
Elevation of Privilege (Uitbreiding van bevoegdheden)	- N.v.t

Databeveiliging

Threat	Risk
Spoofing (Vervalsen)	- N.v.t
Tampering (Knoeien met data)	- Als iemand ongewenste toegang heeft tot de database dan kan hij/zij data aanpassen
Repudiation (Verwerping)	- N.v.t
Information disclosure (Vrijgeven van informatie)	- Iemand met meer rechten op de back-end zou informatie / data kunnen geven aan personen die hier geen rechten voor hebben.
Denial of Service (Weigering van dienst)	- Als een harde schijf van de database corrupt raakt dan is het systeem tijdelijk buiten dienst. - Als een harde schijf vol is geraakt dan kan de dienst ook niet meer aangeleverd worden. - Als een onderdeel van de server stuk is dan liggen de zoekacties ook tijdelijk stil. - Als de server een IO bottleneck bereikt heeft zal de data minder goed beschikbaar zijn.
Elevation of Privilege (Uitbreiding van bevoegdheden)	- Als iemand ongewenste toegang heeft dan kan hij/zij de rechten aanpassen van gebruikers, dus potentieel rechten geven aan gebruikers die hiervoor geen rechten zouden moeten krijgen.

Datacommunicatie

Threat	Risk
Spoofing (Vervalsen)	- Een zoeker kan zich voordoen als een andere zoeker - Een zoeker kan zich voordoen als coördinator - Iemand kan claimen tot de Sarea infrastructuur te behoren
Tampering (Knoeien met data)	- Data van zoekers kan onderweg aangepast worden - Data van de servers naar de gebruikers kan onderweg aangepast worden
Repudiation (Verwerping)	- N.v.t
Information disclosure (Vrijgeven van informatie)	- Confidentiële data kan uitgelekt worden - Data kan bemachtigd worden door mensen zonder de autoriteit hiervoor te hebben
Denial of Service (Weigering van dienst)	- Communicatie naar de dienst kan geblokkeerd worden - Communicatie van de dienst kan geblokkeerd worden
Elevation of Privilege (Uitbreiding van bevoegdheden)	- Uitgelekte gegevens kunnen gebruikt worden om permissies van een ander over te nemen - Tamperen/knoeien met de communicatie kan ongewenste permissies opleveren

Organisatorisch

Threat	Risk
Spoofing (Vervalsen)	- Een gebruiker kan zich voordoen als een gebruiker met andere rechten
Tampering (Knoeien met data)	- Een coördinator kan een aanwijzing aanpassen of verwijderen - Een coördinator kan een foute aanwijzing goedkeuren - Een type gebruiker kan mogelijk meer permissies hebben dan benodigd - Een gebruiker met rechten op de data die deze niet nodig heeft kan meer data bemachtigen dan noodzakelijk - Een gebruiker met wijzigingsrechten op data die deze niet nodig heeft kan leiden tot verlies van integriteit van data - Een kwaadwillige gebruiker met rechten tot de data kan deze mogelijk aanpassen
Repudiation (Verwerping)	- Een coördinator kan dingen zeggen als: ”Ik heb die aanwijzing niet gezien of ik heb die aanwijzing niet goedgekeurd”.
Information disclosure (Vrijgeven van informatie)	- Een coördinator kan gegevens inlezen van gebruikers waartoe hij niet bevoegd is - Een coördinator kan gevoelige informatie lekken over aanwijzingen of andere gevoelige zaken. - Een malafide gebruiker met teveel rechten zou informatie kunnen uitlekken
Denial of Service (Weigering van dienst)	- N.v.t
Elevation of Privilege (Uitbreiding van bevoegdheden)	- Een gebruiker kan een rol met te veel bevoegdheden bemachtigen - Een coördinator kan confidentiële gegevens zien van gebruikers

Database

Threat	Risk
Spoofing (Vervalsen)	- Een aanvaller zou de backend kunnen spoofen om toegang te verkrijgen tot de database buiten de backend om.
Tampering (Knoeien met data)	- Een aanvaller zou via een SQL-Injection bijvoorbeeld een update statement doen waardoor de data wordt aangepast en niet meer integer is. - Wanneer iemand toegang tot de database weet te bemachtigen kan hij/zij deze data aanpassen.
Repudiation (Verwerping)	- Logs zouden gemanipuleerd kunnen worden om toegang en wijzigingen te verbergen.
Information disclosure (Vrijgeven van informatie)	- Een aanvaller zou via een SQL-Injection een select statement kunnen uitvoeren en daarmee confidentiële informatie kunnen vrijgeven. - Een database dump zou door kwaadwilligen gestolen kunnen worden. - Wanneer iemand toegang krijgt tot de database kan hij de data vrijgegeven.
Denial of Service (Weigering van dienst)	- Een aanvaller zou via bijvoorbeeld een SQL-Injection heel veel inserts (toevoegingen) kunnen doen aan de database waardoor deze overbelast raakt, en uiteindelijk een Denial of Service geeft. - Wanneer de database server direct te adresseren is, bestaat de kans op een traditionele (D)DoS aanval. - Wanneer iemand toegang heeft tot de database kan hij deze verwijderen, waardoor grotendeels de hele service niet meer bruikbaar is.
Elevation of Privilege (Uitbreiding van bevoegdheden)	- Een aanvaller zou via een SQL-Injection de database kunnen aanpassen of verwijderen en daarmee meer rechten krijgen dan die daadwerkelijk heeft. - Een aanvaller zou via een SQL-Injection zichzelf rechten kunnen geven zoals de eigenaar van zoekacties

Authenticatie

Threat	Risk
Spoofing (Vervalsen)	- Een aanvaller kan een MITM-attack uitvoeren om het token van een andere gebruiker te bemachtigen en hiermee zijn eigen identiteit vervalsen.
Tampering (Knoeien met data)	- Een aanvaller zou zijn JWT kunnen vervalsen door de informatie aan te passen of de sleutel voor de encryptie te bemachtigen en hiermee zijn data in het token aanpassen.
Repudiation (Verwerping)	- N.v.t
Information disclosure (Vrijgeven van informatie)	- N.v.t
Denial of Service (Weigering van dienst)	- Een aanvaller kan de authenticatieserver overbelasten door hier vele requests naar te sturen. - Een aanvaller kan de authenticatieserver overbelasten door alle connecties op te vragen met een slowloris attack.
Elevation of Privilege (Uitbreiding van bevoegdheden)	- Door zich te authentiseren als een persoon met hogere rechten dan een aanvaller voorheen had kan deze zijn bevoegdheden uitbreiden.

6. Testplan & Taakverdeling

In dit hoofdstuk wordt er gekeken naar het testplan en de taakverdeling. Hierbij wordt per onderdeel de verschillende risico's benoemt en op welke manier dit getest gaat worden in dit project.

6.1 Testplan

GPS

Wat testen we?

Hoe er rekening is gehouden met het vervalsen van locatiegegevens.

Ten behoeve van de risico's

Iemand kan doen alsof hij/zij ergens heeft gezocht terwijl dit niet zo is. (Spoofing)

Hoe willen we testen?

Documentatie doornemen en kijken naar de werking.

Welke toegang hebben we hiervoor nodig?

Documentatie van de Sarea Applicatie.

Databeveiliging

Wat testen we? (1)

Hoe goed de database beveiligd is tegen ongewenste toegang van derden.

Ten behoeve van de risico's

Als iemand ongewenste toegang heeft tot de database dan kan hij/zij data aanpassen.

Hoe willen we testen?

- Documentatie
- Alle mogelijke lekken in de documentatie opsporen in de testomgeving
- SQL-injections op de testomgeving uitproberen

Welke toegang hebben we hiervoor nodig?

- Documentatie
- Toegang tot de testomgeving

Wat testen we? (2)

Confidentialiteit van de mensen met rechten op confidentiële informatie.

Ten behoeve van de risico's

Iemand met meer rechten op de backend zou informatie/data kunnen geven aan personen die hier geen rechten voor hebben.

Hoe willen we testen?

- Policies doorlezen op dataconfidentialiteit eisen
- Kijken hoe duidelijk alles wordt aangegeven binnen de applicatie zelf

Welke toegang hebben we hiervoor nodig?

- Documentatie
- Toegang tot de testomgeving

Datacommunicatie

Wat testen we?

De encryptie standaarden en implementatie hiervan binnen de applicatie.

Ten behoeve van de risico's

- Een gebruiker kan zich voordoen als een coördinator
- Data kan onderweg onderschept worden en gewijzigd worden
- Confidentiële data kan uitgelekt worden
- Een gebruiker kan zich voordoen als een andere zoeker

Hoe willen we testen?

- Documentatie doornemen over de standaarden en implementatie.
- Implementatie en libraries in de source code controleren.

Welke toegang hebben we hiervoor nodig?

- Source code
- Documentatie

Organisatorisch

Wat testen we?

- De eisen die gesteld worden aan de gebruikers voordat deze permissies krijgen
- De opgestelde policies

Ten behoeve van de risico's

- Een gebruiker kan een rol met te veel bevoegdheden bemachtigen
- Een coördinator kan een aanwijzing aanpassen of verwijderen
- Een coördinator kan een foute aanwijzing goedkeuren
- Een coördinator kan gevoelige informatie lekken over aanwijzingen of andere gevoelige zaken
- Een type gebruiker kan mogelijk meer permissies hebben dan benodigd

Hoe willen we testen?

- Policy review uitvoeren
    - Screening
    - Gebruikers handleiding per rol
    - Overig

Welke toegang hebben we hiervoor nodig?

- Toegang tot de policies
- Toegang tot de gebruikerseisen

Database

Wat testen we? (1)

Hoe goed is de database beveiligd tegen SQL-injections?

Ten behoeve van de risico's

- Een aanvaller zou via een SQL-Injection een select-statement kunnen uitvoeren en daarmee confidentiële informatie kunnen vrijgeven
- Een aanvaller zou via bijvoorbeeld een SQL-Injection heel veel inserts (toevoegingen) kunnen doen aan de database waardoor deze overbelast raakt, en uiteindelijk een Denial of Service geeft
- Een aanvaller zou via een SQL-Injection de database kunnen aanpassen of verwijderen en daarmee meer rechten krijgen dan die daadwerkelijk heeft
- Een aanvaller zou via een SQL-Injection zichzelf rechten kunnen geven zoals de eigenaar van zoekacties

Hoe willen we testen?

- SQL-Injections proberen op de testomgeving
- Implementatie van input sanitization in de source code controleren

Welke toegang hebben we hiervoor nodig?

- Toegang tot de testomgeving (Minimaal)
- Toegang tot de source code (Het liefst)

Wat testen we? (2)

- Hoe goed is de database beveiligd tegen onbevoegde toegang van derden?
- Hoe goed zijn de credentials voor de database afgeschermd in de backend?

Ten behoeve van de risico's

- Een aanvaller zou de backend kunnen spoofen om toegang te verkrijgen tot de database buiten de backend om.
- Logs zouden gemanipuleerd kunnen worden om toegang en wijzigingen te verbergen
- Een database dump zou door kwaadwilligen gestolen kunnen worden

Hoe willen we testen?

- Documentatie doorspitten
- Implementatie van de database controleren
- Controleren op whitelist mogelijkheden

Welke toegang hebben we hiervoor nodig?

- Documentatie
- Implementatie details van de database

Wat testen we? (3)

- Is het direct adresseren van de database server mogelijk?
- Is de authenticatie van de database server zelf goed opgezet?

Ten behoeve van de risico's:

- Een database dump zou door kwaadwilligen gestolen kunnen worden
- Wanneer de database server direct te adresseren is, bestaat de kans op een traditionele (D)DoS aanval

Hoe willen we testen?

- Controleren of het systeem van buitenaf benaderbaar is
- Authenticatie mechanismen controleren

Welke toegang hebben we hiervoor nodig?

- Documentatie
- Testomgeving

Wat testen we? (4)

De policies voor het verkrijgen en wijzigen van data.

Ten behoeve van de risico's:

- Wanneer iemand toegang heeft tot de database kan hij/zij deze verwijderen, waardoor grotendeels de hele service niet meer bruikbaar is.
- Wanneer iemand toegang krijgt tot de database kan hij/zij de data vrijgegeven.

Hoe willen we testen?

Een policy review van de policy gerelateerd aan datatoegang

Welke toegang hebben we hiervoor nodig?

Policies.

Authenticatie

Wat testen we?

- Is het mogelijk om te authentiseren als een andere gebruiker?

Ten behoeve van de risico's

- Door zich te authentiseren als een persoon met hogere rechten dan een aanvaller voorheen had kan deze zijn bevoegdheden uitbreiden.
- Een aanvaller kan een MITM-attack uitvoeren om het token van een andere gebruiker te bemachtigen en hiermee zijn eigen identiteit vervalsen.

Hoe willen we testen?

- Documentatie doornemen over de standaarden en implementatie.

Welke toegang hebben we hiervoor nodig?

- Toegang tot de documentatie.

Taakverdeling

Hieronder de taakverdeling, deze dient als richtlijn. De verdeling is niet in beton gegoten, wat inhoudt dat we elkaar wel helpen waar nodig. We moeten dus wel flexibel zijn met deze verdeling.

Taak	Persoon	Opmerkingen
GPS	10.2.e.	
Databeveiliging (ongewenste toegang van derden)	10.2.e.	SQL-Injections en brute force attacks
Databeveiliging (confidentialiteit)	10.2.e	
Datacommunicatie	10.2.e.	Encryptie
Organisatorisch	10.2.e	
Database (Direct adresseren en authenticatie)	10.2.e.	Toegang van derden
Database (policies)	10.2.e.	
Authenticatie	10.2.e.	

7. GPS

Gevonden risico

Een persoon kan zijn/haar gps gegevens aanpassen waardoor het lijkt alsof hij/zij ergens anders is dan daadwerkelijk het geval is. Dit wordt ook wel “spoofing” genoemd. In het geval van Sarea houdt dat in dat een kwaadwillend persoon kan doen alsof hij/zij ergens heeft gezocht terwijl dit niet zo geweest hoeft te zijn. Dit kan leiden tot verkeerde aanwijzingen, of ervoor zorgen dat gebied B niet wordt doorzocht, omdat een zoeker zijn/haar locatie heeft gespooft (vervalst) waardoor het lijkt alsof gebied B wel is doorzocht.

In het kort

Zoeker A kan doen alsof hij/zij heeft gezocht op locatie A, terwijl zoeker A hier nooit is geweest, maar juist heeft gezocht op locatie B.

Uitvoerbaarheid van spoofing

Spoofing is erg simpel uit te voeren, het behoeft namelijk geen specifieke IT-kennis. Spoofing kan namelijk worden uitgevoerd door simpelweg een app te downloaden vanuit de App Store of Play Store. Vervolgens kan met een druk op een knop de gewenste locatie worden geëmuleerd. Iedere app die om de huidige locatie vraagt van het apparaat zal dan de locatie gebruiken die de spoofing app emuleert.

Oplossing

Tegen spoofing zelf is eigenlijk niets te doen. Wel is het mogelijk om functies in de app te bouwen die spoofing kunnen detecteren. Een voorbeeld van een mogelijke oplossing met verschillende varianten staat hieronder omschreven.

Actie(s) ondernemen wanneer een verplaatsing plaatsvindt met een te grote snelheid.

Stel een zoeker is op locatie A en verplaatst zich ineens naar locatie B, wat 5km verderop is, dan is er al een aanwijzing dat er mogelijk spoofing in het spel is. Het is namelijk niet mogelijk om binnen een seconde 5 kilometer verderop te zijn, door spoofing is dit wel mogelijk.

Variaties op de oplossing

Onderstaande variaties zouden zowel alleen als in combinatie kunnen worden toegepast.

- Locatie wel gebruiken maar voorzien van een “mogelijk onbetrouwbare locatie” label.
- Coördinator een melding geven dat een zoeker mogelijk onbetrouwbare locatiegegevens aanlevert.

8. Databeveiliging

Gevonden risico's

Bij Sarea ontbreekt op dit moment een document met security policies die de veiligheid waarborgt van de database.

In het kort

Er ontbreekt een document met security policies voor de database

Wat is er al wel?

Ondanks het ontbreken van een beleid omtrent database policies, staat er in de documentatie wel al wat beschreven.

De technische aspecten van de database die aanwezig zijn, staan al omschreven in de documentatie zoals:

- Een diagram die aangeeft hoe de verschillende deelsystemen communiceren met de database
- Een sequence diagram die aangeeft hoe de database wordt gebruikt omtrent inloggen
- Hoe de gps-communicatie wordt opgeslagen in de backend
- Wat voor type database er wordt gebruikt
- Hoe de authenticatie wordt geregeld richting de database.
- De repositories die in gebruik is in combinatie met de database.
- Een ERD(diagram met alle velden) van de database

Waarom is dit een probleem?

Het technische aspect van de database staat dus duidelijk beschreven, maar aan de organisatorische kant ontbreekt praktisch alles. Dit is een kwetsbaar punt, omdat er bij zo'n dynamische database duidelijk bepaalde dingen op papier moeten staan.

Zo staat nu nergens omschreven:

- Wie heeft toegang tot de database
- Hoe de wachtwoorden worden opgeslagen
- Welke rollen organisatorisch rechten hebben tot de database en welke rechten bepaalde actoren hebben
- Hoelang wachtwoorden worden opgeslagen en wanneer ze gewijzigd moeten worden.

En nog meer zaken die later worden beschreven.

Oplossing

Het maken van een database securitybeleid met database policies. (Beaver,2007)

Hieronder een aantal policies die wij aanraden voor Sarea:

Authentication control policy

In het database securitybeleid moet een database acces control. In dit stuk van het beleid moet staat wie bij de gevoelige data in de database mag en hoe deze data wordt afgeschermd van mensen die daar niet bij mogen.

Ook wordt daar de authenticatie in geregeld. Met genoteerd hoe een geautoriseerde zich moeten authentiseren. Daar zijn een paar keuzes voor:

Discretionary Access Control (DAC)

Met DAC bepaalt de eigenaar de autorisatie op basis van bepaalde regels.

Mandatory Access Control (MAC)

Met MAC wordt autorisatie geregeld op basis van centrale autorisatie regels.

Role Based Access Control(RBAC)

RBAC geeft autorisatie op basis van de rol van een persoon die informatie wil verkrijgen. Deze Access control past goed bij Sarea, omdat het ervoor zorgt dat bijvoorbeeld een coördinator bepaalde dingen kan inlezen en inschrijven, maar op basis van zijn rol ook niet alles in kan zien.

Naast de acces control staat in dit gedeelte van het beleid ook hoe de database is beveiligd:

- Wordt er voor de backend gebruik gemaakt van two factor authentication?
- Welke data is beschikbaar voor welke rol?

Data Backup policy

In de data backup policy staat en wordt uitgelegd hoe, wat en waar de data backups worden opgeslagen en hoe die bereikbaar zijn.

Het maken en opslaan van een data backup policy heeft veel voordelen zoals:

- Helpt het nader toelichten van de verantwoordelijkheden van de backups en herstel na problemen
- Geeft aan waar backups moeten worden opgeslagen en wie er toegang tot heeft
- Hoe vaak data geback-upt moet worden en hoe.

Dit zijn de grootste voordelen van het hebben van een data backup policy. Daarnaast is het eens stuk veiliger omdat bij een probleem met de database het essentieel is dat er een goede backup is, al helemaal als het een database met geclassificeerde informatie is.

Wachtwoord management policy (Oracle z.d.)

In het wachtwoord policy staan de vereisten waar een wachtwoord van een gebruiker of andere rol aan moet voldoen. Voorbeelden van eisen aan een wachtwoord zijn:

- Het wachtwoord bevat geen delen van de gebruikersnaam
- Minstens 8 karakters lang
- Een combinatie van bijvoorbeeld 1 hoofdletter en 1 speciaal teken.

Naast de eisen aan een wachtwoord staat in een wachtwoord policy hoelang een wachtwoord geldig is en wanneer een gebruiker of andere rol zijn wachtwoord moet vervangen.

Dit is een belangrijk deel voor Sarea omdat de app op dit moment geen eisen stelt aan de wachtwoorden van een gebruiker.

Daarnaast moet er in het wachtwoord policy staan na hoeveel foute inlog pogingen een gebruiker zijn account wordt gelocked.

Change Management/Business continuity policy

In deze policy staat wat er moet gebeuren als de database down gaat. En hoe deze zo snel mogelijk weer up is.

Een paar mogelijke dingen die in deze policy kunnen staan zijn:

- De maximale downtime die de database mag hebben
- De preventieve maatregelen die zijn genomen tegen het down gaan van de database
- Stap voor stap een strategie van probleem diagnose tot weer een werkende database
- De belangrijke onderdelen van de database.
- Wat als eerste weer back online moet zijn.

Data Retention policy

Een data retention policy is een policy die ervoor bepaald hoe de informatie bepaald wordt en dat deze bewaring van informatie voldoet aan de wet.

Kort gezegd staat in een data retention policy: welke data wordt opgeslagen, hoelang deze data opgeslagen blijft, wat er met de data gebeurt na de opgeslagen periode (wordt deze gearchiveerd of verwijderd bijvoorbeeld) en de regels die er zijn bij het bewaren van die data. Ook staan hier vaak alle andere facetten die het opslaan van data met zich meebrengen.

Naast deze essentiële policies zijn er nog meer policies die in het beleid kunnen staan, namelijk:

- **System monotoring policy**: Hoe wordt de database gemonitord en hoe worden incidenten gemeld
- **Information classfication policy**: De classificaties van de verschillende informatie in de database
- **Separation of duties policy:** De verantwoordelijkheden van de verschillende actoren en rollen in de organisatie van de database.

Wat moet er in een policy staan?

Hieronder een voorbeeld van alle dingen die mogelijk in een policy kunnen staan.

Introductie

Een korte introductie over het onderwerp van de policy. Bijvoorbeeld wachtwoord management

Het doel van de policy

Kort samengevat wat de doelen zijn van de policy. Ook staat hierin de strategie van de policy

Scope

Hierin staat voor wie en wat deze policy van belang is. Denk bijvoorbeeld aan voor welke rollen geldt deze policy en welk database systeem is hierbij betrokken.

Rollen en verantwoordelijkheden

Hierin stat beschreven welke rollen deze policy moeten uitvoeren en wat hun verantwoordelijkheden zijn.

Statement(s)

Hierin staat de hoofdzaak van de policy beschreven zoals:

“Wachtwoorden moeten minimaal 8 karakters lang zijn met minimaal een hoofdletter en een cijfer.”

Dit kunnen er meerdere zijn, maar altijd minimaal een.

Uitzonderingen

Als er uitzonderingen zijn voor de policy moeten die ook beschreven worden. Mogelijk bij dit voorbeeld zijn er andere wachtwoord eisen voor coördinatoren, als dat zo is moet dat ook in de policy beschreven staan.

Procedures

In dit onderdeel staat hoe de policy geïmplementeerd gaat worden.

Sancties

Alle mogelijke sancties die staan op het breken van de policy staan in dit onderdeel.

Review

In dit onderdeel staat hoe vaak een policy geëvalueerd moet worden.

Referenties

Als een policy refereert naar een security standaard, bijvoorbeeld ISO of IEC, dan staat dat in dit onderdeel vermeld.

Veranderingen

Als er dingen veranderd zijn na het maken van de policy, wordt dat in dit onderdeel bijgehouden.

9. Datacommunicatie

9.1 Confidentialiteit van de mensen met rechten op confidentiële informatie.

In deze test wordt er gekeken naar dekking van potentiele risico's de beschikbare policies binnen de Sarea applicatie en het gebruik hiervan op basis van de confidentialiteit van de mensen met rechten op confidentiële informatie. Het doel van deze test is het achterhalen van onafgedekte risico's.

Gevonden risico

Het eerste opvallende is dat er geen policies zijn voor het omgaan met confidentiële data. Hierdoor kan er moeilijk gekeken worden naar risico's in de bestaande policies. Het niet bestaan van deze policies is een risico omdat het onduidelijk is hoe iemand met confidentiële gegevens om moet gaan. Wel staat er in de blauwdrukken van het Sarea systeem dat er bij de eerste keer opstarten een kleine guide wordt gegeven over het gebruiken van de app en het delen van de data.

Uitvoerbaarheid

Deze vorm van een datalek is erg makkelijk en vormt hierdoor een groot probleem. Mensen zijn geneigd informatie te delen met derde voor vele redenen. Zonder goeie policies over het delen van data kan bedoelt en onbedoeld data niet bedoelt voor derde partijen toch beschikbaar komen voor deze partijen door een gesprek aan te gaan met een partij die meer kennis heeft.

Oplossing

Het maken van policies over het delen van data. Deze policies zullen richtlijnen voor coördinatoren kunnen bevatten over het delen van confidentiële en of essentiële data. Hierbij kan gedacht worden aan richtlijnen over welke data wel en niet confidentieel worden beschouwd. Welke personen toegang mogen hebben tot de data bijvoorbeeld voogden of verantwoordelijken voor de vermiste persoon.

Veder moeten deze policies mogelijkheden bevatten om deze data waar nodig toch door te kunnen geven aan partijen die deze nodig hebben.

9.2 Encryptie

In deze test wordt gekeken naar het gebruik van encryptie over het dataverkeer van alle clients die met de Sarea infrastructuur communiceren. Mocht de verbinding niet encrypted zijn bestaat de kans dat verkeer afgeluisterd of aangepast wordt. Hierdoor zouden gegevens kunnen lekken, onjuiste informatie doorgestuurd kunnen worden of mogelijk inloggegevens gestolen worden.

Gevonden risico

Encryptie wordt niet vanuit de Sarea backend zelf geregeld.

Uitvoerbaarheid van een MitM

Het afluisteren van verkeer is een reëel risico wanneer de data niet encrypted is. Dit kan met een zogenaamde Man in the Middle aanval. Wanneer de verbinding over een apparaat loopt die in handen in van een kwaadwillige kan deze alle data vrij uitlezen en ook manipuleren.

Oplossing

Omdat de encryptie niet vanuit de Sarea back end geregeld is maakt dit het de verantwoordelijkheid van de reverse proxy die de back end bereikbaar maakt voor de rest van de wereld. Dit biedt wel voordelen voor het centraliseren van de infrastructuur die de verbindingen encrypt. Hierdoor wordt het makkelijker om later encryptieprotocollen te veranderen. Deze opstelling wordt in de testomgeving al toegepast. Echter omdat dit geen onderdeel van het project zelf is moet hier wel rekening mee gehouden worden bij het uitrollen van het eindproduct.

Een aantal eisen waar de reverse proxy minimaal aan moet voldoen in het eindproduct zijn:

- Het toepassen van een SSL verbinding
- Het gebruiken van een geldig SSL certificaat
- Een moderne TLS versie gebruiken
  - Minimaal 1.2
  - Optimaal 1.3
- Het weigeren van plain tekst verbindingen opzetten

Verder moeten verbindingen die niet via de reverse proxy lopen geblokkeerd worden. Ten slotte is het ook verstandig om verbindingen richting de database vanaf het internet niet toe te staan.

10. Organisatorisch

10.1 De eisen die gesteld worden aan de gebruikers voordat deze permissies krijgen

In deze test wordt er gekeken naar de eisen aan de gebruikers voordat deze permissies krijgen en welke maatregelen er zijn genomen om te zorgen dat deze rechten niet worden misbruikt.

Gevonden risico

Ook bij deze is het opvallende dat er geen policies zijn over dit onderwerp. Hierdoor bestaat het risico dat ongeschikte mensen een rol met te veel bevoegdheden kan bemachtigen.

Uitvoerbaarheid

Voor het uitvoeren hiervoor moet er een rol bestaan met hogere permissies binnen een zoektocht. Binnen de applicatie zoals beschreven in de blauwdrukken van de Sarea app zijn er maar twee soorten rechten. Een zoeken en een Coördinator. Het worden van coördinator is simpel. Je creëert de zoektocht. Een coördinator heeft hierin geen toegang tot andere zoektochten en heeft alleen zijn rechten op de huidige zoektocht. Het is dus moeilijk voor een persoon om deze rechten te bemachtigen

Oplossing

De makkelijkste manier om te veel rechten te krijgen is het bemachtigen van de coördinator rol van de huidige coördinator. Om dit tegen te gaan kan er een policy gemaakt worden over het overgeven van de coördinator rol. Verder kan een melding in de applicatie gegeven worden wanneer iemand zijn rechten wil overdragen aan een andere coördinator.

11. Database

11.1 SQL Injecties

Gevonden risico

Een aanvaller zou via SQL injecties data kunnen aanpassen in de database.

Uitvoerbaarheid van SQL injecties

SQL injecties zijn een van de grootse risico's die een SQL database met zich meebrengt. Via een SQL injecties kan een aanvaller dingen zien, aanpassen of zelfs verwijderen uit de database. Sarea draait een database met MYSQL. Dus SQL injecties zijn een van de grootste dreigingen voor de database. SQL injecties zijn niet moeilijk uit te voeren. Bij elk veld waar een user om input wordt gevraagd kan een user met een beetje kennis van een SQL-databases een injection kunnen uitvoeren.

Oplossing

Op dit moment wordt bij het invoeren van gegevens gecheckt of bepaalde tekens in het mailadres of wachtwoord zitten. Dit is een manier om in die velden SQL injecties tegen te gaan. Mogelijke aanvullende oplossingen zijn:

- Zorg ervoor dat alle componenten die invloed hebben op de database. Denk aan onder andere: libraries, plugins, frameworks en de webserver software altijd up to date zijn.
- Gebruik het principe least privilige. Dit betekent: geef een user nooit meer privileges dan die moet hebben. Als een website alleen content moet ophalen via een select statement geef de connectie met de database van de website dan geen insert, delete of update statements.
- Gebruik geen gedeelde database accounts tussen de verschillende webservers of applicaties.
- Zorg ervoor dat database error messages nooit aan de kant van de user te zien zijn. Aanvallers kunnen informatie in die messages gebruiken.

Daarnaast zijn er meerdere manieren om user input nog veiliger te checken en filteren:

- Dit kan door het gebruiken van prepared statements. Deze worden onder andere meegegeven in liberies zoals MYSQLi en PDO.
- Check of de input van de user overeenkomt met wat je verwacht. PHP heeft hier veel opties voor zoals is_numeric(), ctype_digit() en nog veel meer.
- De input van de user kan ook gefilterd worden via escaping. mysql_real_escape_string(), sqlite_escape_string() zijn hier voorbeelden van.
- Filteren van de input stopt de meeste triviale aanvallen, maar lost niet de onderliggende kwetsbaarheid op.

11.2 Brute-force attack

Gevonden risico

Een aanvaller zou via een Brute-force attack toegang kunnen krijgen tot de database.

Uitvoerbaarheid van Brute-force attacks

Via een Brute-force attack probeert een aanvaller zoveel mogelijk gebruikersnaam-wachtwoordcombinaties totdat hij/zij toegang heeft tot voor de aanvaller onbevoegde systemen.

Een aanvaller zou een brute force attack kunnen uitvoeren door doormiddel van een script of handmatig wachtwoorden kunnen uitproberen totdat dit lukt. Brute Force attacks zijn niet heel moeilijk om uit te voeren. Elke aanvaller met een beetje IT-kennis kan een tool downloaden en daarmee vrij makkelijk Brute Force attacks uitvoeren

Brute force attacks zijn vooral gevaarlijk als:

- Er niet gebruikt wordt gemaakt van lange, ingewikkelde wachtwoorden
- Er geen duidelijk beleid of policy is rond wachtwoorden.
- Er geen countermaatregelen worden genomen zoals een beperkt aantal pogingen per host.

Sarea is op dit gebeid wel kwetsbaar:

- Er is op dit moment geen standaard voor wachtwoorden. Bijvoorbeeld hoelang een wachtwoord moet zijn en wat voor tekens er gebruikt moeten worden.
- Er is ook geen policy of beleid is rond wachtwoorden.
- De maatregelen tegen brute force attacks zijn minimaal. Een host die ‘teveel’ pogingen doet na een tijdje wordt dan tijdelijk geblokkeerd. Maar het aantal pogingen staat niet beschreven en ook staan er nog geen duidelijke consequenties voor het te vaak proberen.

Oplossing

Op dit moment wordt bij Sarea een host gelockt na een overvloed van requests aan de server. Dit is op dit moment de enige maatregel die er wordt genomen tegen Brute Force Attacks. Dit is helaas niet genoeg. Aanvullende opties voor betere beveiliging tegen Brute Force Attacks zijn:

- Het locken van een account na een aantal inlogpogingen. Bijvoorbeeld na 3 keer een tijdelijk of permanente lock van dat account.
- Het gebruiken van two factor authentication of CAPTCHA. Hierdoor wordt er na een succesvolle inlogpoging een tweede laag toegevoegd. Two factor authentication zorgt ervoor dat je zeker weet dat degene die inlogt ook daadwerkelijk de bezitter is van dat account. CAPTCHA sluit het gebruik van Bots uit.
- Het verplichten van een ‘sterk’ wachtwoord. Sterke wachtwoorden kosten meer rekenkracht en tijd voor de aanvaller. Voorbeelden van een vereisten voor een wachtwoord zijn: minimaal 8 karakters, 1 cijfer en 1 speciaal teken. Dit kan het beste verwerkt worden in het wachtwoord management policy
- Maak gebruik van hashing voor wachtwoorden. Sla bijvoorbeeld de wachtwoorden op met een SHA12 versleuteling.

11.3 Toegang van derden

Om de database veilig te houden moeten derden hier buiten gehouden worden. Dit is ter voorkomen van het stelen of aanpassen van data.

Gevonden risico

De backend van Sarea is niet verantwoordelijk voor het afschermen van de databaseserver tegen verbindingen van buitenaf.

Uitvoerbaarheid van toegang tot de database bemachtigen

Een aanval uitvoeren op de database van buitenaf zou niet makkelijk moeten zijn. Dit is echter afhankelijk van de authenticatie gegevens van de database. Wanneer een iemand probeert de database te bereiken zal deze ook inloggegevens nodig hebben om bij de data te mogen komen. Deze beveiliging zou aanvallers moeten weigeren. Echter is het mogelijk dat een aanvaller deze inloggegevens alsnog kan bemachtigen en daarom is dit als enige mechanisme niet voldoende.

Oplossing

Dankzij het werken met Docker containers is het lastig om de container te configureren voor het netwerk waar deze op komt. Daarom zal bij de realisatie van de productie omgeving toegang tot de database van buitenaf voorkomen moeten worden vanaf de firewall. Hierdoor wordt de mogelijkheid tot het pogen in te loggen verlaagd. De combinatie van inloggegevens en het blokkeren van toegang vanaf het internet samen moet de uitvoerbaarheid van de aanval genoeg verlagen.

12. Authenticatie

12.1 Een zoeker zou zichzelf de rechten kunnen geven die een coördinator ook heeft.

Gevonden risico's

Iemand zou zich kunnen authentiseren als een persoon met hogere rechten, dan dat die persoon voorheen had. Hiermee kan iemand zijn/haar bevoegdheden uitbreiden. Dit wordt in de IT-wereld ook wel 'Elevation of privilege' genoemd. In het geval van Sarea zou dat betekenen dat een persoon die als rol een zoeker is toegekend, door middel van verschillende soorten aanvallen zichzelf hogere rechten zou kunnen geven dan een zoeker eigenlijk heeft. Het kan dus zijn dat een 'kwaadwillende' zoeker evenveel rechten of misschien zelfs wel meer rechten dan een coördinator heeft.

Uitvoerbaarheid van elevation of privilege

Voor het uitvoeren van een elevation of privilege aanval is de nodige kennis vereist. Het is dus niet door iedereen even eenvoudig uit te voeren. Bij een elevation of privilege aanval draait het erom toegang te krijgen tot de database, hierin staan immers alle gebruikers en hun rol/rechten. Als de database goed beveiligd is dan is de kans op een geslaagde aanval vele malen kleiner.

Oplossingen

In het geval van Sarea zal het niet snel voorkomen dat een kwaadwillend persoon meedoet met een zoekactie, laat staan het verkrijgen van meer rechten. Echter, het is wel aanbevolen om de database zo goed mogelijk te beschermen. Dus niet alleen maar een wachtwoord, maar een combinatie van een wachtwoord en een andere methode.

Tweefactorauthenticatie / multi-factor authenticatie implementeren

Mocht een kwaadwillend persoon inloggegevens weten te krijgen dan is het alsnog niet mogelijk om in te loggen met multi-factor authenticatie. Bij multi-factor authenticatie moet een login eerst goedgekeurd worden alvorens er ingelogd wordt.

Variaties op de oplossing

- Cijfercode die iedere zoveel seconden veranderd. (Deze cijfercode kan gegenereerd worden door een app als Google Authenticator).
- Fysieke key [sleutel] (Hardware token)

12.2 Een aanvaller kan een MITM-attack uitvoeren om het token van een andere gebruiker te bemachtigen en hiermee zijn eigen identiteit vervalsen.

Gevonden risico's

Een kwaadwillend persoon kan een zogeheten man-in-the-middle-aanval uitvoeren, dit wordt vaak afgekort naar MITM Attack. Bij een MITM Attack probeert de aanvaller gegevens te onderscheppen, dit kunnen wachtwoorden zijn, maar in dit geval ook de Token (vergelijkbaar met een sleutel) die gebruikt wordt door de JSON Web Token functionaliteit. Doordat een aanvaller de token van een andere gebruiker heeft is de aanvaller niet makkelijk te achterhalen, aangezien alle acties worden geregistreerd alsof ze door degene zijn uitgevoerd waarvan de token is onderschept.

Uitvoerbaarheid van een man-in-the-middle-aanval

Een man-in-the-middle-aanval is in verschillende varianten mogelijk. Alle varianten vereisen de nodige IT-kennis en zijn niet onder alle omstandigheden uit te voeren. Een man-in-the-middle-aanval heeft namelijk vele malen minder kans van slagen als er gebruik wordt gemaakt van een beveiligd netwerk.

Oplossingen

Momenteel is Sarea nog in een testfase en is de applicatie nog niet live, dit is waarschijnlijk ook de reden dat onder andere de tokens nog niet beveiligd zijn met encryptieversleuteling. Onderstaande oplossing is dus alleen nodig als er in de live versie nog niet gewerkt wordt met encryptieversleuteling.

Versleutel tokens door middel van encryptie

Door tokens te versleutelen kan een kwaadwillend persoon niet rechtstreeks de informatie inzien of aanpassen, hier is namelijk een zogeheten sleutel voor nodig. Er zijn verschillende vormen van encryptie. Zo zijn worden er voor zwakke computers ook zwakkere encryptiealgoritmen gebruikt dan voor computers met meer rekenkracht. Een sterker encryptiealgoritme is veiliger, maar belast het systeem ook meer. Aangezien Sarea niet zal werken met zwakke computers is er de mogelijkheid om gebruik te maken van een sterk encryptiealgoritme.

Variaties op de oplossing

In hoofdstuk 9.2 staat uitgebreider omschreven hoe een goede encryptie zou kunnen worden geïmplementeerd en waar deze dan aan moet voldoen.

13. Conclusie & advies

Na in een relatief korte periode onderzoek te hebben gedaan naar de veiligheid van de Sarea applicatie kunnen wij een aantal dingen concluderen. Op basis van onze conclusies willen wij Sarea ook een advies meegeven.

Bij het gps deel zou een zoeker kunnen doen alsof hij/zij ergens heeft gezocht terwijl dit niet zo is. Dit probleem zou kunnen worden afgevangen door een functionaliteit te implanteren die de snelheid van een gebruiker bijhoudt. Zodra de snelheid te hoog ligt dan is er sprake van een foutieve locatie.

Ook ontbreekt op dit moment een document met security policies die de veiligheid waarborgt van de database. Door het maken van een database securitybeleid met database policies zou dit probleem kunnen worden opgelost.

Het is ook opgevallen dat er geen policies zijn voor het omgaan met confidentiële data. Hierdoor kan er moeilijk gekeken worden naar risico's in de bestaande policies. Door policies te maken wordt dit probleem verholpen. Bij het maken van de policies kan gedacht worden aan richtlijnen over welke data wel en niet confidentieel worden beschouwd. Welke personen toegang mogen hebben tot de data bijvoorbeeld voogden of verantwoordelijken voor de vermiste persoon. Ook wordt encryptie niet vanuit de Sarea backend zelf geregeld. Een reverse proxy is aanbevolen om hier mee om te gaan

Naast de missende policies van de database en confidentiële data. Mist er een policy die de overdracht van een coördinator rol vastlegt. Hierdoor loopt er een risico dat een gebruiker te veel rechter bemachtigd.

Ook zijn er verdere adviezen gegeven over de verdediging tegen SQL injecties. Tegen SQL injecties werden al maatregelen genomen en in dit rapport zijn dan ook aanvullende oplossingen geboden die verdere veiligheid zouden kunnen waarborgen.

Verder is er gemerkt in het onderzoek dat in huidige staat Sarea kwetsbaar is tegen Brute-force attacks. Deze kwetsbaarheid zou verholpen kunnen worden met een sterker wachtwoordbeleid met verschillende maatregelen tegen Brute-force attacks.

In het onderzoek naar onbevoegde toegang van derden kwam aan het licht dat de backend van Sarea niet verantwoordelijk is voor het afschermen van de databaseserver tegen verbindingen van buitenaf. De aan te raden oplossing is een firewall die onbevoegde verbindingen weert.

Daarnaast is er gekeken naar elevation of privilege attacks die het mogelijk zou maken dat een gebruiker een rol kan innemen met meer rechten. De grootste verbetering was in dit geval het gebruik maken van two factor authentication.

Als laatst is er gekeken naar een mogelijke man-in-the-middle-aanval. Het belangrijkste advies is het gebruik van encryptie bij de authenticatie tokens.

Als een deel van deze adviezen zal worden geïmplementeerd bij Sarea dan zal dit de veiligheid van Sarea een grote stap vooruit laten maken.

14. Bibliografie

Beaver, K. (2007, 8 januari). *Database security policies to think about*. Geraadpleegd van https://searchsqlserver.techtarget.com/tip/Database-security-policies-to-think-about.

7 Security Policies. (z.d.). Geraadpleegd op 16 april 2020, van https://docs.oracle.com/cd/B12037_01/network.101/b10773/policies.htm