Organisatieonderdeel Politie Dienstencentrum
Dienst IM – Advies
Team Informatiebeveiliging

Behandeld door 5.1.2.e
Functie IV-expert informatiebeveiliging
Telefoon 06-5.1.2.e
E-mail 5.1.2.i @vtspn.nl
Review door 5.1.2.e /5.1.2.e
Functie reviewer IV-expert informatiebeveiliging
Telefoon 06-5.1.2.e

Aan:

Ons kenmerk
Uw kenmerk
In afschrift aan
Datum 09-01-2019
Bijlage(n)
Pagina 1

Onderwerp **Informatiebeveiligingsadvies Obi-Engage**

POLITIE

Inhoudsopgave

1 Scope en onderzoeksvraag

1.1 Aanleiding

Sociale media zijn breed omarmd door de politieorganisatie. Regionale Service Centra (RSC's), Basisteams, wijkagenten en de landelijke eenheid zetten sociale media in voor interactie, klantcontact en het uitdragen van eigen boodschappen.

Het beleidsdocument: "Online op één lijn, Communiceren via social media: zakelijk en privé" beschrijft de landelijke afspraken voor het gebruik van social media om te communiceren namens de politie. (goedgekeurd KMTO besluit 2020)

Om eenduidigheid én robuustheid aan te brengen in het gebruik van die sociale media heeft de korpsleiding, de opdracht gegeven het gebruik, werkwijzen en ondersteunende middelen te verankeren bij de regionale en landelijke eenheden. Waaronder de implementatie van de webcaretool OBI4wan-Engage.

1.2 Onderzoeksvraag

Hoe kan ervoor gezorgd worden dat de (persoons-)gegevens binnen OBI4wani-Engage voldoende zorgvuldig (lees: veilig) worden verwerkt?

1.3 Opdrachtgever

5.1.2.e

1.4 Randvoorwaarden

OBI4wan-Engage wordt niet gebruikt voor opsporingsdoeleinden.

1.5 Geraadpleegde personen

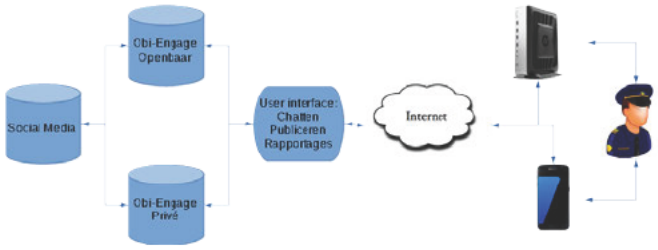
Medewerker	Functie	Informatie	Analyse	Conclusie	Aanbeveling
5.1.2.e	5.1.2.e	X	X		
5.1.2.e	5.1.2.e	X	X	X	X
5.1.2.e	5.1.2.e	X	X		
5.1.2.e	5.1.2.e	X	X		
5.1.2.e	5.1.2.e		X	X	X

Met opmerkingen 5. **(1):** Ik weet niet meer of 5.1. hier nog een rol in heeft.

2 Informatievoorziening

2.1 Informatiestroom online klantcontact

De gegevens binnen OBI4wan-Engage zijn afkomstig van online klantcontact. Denk daarbij aan tweets, Facebookberichten, Instagramberichten gericht aan een basisteam, regionale eenheid, wijkagenten of de landelijke eenheid.
Het gaat om openbare en privé berichten op de sociale media van politie accounts.
Binnen een Eenheid wordt er tussen RSC's, basisteams, teams communicatie en andere afdelingen op het gebied van online klantcontact samengewerkt. Elk team handelt haar eigen berichten af (WBT of App), of werkt samen met andere teams, eenheden of afdelingen. Dat gaat zowel binnen OBI4wan-Engage (overzetten of toekennen van berichten), als buiten OBI4wan-Engage door berichten te mailen naar afdelingen zoals DRIO/OPS/meldkamer.



2.2 OBI4wan-Engage

Afhankelijk van de rol van de medewerker worden onderstaande activiteiten (zie bovenstaande user interface) ondersteunt door OBI-Engage.

Activiteit	Omschrijving
Chatten	Toegang tot de interne chat in OBI-Engage: hiermee kunnen eerstelijns vragen gesteld worden aan superusers uit andere eenheden en basisteams.
Webcare	Inlezen, analyseren en beantwoorden Social Media berichten, notities aanmaken, bewerken en verwijderen
Publiceren	Nieuwe berichten versturen/plannen
Raadplegen rapportages/statistieken	Inzicht in webcareprestaties op niveau van 1) social media accounts, en 2) gebruikersniveau (collega's) en inzicht in de ontwikkeling van de eigen social media accounts (aantal likes, volgers/vrienden, bereik, etc.)
Narrowcasting	Narrowcasting geeft weer wat er momenteel leeft op Social Media, tevens wordt weergegeven wat de organisatie met deze berichten doet.

3 Beveiligingsanalyse

3.1 Beveiligingsdoel

De beveiligingsdoelen voor OBI4wan-Engage zijn als volgt geformuleerd:

- De applicatie voldoet aan de door de business gestelde beschikbaarheidseisen;
- De gegevens binnen de applicatie zijn correct/actueel;
- De applicatie/het werkproces is zodanig ingericht dat onbevoegden geen toegang krijgen tot gegevens en misbruik van gegevens wordt voorkomen.

3.2 Beveiligingsbehoefte

In deze stap wordt bepaald hoe belangrijk het gebruik van OBI-Engage is voor de organisatie en welke mate van beveiliging gewenst is. De beveiligingskenmerken en de impact voor de organisatie in het geval van een probleem met de beschikbaarheid, integriteit en/of vertrouwelijkheid van het systeem met daarin opgeslagen informatie wordt bepaald door de business.

3.2.1 Beveiligingskenmerken

De business formuleert de beveiligingsbehoefte als een viertal kenmerken:

- **Waarde van de informatie**. Dit betreft de intrinsieke waarde van informatie, hoeveel hebben wij er voor over of hebben anderen er voor over om over deze informatie te kunnen beschikken? De geldelijke waarde zou hier een rol kunnen spelen, maar is niet zaligmakend.
  Begrippen: Aanzienlijk, gemiddeld, beperkt;
- **Gebruik van de informatie.** In hoeverre mag de informatie worden gebruikt binnen andere trajecten? Dit betreft delen en verstrekken.
  Begrippen: 'For your eyes only', mag worden gebruikt na toestemming vooraf, mag vrijelijk worden gebruikt;
- **Wetsartikel waaronder de informatie wordt verwerkt**. Dit is een aanduiding van het regime van de Wpg of Wbp waaronder de informatie is verzamelt of valt. Gedurende de levensduur van informatie kan dit veranderen.
  Begrippen: Wpg artikel 8, 9, 10, 12, 13 en Wbp persoonsgegeven, bijzonder persoonsgegeven;
- **Oorsprong van de informatie.** In hoeverre men mag vertrouwen dat de informatie klopt met de werkelijkheid wordt in hoge mate bepaald door de bron van de informatie.
  Begrippen: Informant, getuige, eigen waarneming, verhoor, camera;

	Waarde informatie	Gebruik informatie	Wetsartikel	Oorsprong informatie
Classificatie Business	Beperkt	Mag vrijelijk worden gebruikt	AVG/Wpg	Social Media

3.2.2 *Impactanalyse*

De impact voor de business en omgeving wordt duidelijk in het geval van een probleem met de beschikbaarheid, integriteit en/of vertrouwelijkheid van het systeem en de daarin opgeslagen informatie. Hieronder een overzicht van potentiele effecten per classificatie. Let wel, voor het maken van een keuze hoeven niet alle genoemde effecten tot uiting te komen.

Classificatie[1]	Beschikbaarheid	Integriteit	Vertrouwelijkheid
Hoog (3)	**Bedrijfskritisch::** Het ontbreken van de informatie leidt tot *Personen*: dodelijke/zwaargewonde slachtoffers *Objecten:* uitschakeling vitale objecten *Samenleving:* maatschappelijke ontwrichting *Imago:* grote imagoschade *Bedrijfsvoering*: ernstige verstoring	**Bewijsbaar:** Onjuistheden in de informatie leidt tot *Personen*: dodelijke/zwaargewonde slachtoffers *Objecten:* uitschakeling vitale objecten *Samenleving:* maatschappelijke ontwrichting *Imago:* grote imagoschade *Bedrijfsvoering*: ernstige verstoring	**Geheim:** Bekend worden van de informatie kan leiden tot *Personen*: dodelijke/zwaargewonde slachtoffers *Objecten:* uitschakeling vitale objecten *Samenleving:* maatschappelijke ontwrichting *Imago:* grote imagoschade *Bedrijfsvoering*: ernstige verstoring
Midden (2)	**Noodzakelijk:** Het ontbreken, leidt tot *Personen:* fysiek letsel *Objecten:* schade aan niet vitale objecten *Samenleving:* verstoring van de openbare orde *Imago*: imagoschade *Bedrijfsvoering*: verstoring	**Betrouwbaar:** Onjuistheden in de informatie leiden tot *Personen:* fysiek letsel *Objecten:* schade aan niet vitale objecten *Samenleving:* verstoring van de openbare orde *Imago*: imagoschade *Bedrijfsvoering*: verstoring	**Vertrouwelijk**: Bekend worden van de informatie leidt tot *Personen:* fysiek letsel *Objecten:* schade aan niet vitale objecten *Samenleving:* verstoring van de openbare orde *Imago*: imagoschade *Bedrijfsvoering*: verstoring
Laag (1)	**Ondersteunend**: Het ontbreken van de informatie leidt tot *Personen:* intimidatie *Objecten:* geringe schade, *Samenleving:* geen hinder *Imago:* geringe schade *Bedrijfsvoering*: hinder	**Bruikbaar:** Onjuistheden in de informatie leidt tot *Personen:* intimidatie *Objecten:* geringe schade, *Samenleving:* geen hinder *Imago:* geringe schade *Bedrijfsvoering*: hinder	**Intern:** Bekend worden van de informatie leidt tot *Personen:* intimidatie *Objecten:* geringe schade, *Samenleving:* geen hinder *Imago:* geringe schade *Bedrijfsvoering*: hinder
Geen (0)	**Niet nodig**: Informatie kan zonder gevolgen langere tijd niet beschikbaar zijn.	**Niet zeker:** Informatie mag worden veranderd.	**Openbaar:** Informatie mag door iedereen worden ingezien.

Score gebruik OBI-Engage
De business heeft de gegevens binnen OBI-engage als volgt geclassificeerd, de cijfers geven de impactscore weer die in de risicomatrix gebruikt worden.

Categorie	Beschikbaarheid	Integriteit	Vertrouwelijkheid	
Classificatie	Midden	Midden	Laag	Midden

[1] Getal geeft score aan die gehanteerd wordt in paragraaf 3.3.2 risicomatrix

3.3 Dreigingen en risico's[2]

3.3.1 Specifieke kwetsbaarheden en dreigingen

Een object wordt als kwetsbaar gezien als er een inherente eigenschap is die potentieel kan worden misbruikt. Vanzelfsprekend bepaalt de mate en wijze van optreden van een dreiging of een kwetsbaarheid relevant is om tegenmaatregelen te treffen.

Nr	Kwetsbaarheid	Dreiging	Kans[3]	Impact[4]	Risico
1	Inloggen	1.1 Username betreft voor- en achternaam van medewerker Nationale Politie, gegevens komen in handen van onbevoegden met als gevolg bedreiging.	1	1	1
		1.2 Username betreft voor- en achternaam van medewerker Nationale Politie, hierdoor zijn accounts makkelijker te hacken omdat enkel nog het wachtwoord ontbreekt. Hacker kan fake-berichten publiceren.	2	2	2
2	Prive-berichten	2 Door onjuiste afhandeling kunnen privé berichten met bijvoorbeeld opsporingstips terechtkomen binnen Narrowcasting, gegevens komen in handen van onbevoegden.	1	1	1
3	Autorisatieproces	3 Momenteel is er geen goed werkend autorisatieproces wat rekening houdt met in-, door-, en uitstroom van medewerkers, hierdoor blijven accounts onterecht actief.	3	1	3
4	Testomgeving	4 Momenteel is er geen aparte ontwikkel/testomgeving, hierdoor kunnen er problemen ontstaan binnen de productieomgeving op het gebied van de betrouwbaarheid van de informatievoorziening.	1	2	2
5	SAAS-oplossing	5.1 Comptabiliteitsproblemen met het netwerk van de Nationale Politie, hierdoor kunnen er beschikbaarheidsproblemen ontstaan.	2	2	4
		5.2 Indien de leverancier de dienst staakt, komt de continuïteit in gevaar dan wel ontstaan er problemen met betrekking tot toegang tot de data.	1	2	2

Met opmerkingen |5. **(2):** Betreft eerste gedeelte van het politie e-mail adres . Dus zonder @politie.nl In samenwerking met OBI zijn wij bezig om in 2023 en 2FA in te stellen.

Met opmerkingen |5. **(3]:** Er zit nog een extra stap bij. Er moet nog een derde veld ingevuld worden met de naam van de omgeving waarin men werkt.

Met opmerkingen |5. **(4]:** Dit stuk kan vervangen worden dat het autorisatieproces op dit moment ingeregeld worden middels de ATL. Afgerond eind 2022.

Met opmerkingen |5. **(5]:** Kan vervangen worden door > Testomgeving is in de nieuwe uitvraag contract aangeschaft. Media okt/ nov 2022 kan men dar gebruik van maken.

[2] Standaardrisico's worden gemitigeerd door de uitvraag van bijlage 1 en bijlage 2
[3] >=Jaarlijks=1, maandelijks = 2, wekelijks = 3
[4] Score Afkomstig uit 3.2.2 impactanalyse

3.3.2 *Risicomatrix*

Onderstaand overzicht geeft een duidelijk beeld van de hierboven geïdentificeerde risico's. Nummers tussen haakjes komen overeen met dreigingen paragraaf 3.3.1.

Impact	*Hoog*	Gemiddeld risico	Hoog risico	Zeer hoog risico
	Midden	Laag risico 4 / 5.2	Gemiddeld risico 5.1 / 1.2	Hoog risico
	Laag	Laag risico 1.1 / 2	Laag risico	Gemiddeld risico 3
		>=Jaarlijks	*Maandelijks*	*Wekelijks*
		Kans		

3.4 Standaard beveiligingseisen

Onderstaande beveiligingseisen zorgen voor een basisniveau op het gebied van informatiebeveiliging. De verantwoordelijke is vrij in keuze van maatregelen per beveiligingseis.

Nr	Beveiligingseis	Wordt aan voldaan ja/nee/deels	Aanbeveling
1	De leverancier kan aantonen dat men voldoet aan een ICT-beveiligingsnormering bijvoorbeeld ISO27001/270002.	Ja	N.vt.
2	De leverancier kan aantonen dat het betreffende softwarepakket minimaal de kwetsbaarheden van het Open Web Application Security Project (OWASP, bijlage 1) afdekt.	Ja	N.vt.
3	De leverancier kan aantonen dat de cloud-omgeving minimaal voldoet aan de Cloud Security Principles (bijlage 2) van het Nationaal Cyber Security Centrum.	Ja	N.vt.
4	De leverancier kan aantonen dat men voor de informatievoorziening OBI-Engage een risicoanalyse uitgevoerd heeft en op basis hiervan aanvullende beveiligingseisen/maatregelen zijn doorgevoerd.	Ja	N.vt.
5	De leverancier kan aantonen dat men regelmatig vulnerability scans / pentests laat uitvoeren en op basis hiervan verbeteringen aanbrengt.	Ja	N.vt.
6	De leverancier kan aantonen dat men enkel gebruik maakt van datacenters binnen Nederlands grondgebied zonder eigendomsverhouding met een partij uit de Verenigde Staten.	Ja	N.vt.
7	Juridische afspraken worden met de leverancier gemaakt rondom toegang/eigenaarschap data en continuïteit (Indien de leverancier de dienst staakt, komt de continuïteit in gevaar dan wel ontstaan er problemen met betrekking tot toegang tot de data).	Nee	1 / 3
8	Richt de applicatie/(controle-)procedures zodanig in zodat er voldaan wordt aan de wettelijke bewaartermijnen.	Nee	1 / 7

5.1 2 **Met opmerkingen (6):** Staan volgens mij afspraken in de GEB en verwerkingsovereenkomst

5.1 2 **Met opmerkingen (7):** Ingesteld bewaartermijn in OBI is 30 maanden. Is gelijk gesteld met de bewaartermijn van telefonie.

3.5 Specifieke beveiligingseisen

Specifieke beveiligingseisen moeten worden getroffen om de hierboven geïdentificeerde risico's te mitigeren. De verantwoordelijke is vrij in keuze van maatregelen per beveiligingseis.

Nr	Beveiligingseis	Mitigeert dreiging[5]	Wordt aan voldaan ja/nee/deels	Aanbeveling[6]
1	De inloggegevens zijn niet herleidbaar naar medewerkers van de Nationale Politie	Username betreft voor- en achternaam van medewerker Nationale Politie, gegevens komen in handen van onbevoegden met als gevolg bedreiging.	Nee	
2	Er wordt extra beveiliging toegepast bij de inlogprocedure.	Username betreft voor- en achternaam van medewerker Nationale Politie, hierdoor zijn accounts makkelijker te hacken omdat enkel nog het wachtwoord ontbreekt. Hacker kan fake berichten publiceren.	Nee	
3	Gebruikers krijgen een training, waarbij specifiek aandacht wordt besteed aan de afhandeling van privé-berichten binnen OBI-engage	Door onjuiste afhandeling kunnen privé berichten met bijvoorbeeld opsporingstips terechtkomen binnen Narrowcasting, gegevens komen in handen van onbevoegden.	Deels	
4	Er is sprake van een ingericht autorisatieproces, waarbij specifiek aandacht wordt besteed aan door- en uitstroom van gebruikers.	Momenteel is er geen goed werkend autorisatieproces wat rekening houdt met in-, door-, en uitstroom van medewerkers, hierdoor blijven accounts onterecht actief.	Nee	
5	Nieuwe releases dienen te worden ontwikkeld en getest in aparte omgeving, er worden hier afspraken overgemaakt met de leverancier.	Momenteel is er geen aparte ontwikkel/testomgeving, hierdoor kunnen er problemen ontstaan binnen de productieomgeving op het gebied van de betrouwbaarheid van de informatievoorziening.	Nee	

1 / 5

Met opmerkingen [5.1 2] **(8):** Betreft eerste gedeelte van het politie e-mail adres . Dus zonder @politie.nl In samenwerking met OBI zijn wij bezig om in 2023 en 2FA in te stellen.

Met opmerkingen [5.1 2] **(9):** Er zit nog een extra stap bij. Er moet nog een derde veld ingevuld worden met de naam van de omgeving waarin men werkt.

1 / 8

Met opmerkingen [5.1 2] **(10):** Alleen in de rol van supersuser heeft met toegang tot de narrowcast zoekopdrachetn

Met opmerkingen [5.1 2] **(11):** Dit stuk kan vervangen worden dat het autorisatieproces op dit moment ingeregeld worden middels de ATL. Afgerond eind 2022.

Met opmerkingen [5.1 2] **(12):** Test omgeving is aangeschaft

[5] Zie tabel 3.3.1
[6] Zie paragraaf 4.2

Nr	Beveiligingseis	Mitigeert dreiging[7]	Wordt aan voldaan ja/nee/deels	Aanbeveling[8]
	Nieuwe releases dienen tijdig kenbaar gemaakt te worden bij de Nationale Politie, zo kunnen er indien nodig aanpassingen worden doorgevoerd aan netwerkzijde van de Nationale Politie en kunnen afwegingen worden gemaakt op het gebied van informatiebeveiliging. Er worden hier afspraken overgemaakt met de leverancier.	Comptabiliteitsproblemen met het netwerk van de Nationale Politie, hierdoor kunnen er beschikbaarheidsproblemen ontstaan.	Deels	1,2

[7] Zie tabel 3.3.1
[8] Zie paragraaf 4.2

4 Conclusie

4.1 Resultaten

In deze beveiligingsanalyse is gezocht naar een antwoord op de vraag: "Hoe kan ervoor gezorgd worden dat de (persoons-)gegevens binnen OBI4wan-Engage voldoende zorgvuldig (lees: veilig) worden verwerkt?

Op basis van de impactanalyse is de betrouwbaarheid van de applicatie als volgt vastgesteld, zie paragraaf 3.2.2:

- Beschikbaarheid: Noodzakelijk
- Integriteit: Bruikbaar
- Vertrouwelijkheid: Intern (Dreiging zit met name in het feit toegang krijgen tot de functionaliteit van OBI4wan-Engage, waarmee onbevoegden fake-berichten zouden kunnen verspreiden). Op basis hiervan zou de classificatie verschuiven naar "vertrouwelijk".

De toepassing beschikt over een goed basisniveau qua beveiliging, de leverancier geeft aan dat men voldoet aan de eisen in bijlage 1 en 2 en kan dit aantonen. Echter zijn na overleg met de leverancier en functioneel beheer een 5-tal specifieke dreigingen geïdentificeerd. Deze kennen een laag tot gemiddeld risico en worden momenteel niet afgedekt door maatregelen.

Met opmerkingen 5. **(13):** 5.2.1 volgens mij

Indien onderstaande aanbevelingen worden uitgevoerd is de verwachting dat het algemeen risico verschuift van "gemiddeld" naar "laag".

4.2 Aanbeveling

Gelet op de uitgangspunten, de gegevensclassificatie en de huidige maatregelen doet het Team Informatiebeveiliging de volgende aanbevelingen:

1. Verantwoordelijke neemt kennis van genoemde dreigingen, risico's en aanbevelingen in dit document;
2. De SLA-overeenkomst wordt aangevuld met de volgende onderwerpen:
   a. Beschikbaarheidseisen business, rekening houdend met incidenten/langdurige uitval;
   b. Uitrol updates/nieuwe releases, rekening houdend met comptabiliteitsproblemen/informatiebeveiliging vanwege SAAS-oplossing->Netwerk Nationale Politie;
   c. Wijzigingsverzoeken business
   d. Backup-recovery plan
   e. Aparte test- en ontwikkelomgeving
   f. Incidentafhandeling
3. Er worden afspraken gemaakt met de leverancier omtrent contractbeëindiging/faillissement, rekening houdend met eigenaarschap/toegang data en continuïteit;
4. Aanpassen en verbeteren inlogprocedure:
   a. username dient niet herleidbaar te zijn naar medewerker Nationale Politie
   b. Toegang tot de applicatie dient beter te worden beveiligd denk bijvoorbeeld aan toevoegen 2-factor authenticatie.
5. Gebruikers krijgen een training voordat toegang wordt verkregen tot OBI-engage, specifiek aandacht is er voor de afhandeling van privé-berichten, voorkomen moet worden dat deze via narrow-casting naar onbevoegden wordt gelekt.

Met opmerkingen 5. **(14):** Nieuw aangepast SLA wordt gemaakt. 1

Met opmerkingen 5. **(15):** Zal altijd een uitdaging blijven ivm SAAS. 1

Met opmerkingen 5. **(16):** Stond al in SLA

Met opmerkingen 5. **(17):** Aangekocht

Met opmerkingen 5. **(18):** Staat in verwerkersovereenkomst

Met opmerkingen 5. **(19):** 2023 1

Met opmerkingen 5. **(20):** Is verwerkt in training 1

6. Leverancier geeft jaarlijks een SOC 2-rapport af en door het jaar heen informatie over de kwaliteit van de dienstverlening, bijvoorbeeld door periodieke Service Level Rapportages.
    a. SOC: Service organization control, een rapportage op basis van vastgestelde principes welke een relatie hebben met de opzet, bestaan en werking van operational IT-controls met betrekking tot uitbestede processen. Deze rapportagestandaard is in het leven geroepen om uitbestede processen beter auditbaar te maken. Kortom er kan accuraat worden getoetst hoe de serviceorganisatie data beheert en/of bewaakt.
7. Richt de applicatie/(controle-)procedures zodanig in zodat er voldaan wordt aan de wettelijke bewaartermijnen:
    a. 5.1.2.e geeft aan dat de bewaartermijn is vastgesteld op artikel 8 Wpg.
8. Functioneel beheer draagt er zorg voor dat er sprake is van een autorisatieproces:
    a. Medewerkers krijgen enkel de functies aangeboden die zij nodig hebben voor hun werk (need-to-know);
    b. Er is aandacht voor door- en uitstroom van medewerkers.

Met opmerkingen 5. (21): Ia al ingericht. 30 maanden

Met opmerkingen 5. (22): Ook deze 2 punten wordt ingeregeld via ATL. (eind 202)

Het spreekt vanzelf dat niet iedere schade kan worden voorkomen. Ingeschat wordt echter dat met deze aanbevelingen een optimum bereikt wordt tussen beveiliging<->operationele omgeving.

POLITIE

Bijlage 1 OWASP-eisen

1. **Injection:** De leverancier heeft maatregelen genomen tegen Injectiekwetsbaarheden zoals sql-, os commando- of ldap-injectie, deze ontstaan wanneer niet-geverifieerde data door een hacker wordt verzonden als onderdeel van een commando of query. Deze data kan onbedoelde commando's uitvoeren of ongeautoriseerde toegang tot gegevens verschaffen.
2. **Broken authentication:** De leverancier heeft maatregelen genomen rondom authenticatiecontrole- en sessiebeheermechanismes, deze worden vaak niet correct geïmplementeerd, waardoor aanvallers de identiteit van andere gebruikers aan kunnen nemen.
3. **Sensitive data exposure:** De leverancier heeft maatregelen genomen om gevoelige data extra te beschermen door middel van versleuteling of andere speciale voorzorgsmaatregelen.
4. **XML external entities:** De leverancier heeft maatregelen genomen tegen verouderde of slecht geconfigureerde xml-verwerkers, deze staan vaak het laden van externe entiteiten toe. Aanvallers kunnen dit misbruiken om bijvoorbeeld toegang tot lokale bestanden te krijgen, os-commando's uit te voeren of DoS-situaties te creëren om het systeem (tijdelijk) onbruikbaar te maken.
5. **Broken access control:** De leverancier heeft maatregelen genomen rondom gebruikersrechten binnen de applicatie. Beperkingen wat een gebruiker wel of niet mag uitvoeren binnen een applicatie worden in veel gevallen niet correct afgedwongen. Aanvallers kunnen deze fouten misbruiken om toegang te krijgen tot functionaliteit en/of informatie zonder dat ze hiertoe geautoriseerd zijn.
6. **Security misconfiguration:** De leverancier heeft maatregelen genomen rondom een correcte configuratie die wordt afgestemd op de applicatie, frameworks, applicatieserver, webserver, databaseserver en platform. Beveiligingsinstellingen moeten worden gedefinieerd, geïmplementeerd en onderhouden omdat deze standaard vaak onveilig zijn. Daarnaast moet alle software up-to-date zijn.
7. **Cross-site scripting:** De leverancier heeft maatregelen genomen tegen xss-injectie, als een applicatie gegevens zonder filtering en/of encodering naar een web browser zendt stelt dit aanvallers in staat om scripts uit te voeren, gebruikerssessies te kapen, websites te beschadigen of de gebruiker naar andere sites te leiden.
8. **Insecure Deserialization:** De leverancier heeft maatregelen genomen tegen onveilige deserialisatie, Applicaties converteren objecten alvorens deze worden opgeslagen. Het terug converteren van deze objecten gebeurt vaak onveilig en kan worden misbruikt om os commando's uit te voeren. In sommige gevallen stelt het de applicatie zelfs kwetsbaar op voor andere injectie aanvallen.
9. **Components with vulnerabilities:** De leverancier maakt enkel gebruik van betrouwbare componenten, Componenten zoals libraries, frameworks en andere software-modules draaien vaak met volledige autorisatie. Als een kwetsbaar onderdeel wordt geëxploiteerd kan dit tot dataverlies leiden of een overname van de server faciliteren. Componenten met reeds bekende kwetsbaarheden ondermijnen de beveiliging van de applicatie en faciliteren een scala aan mogelijke aanvallen.
10. **Insufficient logging & monitoring:** De leverancier heeft maatregelen genomen rondom logging en monitoring. Een tekort aan logging en monitoring kan aanvallers de tijd geven zich dieper in een systeem te nestelen en proberen zich permanent toegang te verschaffen.

POLITIE

Bijlage 2 Cloud Security Principles

Met opmerkingen 5. **(23):** 5.1.2.e heft hier al een advies over geschreven

1. **Data in transit protection:** De leverancier heeft maatregelen genomen tegen tampering en eavesdropping, door netwerkbeveiliging en encryptie:
    a. Data in transit is beveiligd tussen de end-user en de service.
    b. Data in transit is beveiligd binnen de service.
    c. Data in transit is beveiligd tussen meerdere services.
2. **Asset protection:** De leverancier heeft maatregelen genomen tegen diefstal, verlies, beschadiging en tampering van data en apparatuur:
    a. Er kan worden aangetoond waar (locatie) de data wordt opgeslagen
    b. Er kan worden aangetoond vanuit welke locatie beheer plaatsvindt
    c. Er kan worden aangetoond dat er fysieke beveiligingsmaatregelen genomen zijn binnen het datacenter
    d. Data at rest is beveiligd tegen onbevoegde toegang door middel van encryptie of overige security controls.
    e. Data/accountgegevens worden binnen de afgesproken termijn op juiste wijze vernietigd
    f. End-of-live apparatuur wordt op juiste wijze vernietigd.
    g. De dienst voldoet aan de afgesproken beschikbaarheidseisen.
3. **Seperation between users:**
    a. Er kan worden aangetoond dat de data niet vermengd wordt met data van overige partijen.
4. **Governance framework:**
    a. Er kan worden aangetoond dat er sprake is van een governance framework:
        i. Er is een functioneel verantwoordelijke voor beveiliging binnen de dienst
        ii. Het bestuur van de dienst wordt op de hoogte gehouden door middel van rapportages op het gebied van informatiebeveiliging
        iii. Er is een continue proces tussen identificeren kwetsbaarheden en compliancy/voldoen aan standaard richtlijnen.
5. **Operational security:** De leverancier heeft maatregelen genomen om de dienst op juiste wijze te beheren:
    a. Er kan worden aangetoond dat er sprake is van een juiste configuratie en change management.
    b. Er kan worden aangetoond dat vulnerability management plaatsvindt
    c. Er kan worden aangetoond dat de dienst wordt gemonitord (detectie van aanvallen)
    d. Er kan worden aangetoond dat er procedures zijn op het gebied van incident management.
6. **Personnel security:** De leverancier heeft maatregelen genomen om zorg te dragen voor betrouwbaar beheerpersoneel:
    a. Er kan worden aangetoond dat medewerkers die beheer uitvoeren een screening doorlopen hebben en geheimhouding getekend.
    b. Er kan worden aangetoond dat er continue gewerkt wordt aan awareness op het gebied van informatiebeveiliging.
7. **Supply chain security:** De leverancier heeft maatregelen dat onderaannemers aan eenzelfde niveau van beveiliging voldoen:
    a. Er kan worden aangetoond hoe data gedeeld wordt met overige partijen
    b. Er kan worden aangetoond welke beveiligingseisen zijn gesteld aan onderaannemers

8. **Secure user management:** De leverancier heeft maatregelen genomen op het gebied van gebruikersondersteuning:
    a. Er kan worden aangetoond dat er authenticatie plaatsvindt voordat er wijzigingen binnen de dienst worden uitgevoerd. (een onbevoegde die de helpdesk belt moet niet zomaar wijzigingen kunnen doorvoeren op verzoek)
9. **Idendity & authentication:** De leverancier heeft maatregelen genomen op het gebied van idendity & authentication controls:
    a. Er kan worden aangetoond dat er idendity & authentication controls actief zijn voordat gebruikers toegang krijgen tot specifieke gebieden van de applicatie.
10. **External interface protection:** De leverancier heeft maatregelen genomen zodat alle interfaces zijn geïdentificeerd en beveiligd:
    a. Er kan worden aangetoond met welke fysieke en logische interfaces de data toegankelijk is en hoe deze interfaces zijn beveiligd.
11. **Secure service administration:** De leverancier heeft maatregelen genomen voor het inrichten van een beheermodel overeenkomstig met de best practices of overige richtlijnen binnen de branche.
    a. Er kan worden aangetoond welk beheermodel gebruikt wordt en welke risico's dit met zich meebrengt in relatie tot de data.
12. **Audit information:** De leverancier heeft maatregelen genomen op het gebied van auditinformatie richting klanten.
13. **Secure use of the service:** De leverancier heeft duidelijk gemaakt welke onderhouds- en of beheerwerkzaamheden verantwoording zijn van de afnemer.