

Interne Memo

Aan 5.1.2.e

Onderwerp

Beoordeling documenten
OBI4WAN

Organisatieonderdeel

Politie Diensten Centrum
Dienst IM
Team Informatie Beveiliging

Behandeld door

5.1.2.e

Functie

IV-Expert

Telefoon

+31 5.1.2.e

E-mail

5.1.2.e @politie.nl

Ons kenmerk

PC 5.1.2.i

Uw kenmerk

Klik hier als u tekst wilt invoeren.

In afschrift aan

Klik hier als u tekst wilt invoeren.

Datum

3 juni 2019

Bijlage(n)

0

Pagina

1

Beste 5.1.2.

Samen met 5.1.2.e, afdeling Veiligheid & Continuïteitsmanagement, heb ik naar de geleverde documenten van OBI4WAN gekeken.

Hieronder staan onze bevindingen.

Met betrekking tot de ISO certificaten:

- Certificaat ISC274 (OBI4Wan) verwijst naar een statement of applicability (SoA) met als datum 13-02-2018
- Certificaat ISC 269 (HowAboutYou) verwijst naar een statement of applicability met datum 25-06-2018
- Bij de stukken is wel een SoA meegeleverd maar die is niet gedateerd.
- We kunnen dus niet nagaan of de geleverde SoA gelijk is aan de SoA's die genoemd zijn bij de Certificaten

Met betrekking tot de Nadere overeenkomst:

- De Nadere Overeenkomst vermeld 7 bijlagen die onlosmakelijk verbonden zijn met de overeenkomst.
- Deze bijlagen zijn niet meegeleverd.
- We hebben die bijlagen niet kunnen beoordelen
- Ons valt op dat de offerte waarop de Nadere Overeenkomst gebaseerd is komt van Protinus IT.

Met betrekking tot de verwerkersovereenkomst:

- Uit de stukken maken we op dat er (minstens) drie partijen betrokken zijn bij de dienstverlening
 1. Protinus als aanbieder van de tooling
 2. OBI4Wan als maker van de software
 3. HowAboutYou als serviceverlener mbt de online media monitor
- In de verwerkersovereenkomst wordt alleen OBI4wan genoemd
- Wij verwachten dat de overige partijen ook in de verwerkersovereenkomst is opgenomen
- Het is ons niet helder wie de verwerker is en welke partijen subverwerkers zijn.
- In de verwerkersovereenkomst wordt een oud email adres gebruik 5.1.2.i @vtspn.nl het domein vtspn.nl is niet meer in gebruik.

**Onderwerp**

Beeoordeling documenten
OBI4WAN

Datum

3 juni 2019

Pagina

2 van 2

Met betrekking tot de Dienstbeschrijving.

- Uit de Dienstbeschrijving is niet te achterhalen hoe de verkeerstromen lopen.
- Ook kunnen we niet bepalen op welke plekken controles in de verkeerstromen moeten/kunnen plaatsvinden (bv websocket)
- We willen graag meer duidelijkheid over de verkeerstromen.
-

Conclusie:

De geleverde documenten zijn niet consistent en/of volledig.

Op basis van de geleverde stukken kunnen we niet met zekerheid aannemen dat alle zaken rondom de beveiliging goed geregeld zijn.

Antwoorden op de oorspronkelijke vragen:

1. Is een SOC2 verklaring noodzakelijk of kan een ISO 27001 certificaat volstaan?
Aangezien ons niet helder is of de geleverde SoA hoort bij de twee certificaten vinden we op dit moment een ISO 27001 certificaat onvoldoende
2. Mag een politie email adres gebruikt worden als gebruikersnaam?
Dat mag pas als de beveiliging is voldoende is aangetoond (nu nog niet het geval) en het contract en de verwerkersovereenkomst(en) volledig zijn.
3. Mag Websocket ongecontroleerd doorgelaten worden?
Omdat de beveiliging naar onze mening (nog) niet voldoende ingericht kan dit niet toegestaan worden.

Nadere afstemming tussen ons en project en de leverende partij(en) vinden we noodzakelijk.