Classificatie: RIVM Vertrouwelijk

RIVM
Risicoanalyse rapportage

IB Risicoanalyse CIMS-CBS datalevering

Inhoud

Scope omschrijving

Deze IB risicoanalyse is gedaan ten behoeve van het onderzoeksvoorstel CIMS-CBS datalevering.

In het onderzoeksvoorstel wordt getracht de vraag te beantwoorden rondom verschillen in vaccinatiebereidheid onder verschillende bevolkingsgroepen, waarover tot nu weinig bekend is. In dit voorstel wordt het CBS naar voren geschoven als verzamelaar en vervolgens als onderzoeksomgeving om bovenstaande vraag te beantwoorden.

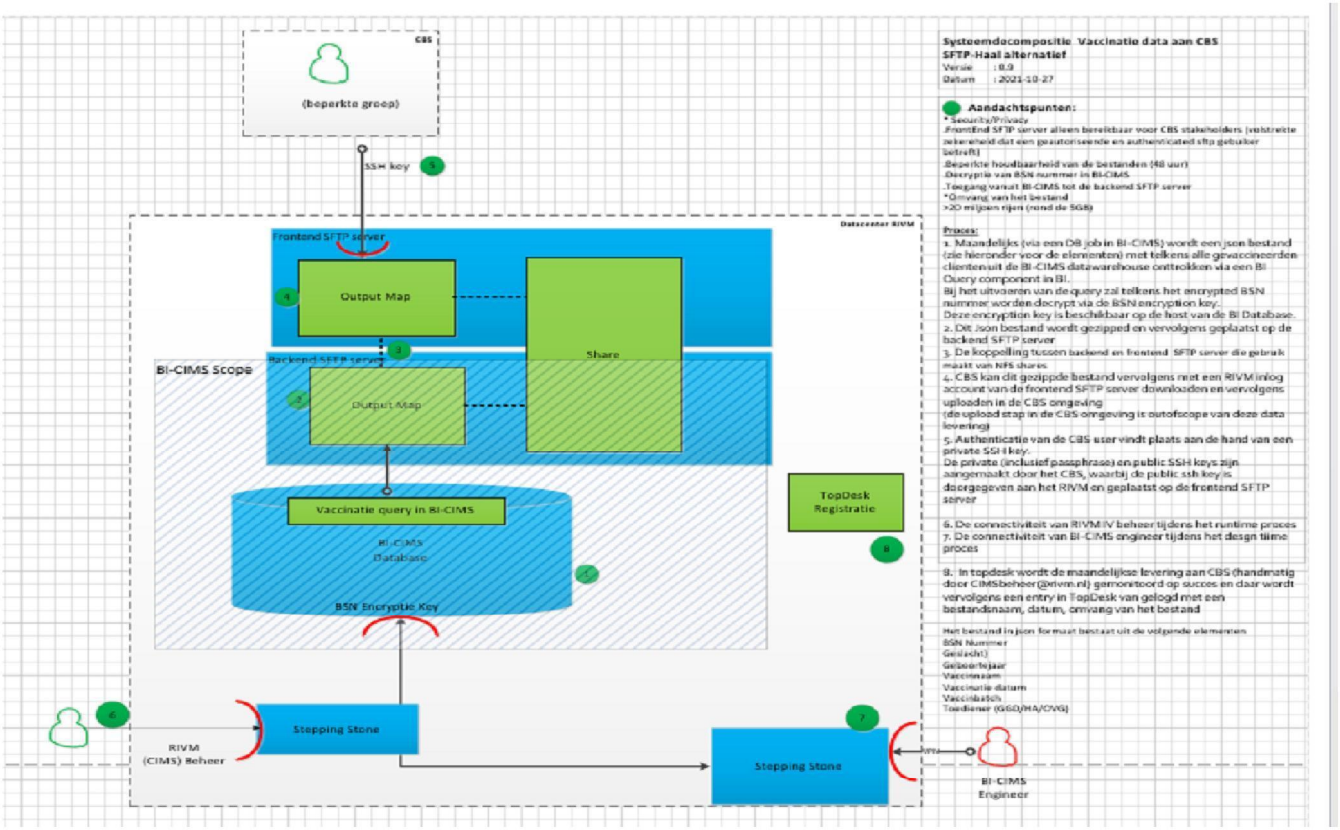
Naast data van de GGD en uiteraard data van het CBS zelf zullen de vaccinatie gegevens van het RIVM een van de bronnen zijn waarop het onderzoek zal gaan plaats vinden. Hiertoe zal er op regelmatige basis (maandelijks) vanuit het RIVM een vaccinatie data set richting het CBS worden aangereikt. De vaccinatiedata worden nu (nog) niet ter beschikking gesteld aan het CBS. De data komen in de RA omgeving van het CBS terecht, waarna RIVM onderzoekers er analyses mee kunnen gaan doen

In het technisch document 'DPV_316Vaccinatiedatalevering aan het CBS' is een beschrijving opgesteld op welke wijze, wanneer, vanuit welke RIVM bron, met welke selectie criteria deze vaccinatie data set op een veilige en verantwoorde wijze ter beschikking aan het CBS wordt gesteld.

Andere koppelingen zoals genoemd in het onderzoeksdocument (bijvoorbeeld de vaccinatie data vanuit de GGD) vallen buiten scope

De CBS vaccinatie data set zal beschikbaar worden gesteld via een RIVM SFTP server/directory bij het RIVM, die vervolgens door het CBS kan worden opgehaald

Systeemdecompositie/Scope



MANAGEMENTSAMENVATTING

Management Samenvatting

- Dreigingscategorie Actieve aanvaller (extern en intern): Rechtstreekse aanval op de ICT-omgeving vanuit publieke omgeving of interne omgeving met weinig rechten(hackaanval)/ Misbruik van legitiem of niet-legitiem verkregen autorisaties/Social engineering/Malware/Agressie, geweld en intimidatie:

Kans: Laag

Impact: Midden

Risico: Laag-Midden

- Dreigingscategorie: Menselijke fouten

Kans: Laag

Impact: Midden

Risico: Laag-Midden

- Dreigingscategorie: Technische fouten/falen

NVT

Op grond van bovenstaande is er geen behoefte aan een risicoacceptatie

AANPAK RISICOANALYSE

FA

Fase I	Fase II	Fase III	Fase IV	Fase V
CONTEXT	IMPACT	DREIGINGEN	WEERBAARHEID	RAPPORTAGE
Situatieschets van locaties, systemen, informatie & toegang	*Classificatie van proces, systeem en informatie (BIV) & BBN niveau*	*Inzicht in dreigingen & kwetsbaarheden, de consequenties en kans dat het zich voordoet*	*Inventarisatie huidige maatregelen & voorstel aanvullende maatregelen*	*Vastlegging van risico's, maatregelen & terugkoppeling*

Fase 3: Dreigingen

(impact, kans en risico)

Dreigingscategorie Actieve aanvaller (extern en intern):

Rechtstreekse aanval op de ICT-omgeving vanuit publieke omgeving of interne omgeving met weinig rechten(hackaanval)/ Misbruik van legitiem of niet-legitiem verkregen autorisaties/Social engineering/Malware/Agressie, geweld en intimidatie:

Kans: Laag

Impact: Midden

Risico: Laag-Midden

- Gebruik van de onrechtmatig verkregen inloggegevens: Er is multi factor authentication van toepassing; hierdoor wordt de kans hierop behoorlijk bemoeilijkt en verkleind. Dit kan dus als mitigerende maatregel beschouwd worden
- Misbruik van een kwetsbaarheid in het authenticatie en autorisatiemechanisme: Er is multi factor authentication van toepassing; hierdoor wordt de kans hierop behoorlijk bemoeilijkt en verkleind. Dit kan dus als mitigerende maatregel beschouwd worden CIMS beheer en beheerder binnen CBS zouden theoretisch gezien misbruik kunnen maken, maar herleidbaarheid is groot. Logging is ingericht
- Session Hijacking (bijvoorbeeld session replay-aanvallen): Uitwisseling vindt 1x per maand plaats met tijdsslot van 48 uur; dit vindt ook niet elke keer op hetzelfde tijdstip plaats. De kans is klein dat zich hierdoor een geplande aanval wordt uitgevoerd. Tevens is de data (at rest en in transit) versleuteld. Het type data leent zich er ook minder voor om als doelwit te dienen voor kwaadwillenden.
- Rechtstreeks misbruik van een kwetsbaarheid (ontbreken patch, misconfiguratie) in de infrastructuur: Als dit zich zou voordoen gaat het om een beperkte dataset waarbij de oorspronkelijke data niet geraakt wordt
- Afluisteren van netwerkverkeer: Het gaat om versleutelde data in een afgeschermde omgeving (zie technische details: Remote Access omgeving; SFTP server/directory bij het RIVM)
- Diefstal (lezen)/fraude/lekken van (gevoelige) gegevens: Dit zou zich theoretisch kunnen voordoen, maar de kans hierop is klein aangezien er gewerkt wordt met een beperkte groep medewerkers/professionals die uiteraard gescreend zijn en een geheimhoudingsverklaring getekend hebben. Als dit zich door toedoen van een kwaadwillende toch zou voordoen zijn blijven de gegevens in de brondatabase hetzelfde. Er wordt tevens gelogd (heel belangrijk) dus er is een audittrail. Risico op misbruik eigen medewerkers is te verwaarlozen,
- Beheerders loggen in met persoonsgebonden accounts die ook worden gelogd. De economische waarde van de beperkte datasets die maandelijks worden verstuurd is laag dus niet interessant voor criminelen en/of statelijke actoren. Social engineering, sabotage, vernieling en afluisteren daardoor niet van toepassing

Overige aandachtspunten:

- Bespreken mogelijkheden Vulnerability scan/Pentest (na livegang)