Welke maatregelen zijn genomen om de kans op een inbreuk te beperken

Toegangscontrole CIMS

- Wie heeft toegangsrechten in CIMS
- welke rechten/rollenstructuur is er
- hoeveel mensen hebben toegang
- hoe zijn deze mensen aan RIVM verbonden
- welke query rechten / rapportage rechten zijn er binnen CIMS
- welke export- en downloadmogelijkheden zitten er binnen CIMS
- welke grootschalige rapportages (lijstjes met 10+ burgers, met gedetailleerde gegevens) zijn te genereren)
- zijn deze laatste rechten (export / download / rapportage) voorbehouden aan specifieke rollen
- wordt afwijkend gedrag (bv 'select BSN nummer from BSNtabel') gemonitored
- leidt afwijkend gedrag tot een signaal / incident
- welke logging vindt plaats op activiteiten van gebruikers (raadplegen, wijzigen, verwijderen, ...)
- hoe vaak worden logs gecontroleerd en hoe vindt dit plaats (handmatig / geautomatiseerd)
- hoe lang worden deze logs opgeslagen en wie kan hier bij
- welke beheerrollen bij CIMS zijn aanwezig, zijn deze intern / extern belegd
- wat zijn hun toegangsmogelijkheden en hoe wordt hun werk gemonitord

Er is geen sprake van 2FA, bij mijn weten. Hoe wordt nu toegang verkregen tot CIMS?

- gebruikersnaam / wachtwoord?
- is er sprake van toegangsbeperking obv werkplek / IP adres

Gegevensverwerking bij inlezen via SFTP

- SFTP. De bestanden staan enige tijd op de SFTP server. Normaal enkele seconden. Afhankelijk van de grootte en netwerkproblemen kan dit langer zijn. In die tijd kan het bestand ook worden gedownload.
- SFTP. Het bestand is niet end-to-end encrypted. Hierdoor is het risico groot dat het ook aan de bron op een filesysteem staat wat niet met de andere waarborgen omkleed is.

Gegevensverwerking via mail

- Hoe controleren we dat de afzender juist is en dat niet versloft. Anders is het wel heel makkelijk met een breed verspreidde specificatie om jezelf als ingeënt te laten registreren.
- Iedereen kan met zorgmail mailen (en NTA-compliant opereren).
- Over zorgmail. Zodra de ontvanger de bestanden uitpakt zijn ze niet meer encrypted en moeten ze getransporteerd worden. Vanaf de werkplek naar een disk is problematisch.

Gegevensverwerking in de database

- Waar vindt de verwerking plaats (bij RIVM of provider)

- Is de database enrypted
- 'BRP-backup'. "Het staat maar 2 weken op disk (of stond), maar er zijn wel backups van die nog 9 maanden bestaan." Klopt dit? Hoe ziet het backup proces er uit.

Welke maatregelen zijn genomen om de impact van een datalek te beperken

Klopt het dat dat gegevens uit COA en Probas in release 1.0 nog niet worden ingelezen?

Wat wordt gedaan met gegevens die eventueel teveel worden verkregen vanuit BRP, bijvoorbeeld:

- van mensen die RIVM uiteindelijk niet oproept omdat ze op een andere manier worden opgeroepen,
- niet worden gevaccineerd omdat ze jonger zijn dan 18 jaar,
- zich niet laten vaccineren,
- niet reageren op een oproep of aangeven dat ze willen dat RIVM geen gegevens van ze registreert).

Het is mij niet helder:

- welk beleid RIVM hierin heeft gehanteerd en welke keuzes zijn afgewogen;
- hoe de architectuur van CIMS release 1.0 de intrinsieke mogelijkheden heeft om gegevens die niet gebruikt worden te scheiden van gegevens die wel gebruikt worden;
- welk deel van de gegevens nodig zijn en welke niet (geboorteland, voornamen);
- hoe zij de gegevens die niet gebruikt worden versneld kan verwijderen (aangezien deze niet automatisch dezelfde bewaartermijn hebben);
- hoe dit effectief is, als steeds opnieuw de BRP wordt ingelezen.

Te allen tijde moet worden voorkomen dat de schijn kan ontstaan dat de overheid 'zwarte lijsten' zou kunnen maken van vaccinatieweigeraars.

Ik vertrouw er op dat CIMS hier in haar werkwijze rekening mee heeft gehouden dat op een of andere manier te achterhalen is wie wel op oproepen heeft gereageerd en wie niet (en dus een potentiele weigeraar is), maar zou hier graag een nadere onderbouwing van zien.

Een paar punten:

- Gevoeligheid: Gegevens van de GGD waar geen opt-in voor is gegeven zijn gepseudonimiseerd, niet geanonimiseerd. Hierbij blijft het mogelijk zonder hulp van de GGD deze gegevens terug te halen. Dit contractueel dichttimmeren is een risico als het toch per ongeluk wordt gepubliceerd en men kan de gegevens terughalen.