Rijksinstituut voor Volksgezondheid
en Milieu
*Ministerie van Volksgezondheid,
Welzijn en Sport*

A. van Leeuwenhoeklaan 9
3721 MA Bilthoven
Postbus 1
3720 BA Bilthoven
www.rivm.nl

KvK Utrecht 30276683

T 030 5.1.2e
5.1.2e@rivm.nl

VWS

Datum
27 januari 2021

Ons kenmerk
DVP_216

Behandeld door
5.1.2e 5.1.2e
5.1.2e 5.1.2e 5.1.2e
5.1.2e 5.1.2e 5.1.2e 5.1.2e
5.1.2e 5.1.2e
5.1.2e 5.1.2e
5.1.2e 5.1.2e
5.1.2e 5.1.2e 5.1.2e 5.1.2e

memo

Centraal vaccinatieregister CIMS: het voorkomen van illegale handel in data

Aanleiding en doel

Media meldden op 25 jan 2021*: "Illegale handel in privégegevens miljoenen Nederlanders uit coronasystemen GGD"*. Voorliggende memo beschrijft de kenmerken van de GGD-casus als risicofactor en de door RIVM getroffen mitigerende maatregelen voor wat betreft risico's in het gebruik van het centrale registratiesysteem ten behoeve van de covid-vaccinatie. Tevens wordt aangegeven welke extra maatregelen versneld worden ingevoerd voor verbetering en borging van de PDCA-cyclus. In de bijlage is een beknopt overzicht gegeven van de kenmerken van de GGD-casus.

Kenmerken centrale verwerking vaccinatiegegevens: risico-inschatting en maatregelen

In onderstaande paragraaf wordt uiteengezet welke maatregelen per risico zijn genomen om met name genoemde risico's in de GGD-casus te kunnen ondervangen, of waar mogelijk helemaal geen sprake van is. Dit laatste heeft met name te maken met het verschil in aantallen medewerkers die toegang hebben tot het centrale systeem CIMS.

1. **Personeelsbeheer**
   Om centrale gegevensverwerking mogelijk te maken is veel werk verzet vanuit verschillende disciplines. Medewerkers hebben toegang tot het systeem alleen voor de voor hen noodzakelijke functies. Dit is afgedekt met een zogeheten rollen/rechtenmatrix, waarbij tot op schermniveau bepaald is wie wat kan hierin. Zoals al aangegeven staat het aantal medewerkers dat toegang heeft tot CIMS (85 bij start van de vaccinatiecampagne tot oplopend ca. 135 personen tijdens de piek in de campagne) in geen verhouding tot de genoemde aantallen bij de GGD (26.000 personen + externe organisaties). Medewerkers van het call center (Infopunt RIVM) en het meldpunt corona hebben geen toegang tot de persoonsgegevens.

Datum
27 januari 2021

Ons kenmerk
DVP_216

In onderstaande tabel wordt per rol uitgesplitst hoeveel medewerkers toegang hebben tot CIMS.

Rol	Beschrijving	Risico	Totaal	Genomen maatregelen
CIMS medewerker	Negen ingehuurde medewerkers op de regiokantoren van DVP (RIVM) t.b.v. verwerking vaccinatiegegevens, drie vaste medewerkers. Er wordt vanuit gegaan dat het totaal aantal medewerkers op de regiokantoren tot maximaal 50 medewerkers zal stijgen. Daarnaast vindt cliëntbeheer plaats door zeven interne RIVM-medewerkers.	High (extern)	19	1. Verplicht op kantoor aanwezig (thuis database raadplegen is niet mogelijk). 2. Geen mogelijkheid tot printen of gebruik USB. 3. Deze mensen hebben een VOG en geheimhoudingsverklaring afgegeven. 4. Awareness sessies privacy en informatiebeveiliging. 5. Maximaal 30 records tegelijk open ter controle en verwerking. 6. Wekelijks wordt o.l.v. een extra aangestelde teamleider met de medewerkers de stand van zaken besproken en aandacht gevraagd voor de bijzondere verwerkingen. 7. Aandacht wordt gevraagd ook om terughoudend te zijn op sociale media.
Ontwikkelteam	Acht medewerkers van de leverancier betrokken bij doorontwikkeling CIMS en technische applicatiebeheer. Waarvan vijf personen toegang hebben tot productiedata. Drie RIVM medewerkers hebben toegang tot productiedata via de applicatie. Deze 3 medewerkers hebben ook via SQL-tooling toegang tot de database.	High: extern Low: intern	11	8. Medewerkers leverancier hebben een VOG overlegd en integriteitsverklaring afgegeven. 9. Er wordt toegang verschaft via een beveiligde VPN-verbinding tussen leverancier en intern gehoste applicatie. Het ontwikkelteam werkt thuis, waarbij interne RIVM-medewerkers via 2FA toegang krijgen tot de VDI van RIVM, vervolgens op basis van username en password CIMS kunnen benaderen. 10. Logging van activiteiten vindt plaats op zowel databaseniveau als applicatieniveau. 11. SIEM/SOC is ingericht om inzage te krijgen in de logging en direct te kunnen acteren bij verdachte wijzigingen in het systeem. 12. De acceptatieomgeving is geanonimiseerd
Functioneel beheer	Functioneel beheer CIMS twee inhuur en zes RIVM-medewerkers voor eerstelijnssupport CIMS en doorvoeren wijzigingen.	High (extern) Low (intern)	15	13. Medewerkers leverancier hebben een VOG overlegd en integriteitsverklaring afgegeven. 14. Eigen medewerkers hebben een integriteitsovereenkomst getekend. 15. Via rollen en rechten op het systeem beschikken beheerders nooit over meer rechten dan strikt noodzakelijk.
Technisch beheer	Onderscheid gemaakt tussen: Databasebeheer: 5 Core infra tbv netwerk: 17 Specifieke hosting Linux: 15 Platformbeheer: 8 Generieke hosting: 20	High (aantallen)	53	16. Medewerkers leverancier hebben een VOG overlegd en integriteitsverklaring afgegeven. 17. Eigen medewerkers hebben een integriteitsovereenkomst getekend. 18. Vierogen-principes bij opleveren changes en incidenten. 19. Alle activiteiten worden gelogd op persoonsniveau. 20. Backups geencrypt en alleen door specifieke hostging i.s.m. Leverancier te ontsleutelen en toegankelijk te maken. 21. Alleen toegang via beveiligde accounts. 22. Logging van toegang wordt ingelezen door SIEM SOC. 23. Toegang alleen via beheer VDI, geen directe ontsluiting naar buiten van systemen. 24. Externe beheerders van leverancier alleen toegang via no split VPN en steppingstone server. 25. Maandelijks vindt review van uitgegeven accounts plaats en waar nodig worden accounts gedisabled.
NB: de aantallen technisch beheer betreffen totalen. Deze hebben niet allen toegang tot CIMS of zijn direct bij CIMS betrokken. Het risico kan bestaan dat een netwerkbeheerder omgekocht wordt om een poort open te zetten dat de achterdeur van CIMS vormt. Vandaar dat deze rollen hier wel benoemd worden. Alleen specifieke hosting- en platformbeheer hebben tot op zekere hoogte toegang tot de applicatie CIMS.				

Datum
27 januari 2021

Ons kenmerk
DVP_216

2. Toegangsbeheer

Het toegangsbeheer is conform de eisen van het RIVM ingericht en verschillen niet van die van vergelijkbare systemen. Een autorisatiematrix gebaseerd op rollen en rechten vormt de basis. Verder is toegang tot de werkomgeving van RIVM (VDI-omgeving) alleen mogelijk voor geregistreerde medewerkers met een eigen login. Dit kan alleen op basis van 2FA middels een one-time password. Toegang tot CIMS vindt vervolgens plaats op basis van username en password.

3. Informatiebeheer

Uitgangspunt is geautomatiseerde dataverwerking. Aanleverende partijen moeten voldoen aan de aansluitvoorwaarden van RIVM.

Het beheer van informatie is opgedeeld in diverse functies. Cliëntbeheer is bijvoorbeeld een aparte functie binnen CIMS en is slechts aan een beperkt aantal medewerkers toebedeeld. Ook is hiervoor een aparte training beschikbaar en gelden specifieke procedures om gebruik te mogen maken van de toegang tot de clientmodule die de BRP-gegevens bevat.

Voor de CIMS-medewerkers zelf is een specifieke werkinstructie geschreven waarin toegelicht wordt op welke manier met de onderscheiden modules in CIMS moet worden omgegaan. Het is bijvoorbeeld niet mogelijk om dataexports te maken, de printfunctie is niet beschikbaar en de binnenkomende databestanden worden allemaal geautomatiseerd verwerkt.

Alle verwerkingen door personen worden op naam en ongeacht de rollen en rechten gelogd. Logging van activiteiten vindt plaats op zowel het databaseniveau als op het applicatieniveau. Het SIEM/SOC is ingericht om inzage te krijgen in de logging en direct te kunnen acteren bij verdachte wijzigingen in het systeem. De logs worden wekelijks geanalyseerd door de SIEM/SOC.

4. Extra maatregelen

De GGD-casus was voor RIVM aanleiding voor mogelijke extra maatregelen, naast de genomen maatregelen zoals benoemd in het document Oplegnotitie Risico register CIMS 1.0 05012021 vs. 0.9. Deze extra maatregelen worden toegevoegd aan de roadmap (DPV_210 Roadmap covid registratie).

Risico	Extra maatregelen
Personeel	1. Extra awareness vergroten bij nieuwe medewerkers. 2. Procedures rondom in-en uitdiensttreding extra scherp, up-to-date houden van toegangsrechten op alle niveaus. 3. Controle of alle afgegeven verklaringen (VOG, integriteit, geheimhouding) geldig zijn en in dossier zijn. Te doen voor 1 feb 2021.
Informatiebeveiliging	4. Verhogen frequentie van controle op toegangsrechten en controle lograpportages (wekelijks).. 5. Maandelijkse quickscan voor IB invoeren. 6. Versnellen realisatie SIEM/SOC verbeteringen. 7. Pentest op CIMS uitvoeren (wordt ingepland met ADR). 8. Extra audit op het geheel uitvoeren.
Ontwikkeling	9. Mogelijkheid onderzoeken tot het inbouwen van een *break-the-glass* systeem om onnodige zoekopdrachten of bovengemiddelde aantallen zoekopdrachten te detecteren en een waarschuwing te doen uitgaan.

5. Conclusie

RIVM neemt privacy en informatiebeveiliging zeer serieus. De GGD-casus was voor RIVM extra aanleiding om:

1. Huidige genomen maatregelen te evalueren;
2. De borging van die maatregelen te controleren;
3. Na te gaan of versnelling mogelijk is op de huidige maatregelen;
4. Extra maatregelen te nemen waar gewenst om op een nog hoger beschermingsniveau te komen.

Duidelijk is geworden in het geval van de GGD-casus dat de menselijke factor van niet te onderschatten belang is. Extra aandacht voor personeel, zowel intern als extern is van groot belang om het risico op gedwongen criminele activiteiten te beperken en direct actie te kunnen ondernemen wanneer signalen daartoe aanleiding geven.

Datum
27 januari 2021

Ons kenmerk
DVP_216

BIJLAGE - Organisatorische kenmerken/ risico's van de GGD-casus [1]

De casus grootschalige handel in persoonsgegevens uit GGD-systemen is een op zichzelfstaande casus die desalniettemin gevolgen heeft voor de opzet van CIMS, de risico's die onderkend zijn en de te nemen of reeds genomen maatregelen om de risico's te verkleinen.

Kenmerkend voor de GGD-casus:

1. Grootschalige handel door medewerkers;
2. Miljoenen adresgegevens, telefoon- en burgerservicenummers, en medische persoonsgegevens;
3. Inloggegevens van medewerkers zijn door die medewerkers verkocht;
4. Er is sprake van twee databronnen;
5. Toegang door ca. 26.000 medewerkers, inclusief medewerkers call centra;
6. Onbekend aantal mensen heeft extern toegang (Rode Kruis, ANWB, callcentre Teleperformance);
7. Medewerkers werken vanuit huis;
8. Medewerkers zijn omgekocht;
9. Medewerkers hebben VOG overlegd en geheimhoudingsverklaring afgegeven;
10. Steeksproefgewijs controle onder medewerkers.

Overige kenmerken van de casus:

1. Verantwoordelijken waren niet op de hoogte van de illegale handel;
2. Actieve advertentie/ aanbod;
3. Handel aangeboden via chatdiensten (Telegram, Snapchat, Wickr);
4. Tientallen accounts van de chatdiensten;
5. Handel via verschillende grote chatgroepen;
6. Handel gedurende maanden;
7. Handel is specifiek per persoon op aanvraag;
8. Opbrengst euro 30-50 per persoon
9. Handel in grote (tienduizenden personen) datasets;
10. Opbrengst tienduizenden euro's per grote dataset;
11. Betaling in Bitcoin of betaalkaart;
12. Proefinzage bij verkoop grote datasets;
13. Aangifte van datadiefstal;
14. Twee arrestaties.

[1] Bron van de kenmerken: https://www.rtlnieuws.nl/nieuws/nederland/artikel/5210644/handel-gegevens-nederlanders-ggd-systemen-database-coronit-hpzone