College

Raadsinformatiebrief

Aan	Raad
Portefeuillehouder	Marijo Immink
Onderwerp	Raadsinformatiebrief update datadiefstal GGD
Datum	23-02-2021

Kennisnemen van
Stand van zaken datadiefstal GGD

Inleiding
In de media is momenteel veel aandacht voor de datadiefstal GGD. Wij willen u dan ook graag nader informeren over de situatie en wat GGD Hart voor Brabant heeft gedaan.

Informatie algemeen
De afgelopen weken is er veel gesproken, geschreven en gespeculeerd over de gestolen data uit de GGD-systemen. Van essentieel belang is eerst en vooral dat het onderzoek van de politie daarnaar nog loopt. Wel heeft GGD GHOR Nederland het nodig gevonden om over het incident te communiceren. Via deze link: https://ggdghor.nl/actueel-bericht/ggd-en-haar-data-hoe-zit-het-echt-een-repliek/ vindt u een repliek vanuit GGD GHOR Nederland. Daarnaast vindt u via een tweede link een overzicht met veel gestelde vragen en antwoorden over het incident;
https://ggdghor.nl/thema/vragen-antwoorden-datadiefstal/

Intensivering toezicht
In het kader van het toezicht dat de AP dient te houden op de veiligheid van de gegevens in de GGD-systemen en de naleving van de Algemene Verordening Gegevensbescherming (AVG) mag het geen verbazing wekken dat dit toezicht naar aanleiding van het incident is geïntensiveerd.

Stand van zaken onderzoek
Geen van de gearresteerde vijf personen was werkzaam bij GGD. Er zijn tot op heden ook geen aanwijzingen ontvangen van politie en justitie dat (vaste of ingehuurde) medewerkers van de GGD worden verdacht. Ook heeft de GGD zelf intern nadere checks uitgevoerd van onze ‘logging-bestanden’ op eventuele onregelmatigheden. De GGD heeft geen onregelmatigheden aangetroffen. De GGD heeft dus ook op basis van eigen onderzoek op dit moment geen aanwijzingen dat door onze medewerkers data zouden zijn gestolen.

Het is evenwel nog niet duidelijk of door de gearresteerde medewerkers van het landelijk callcenter of medewerkers van andere GGD’en gegevens zijn gestolen en/of ten onrechte ingezien van inwoners uit het werkgebied. Dit moet duidelijk worden uit het landelijke onderzoek van politie en justitie.

Welke maatregelen zijn vooraf genomen om gegevensmisbruik te voorkomen bij GGD?
De GGD werkt aan de virusbestrijding, met de benodigde functionaliteiten op een zo veilig mogelijke manier. De GGD'en hebben vooraf de volgende maatregelen genomen:

- **Controle aan de poort**. Mensen moeten een Verklaring Omtrent Gedrag (VOG) aanleveren en een geheimhoudingsverklaring ondertekenen. GGD Hart voor Brabant heeft zich er bij de aanname van personeel van verzekerd, dat altijd en voor iedereen een VOG en geheimhoudingsverklaring voor handen is.
- **Autorisatieniveaus**. De beide systemen die het betreft (CoronIT en HPZone) kennen verschillende rollen met bijbehorende autorisatieniveaus. Niet iedereen kan bij alle gegevens en kan alle functionaliteiten (zoals het downloaden van data-exports) gebruiken. Binnen GGD Hart voor Brabant is er een autorisatiematrix gebaseerd op rol of functie van iedere medewerker. Medewerkers krijgen alleen die autorisatie, die nodig is voor zijn of haar functie. De autorisatiematrix wordt bijgehouden bij in-, door- en uitstroom van medewerkers. Er vindt hierop een maandelijkse check plaats.
- **Controles op correct gebruik**. De GGD'en controleren sinds de start het gebruik van de systemen door de medewerkers, hebben die controles steeds verder verbeterd en doen dat nog steeds. Vanwege het belang van de virusbestrijding en de gevraagde snelheid zijn de GGD'en – op diverse manieren – met steekproefsgewijze controles van start gegaan. De Autoriteit Persoonsgegevens had vóór het bekend worden van de datadiefstal geen aanvullende vragen gesteld over deze werkwijze. GGD Hart voor Brabant kan via de logging-functionaliteit van Microsoft 30 dagen terugkijken. De GGD gebruikt dit voor steekproeven en om terug te zoeken bij signalen en incidenten.

Welke maatregelen worden genomen sinds het bekend worden van de datadiefstal bij GGD?
Landelijk is aangifte gedaan en wordt grootschalig onderzoek gedaan door politie en justitie. Binnen de organisatie is er continue aandacht voor kwaliteitsbevordering én -bewaking en worden de medewerkers regelmatig bijgepraat over de laatste stand van zaken rondom het incident. De eerder genomen maatregelen zijn gecontroleerd en geïntensiveerd:

- **Controle aan de poort**. GGD Hart voor Brabant heeft nogmaals een check uitgevoerd. De GGD heeft vastgesteld dat alle door GGD ingezette externe medewerkers een VOG en ondertekende geheimhoudingsverklaring hebben. Bij vaste, interne medewerkers is dit ook het geval voor zover ze bij GGD zijn komen werken sinds het beleid omtrent VOG en geheimhoudingsverklaring is geïmplementeerd. Oudgedienden die al vele jaren bij GGD werken hebben geen VOG, omdat dit destijds nog niet bestond. Alle ambtenaren hebben echter sowieso een wettelijke geheimhoudingsplicht. Bij de invoering van de Wet normalisering rechtspositie ambtenaren hebben al de vaste medewerkers digitaal moeten bevestigen dat zij zich houden aan de integriteitsregels, waaronder geheimhouding. De GGD zoekt uit of het nodig is om oudgedienden alsnog te vragen om een VOG en/of geheimhoudingsverklaring.
- **Autorisatieniveaus**. Naar aanleiding van de datadiefstal is ter check nog een keer doorgelicht wie binnen GGD Hart voor Brabant geautoriseerd is tot grote downloads (datadump). Dit is een zeer beperkte groep van medewerkers die dit op grond van hun functie daadwerkelijk nodig hebben, bijvoorbeeld om dashboards te maken.
- **Controles op correct gebruik**. GGD Hart voor Brabant heeft een nadere check uitgevoerd van onze 'logging-bestanden' en geen onregelmatigheden aangetroffen. De GGD ziet geen afwijkingen in de IT-omgeving. GGD heeft het beeld dat er binnen of door GGD Hart voor Brabant geen gegevens in verkeerde handen zijn gevallen. GGD Hart voor Brabant wil de

periode van logging verlengen van 30 dagen naar 1 jaar, zodat zij verder kunnen terugkijken. Verder verwacht GGD GHOR Nederland in maart systemen te implementeren die automatisch en continu zullen controleren op opvallend gebruik van de systemen (zoals grote downloads of onlogische inzage in dossiers).

Verder worden als aanvullende maatregelen genomen:

- **Communicatie.** GGD Hart voor Brabant vindt het van belang om de eigen inwoners gericht te informeren over de situatie, wat GGD eraan doet en hoe mensen een verwijderingsverzoek kunnen indienen. GGD wijst inwoners in eerste instantie op de landelijke lijst met veel gestelde vragen van GGD GHOR Nederland. Zit het antwoord op hun vraag er niet bij, dan adviseren GGD hen om contact op te nemen met het landelijke nummer voor deze datadiefstal. Dit telefoonnummer (085- 130 82 26) is dagelijks bereikbaar van 09.00 uur tot 21.00 uur. Daarnaast attendeert GGD inwoners uit onze regio op de mogelijkheid om hun eigen gegevens in te zien, te wijzigingen of te laten verwijderen.
- **Verzoeken voor gegevensverwijdering**. Mensen kunnen op grond van de Algemene Verordening Gegevensbescherming (AVG) bij de GGD alwaar zij getest of gevaccineerd zijn een verzoek doen tot het verwijderen van hun persoonsgegevens. De GGD heeft hiervoor al jaren een staand beleid en werkprotocol, conform de AVG. Vanuit GGD GHOR Nederland wordt op dit moment gewerkt aan de precieze invulling van het recht op gegevensverwijdering binnen CoronIT en HPZone. Zo wordt bijvoorbeeld uitgezocht welke gegevens in welke gevallen en met inachtneming van welke termijnen verwijderd mogen c.q. moeten worden. Naast de AVG heeft GGD bijvoorbeeld ook te voldoen aan de Wet Publieke Gezondheid, die o.a. eisen stelt aan de bewaartermijn van medische gegevens. Op de website van GGD Hart voor Brabant (www.ggdhvb.nl) vindt men via het onderdeel Corona bij veel gestelde vragen de link naar privacy en corona. Daar is een formulier te downloaden, waarmee een aanvraag kan worden gedaan. Aanvragen worden binnen 4 weken behandeld. GGD Hart voor Brabant heeft sinds vorige week 60 inzage- en verwijderingsverzoeken ontvangen.
- **Uitzetten van functionaliteiten in de systemen**. Om het risico per direct te verminderen zijn landelijk in CoronIT en HPZone diverse functionaliteiten uitgezet. Het is niet meer mogelijk om downloads van gegevensbestanden te doen, prints van gegevensbestanden te maken (omdat dit als PDF kon) en om zoekopdrachten te doen (query's) op BSN en postcode. Het risico op verder misbruik is hiermee zoveel mogelijk gereduceerd.

Vervolg

Als er nieuwe relevante ontwikkelingen zijn op dit dossier, dan stel ik u daar zo snel mogelijk van op de hoogte. Voor nu vertrouw ik erop u met dit schrijven voldoende geïnformeerd te hebben.

Communicatie

Vanuit GGD GHOR Nederland en de GGD'en wordt alle medewerking verleend aan instanties die op grond van hun wettelijke taken toezicht houden, vragen stellen en controles uitvoeren. GGD ziet het maatschappelijke belang daarvan en het gezamenlijke doel is het herstel van vertrouwen. Bovengenoemde informatie is gericht aan het AB van GGD GHOR en wordt via de portefeuillehouder gedeeld met desbetreffende college- en gemeenteraden.