Conclusies en aanbevelingen van de Domeingroep Privacy & Beveiliging bij de Totaalrapportage Informatiebeveiliging GeVS 2022

Achtergrond

Dit jaar is voor het zesde jaar op rij een Totaalrapportage informatiebeveiliging GeVS opgesteld. Dit keer kunnen de 14 BIO-normen over drie verantwoordingsjaren (2020, 2021 en 2022) met elkaar vergeleken worden.

BKWI voegt de afzonderlijke transparantierapportages samen tot één uniforme Totaalrapportage, zoals beschreven in de Verantwoordingsrichtlijn. De Domeingroep Privacy & Beveiliging stuurt de Totaalrapportage met conclusies en aanbevelingen naar het Ketenoverleg, dat de rapportage vervolgens met een bestuurlijke reactie van VNG, SVB en UWV aanbiedt aan de minister van SZW.

Op grond van deze Totaalrapportage en de conclusies en aanbevelingen van de domeingroep kan het Ketenoverleg algemene, niet op individuele partijen gerichte, maatregelen nemen om de informatiebeveiliging op een hoger niveau te krijgen. De minister van Sociale zaken en werkgelegenheid kan bij gemeenten via de toepassing van het 'Interventieprotocol Suwinet' maatregelen nemen gericht op individuele partijen. Bij andere afnemers kan de verantwoordelijke minister binnen de planning- en control-cyclus maatregelen nemen.

De conclusies en aanbevelingen die nu volgen hebben betrekking op alle afnemers.

Conclusies

Afnemers met bevindingen in 2022 en voorgaande jaren

Er zijn meerdere niet-gemeentelijke-afnemers (3 van de 6) die voor meer jaren op rij bevindingen hebben. Er zijn 36 gemeenten die voor meer jaren op rij bevindingen hebben. Met deze cijfers moeten we concluderen dat het blijkbaar lastig is voor partijen om te verbeteren op beveiligingsnormen, zelfs als dat alleen geldt voor opzet en bestaan. De DPB moet hierbij concluderen dat het een zorgelijke trend is dat dit in sommige gevallen al meerdere jaren op rij het geval is. De DPB concludeert dat over de linie genomen de informatiebeveiliging en privacybescherming op de GeVS op dit moment in stijgende lijn niet compliant is aan de getoetste normen.

Aantal gemeentelijke afnemers met 0 bevindingen is licht gestegen

Het totale aantal gemeentelijke afnemers met 0 bevindingen is het afgelopen jaar licht gestegen (71,6% in 2021 en 78,6% in 2022). Hoewel uit de rapportage blijkt dat het aantal gemeentelijke afnemers met 0 bevindingen is gestegen, zegt dit niet alles over het daadwerkelijke niveau van beveiliging. Gemeenten toetsen alleen op opzet en bestaan. Er is geen beeld op werking. Daarmee

kan niet de conclusie worden getrokken dat deze gemeenten veilig zijn. Het risico hiervan is dat zonder een volledig beeld er een misleidend beeld kan ontstaan over de informatieveiligheid. VNG stipt hierbij aan dat gemeenten naast een verticale verantwoording richting het Ministerie van SZW ook een horizontale verantwoording levert richting de gemeenteraad.

Geen niet-gemeentelijke afnemers zonder bevindingen

Alle niet-gemeentelijke afnemers hebben in 2022 bevindingen. Dit is een verslechtering ten opzichte van de twee voorgaande jaren. In 2021 waren er twee partijen zonder bevindingen, net als in 2020. Hierbij moet wel worden aangetekend dat in 2020 geen verantwoording is afgelegd door twee partijen en dat daarnaast van een van de niet-gemeentelijke afnemers is gebleken dat de verantwoording onbetrouwbaar is over 2020 en 2021.

Aantal bevindingen voor afnemers is gestegen

Het totale aantal bevindingen bij gemeentelijke afnemers is licht gestegen. In 2021 was sprake van 481 bevindingen. In 2022 is sprake van 490 bevindingen. Bij niet-gemeenten is de stijging fors gestegen. In 2021 lag het totale aantal bevindingen op 25, in 2022 steeg dit naar 43. Er wordt hier geen verklaring voor gegeven in de totaalrapportage. Vanuit DPB moeten we vaststellen dat onduidelijk is wat de stijging heeft veroorzaakt. Hier concludeert de DPB dat het stijgen van bevindingen geen positieve afdronk geeft dat de algehele veiligheid van de GeVS is geborgd.

Bevindingen die relatief vaak voorkomen

Een analyse van bevindingen die in de Totaalrapportage genoemd worden laat zien dat er bij gemeenten drie normen genoemd kunnen worden die relatief vaak voorkomen: 9.2.5, 12.4.1 en 18.1.4. Deze normen betreffen respectievelijk het beoordelen van toegangsrechten van gebruikers, het registreren van gebeurtenissen en privacy en bescherming van persoonsgegevens. Bij de analyse van niet-gemeenten vallen meerdere normen rond toegangsverlening (9.2.2, 9.2.5 en 9.2.6), maar ook 12.4.1 en 18.1.4 in negatieve zin op. Voor zowel gemeenten als niet-gemeenten is deze set zorgelijk. Er bestaat een hogere kans op een risico van een datalek door ongeautoriseerde toegang met misbruik van de gegevens tot gevolg. Indien dit zich voordoet kan in meerdere gevallen mogelijk geen deugdelijk onderzoek plaatsvinden door de vele bevindingen op het registreren van gebeurtenissen. Om die reden moet de DPB concluderen dat het noodzakelijk is dat er voor deze normen in 2024 (2023 is nog lastig haalbaar) een verbetering komt.

Verantwoording over taken van afnemers in de transparantierapportage laat discrepanties zien

Het valt op dat het aantal gemeenten dat zich verantwoord over niet Suwi-taken niet overeenkomt met het aantal gemeenten dat zich daarover dient te verantwoorden op basis van de administratie van BKWI. Bij sommige niet Suwi-taken verantwoorden zich meer gemeenten dan op basis van de administratie mag worden verwacht, bij andere juist minder. Dit jaar heeft BKWI tijdens de verwerking van de transparantierapportages direct de vergelijking gemaakt met de gebruikersadministratie. We zullen hier actie op ondernemen zodat gemeenten zich op de juiste taken verantwoorden. De eerste stappen zijn hierin gezet vanuit BKWI.

Gebruik GeVS zonder wettelijke grondslag

In 2018 rapporteerden 13 gemeenten dat zij gebruik hadden gemaakt van GeVS bij de uitvoering van taken waar geen wettelijke grondslag voor bestaat (bijvoorbeeld WMO of Jeugdzorg). De betreffende gemeenten zijn daarop gewezen. In 2019 was er nog maar één melding van onrechtmatig gebruik, in

2020 meldden 6 gemeenten dit. In 2021 is dit aantal gedaald naar 2. Vervolgens is dit in 2022 naar 0 gedaald.

Aanbevelingen

De onder Conclusies genoemde punten van zorg in acht nemend en de komst van de BIO 2.0 en zeker NIS2, die meer aantoonbare bewijslast over de werking van maatregelen vraagt, in ogenschouw nemend, beveelt de DPB het volgende aan:

- heroverweeg de huidige verbetercyclus na geconstateerde bevindingen. Concreet betekent dit een aanscherping van verbeteracties in de P&C-cyclus van de SUWI-partijen UWV en SVB, het interventieprotocol voor de gemeentes en het ontwikkelen van een interventieprotocol voor de niet-Suwipartijen;
- heroverweeg het besluit om binnen ENSIA de toetsing alleen op opzet en bestaan te doen. Een geleidelijke invoering van de toets op werking behoort hier ook tot de mogelijkheden. Bijvoorbeeld startend met normen waarop in opzet en bestaan géén bevindingen zijn. VNG staat niet achter deze aanbeveling aangezien gemeenten naast de gezamenlijke verantwoordelijk ook een eigen verantwoordelijkheid richting de raad hebben. Daarnaast wordt in ENSIA verband de mogelijkheid van de toets op werking al onderzocht.
- vraag gericht actie op de normen waar de meeste bevindingen zijn. De DPB neemt hiervoor het initiatief door afnemers te vragen waar zij tegenaan lopen bij de implementatie van de normen. Op basis van deze inventarisatie kan onder andere de guidance bij de normen onder de loep worden genomen en best practices gedeeld worden.