Conclusies en aanbevelingen van de Domeingroep Privacy & Beveiliging bij de Totaalrapportage Informatiebeveiliging GeVS 2021

Achtergrond

Dit jaar is voor het vijfde jaar op rij een Totaalrapportage informatiebeveiliging GeVS opgesteld. Voor de eerste keer kunnen de 14 BIO-normen over twee verantwoordingsjaren (2020 en 2021) 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.

Algemene opmerkingen bij de Totaalrapportage over 2021

1) Het verantwoordingssysteem dat nu is ingericht biedt waarborgen voor het tijdig in kaart brengen en herstellen van bevindingen en het terugbrengen van de risico's die daarmee samenhangen. Hoewel nog niet alle normen door alle afnemers zijn geïmplementeerd, is er wel een verantwoordingssysteem ontstaan dat zicht geeft op verbeterpunten en waarborgen om de normnaleving te verbeteren.
   De domeingroep merkt hierbij wel op dat de Totaalrapportage een feitelijke/getalsmatige weergave is van de verantwoording zoals die door de afnemers wordt aangeleverd. De verantwoording van afnemers is ook kwantitatief van aard. Het is op basis van die verantwoordingen en de cumulatie daarvan in de Totaalrapportage lastig om conclusies te trekken en aanbevelingen te doen die meer kwalitatief van aard zijn. De domeingroep is van mening dat een meer kwalitatieve, inhoudelijke rapportage meer kan bijdragen aan het nog veiliger gebruiken van de voorzieningen dan nu. In een inhoudelijke rapportage gaat het om het verhaal achter de verantwoording van afnemers en kan bijvoorbeeld worden ingegaan op de manier van beoordelen en de interpretatie van de BIO-normen. Dit betekent wel dat andere eisen aan de verantwoording van afnemers worden gesteld en de impact daarvan is groot.

2) De domeingroep signaleert ook dat de verdeling van de verantwoordelijkheden verduidelijking nodig heeft. Op dit moment benaderen afnemers het BKWI met de vraag om uitspraken te doen over de wijze waarop verantwoording moet worden afgelegd en hoe daarbij normen moeten worden geïnterpreteerd. Over de wijze waarop verantwoording moet worden afgelegd, bijvoorbeeld over de stukken die moeten worden aangeleverd, geeft het BKWI, vaak in overleg met de VNG en SZW, antwoord. Over de wijze waarop audits moeten worden uitgevoerd doet het BKWI geen uitspraken. Het BKWI zou hier in de toekomst een faciliterende rol kunnen spelen. De vraag is vanuit welke hoedanigheid het BKWI dat dan zou doen en met welke autoriteit. Hoort de interpretatie van normen bij de taken die BKWI nu uitvoert en zo ja, is het logisch dat BKWI deze faciliterende rol op zich neemt? Welke voor- en nadelen kleven aan een dergelijke faciliterende rol en wat is er nodig om deze rol in te kunnen vullen? De domeingroep stelt voor hierover het gesprek te voeren en afspraken te maken. De domeingroep adviseert om met alle betrokken partijen (ministerie SZW, VNG, NOREA en BKWI) hierover het gesprek aan te gaan.

3) Op basis van de conclusies en aanbevelingen die zijn gedaan bij de Totaalrapportage over verantwoordingsjaar 2020 is de domeingroep in gesprek gegaan met het ministerie. Uit dit gesprek bleek dat sommige aanbevelingen van de domeingroep niet snel te realiseren zijn. Het gaat dan om de aanbevelingen 'werking' onderdeel te maken van de verantwoording door gemeenten en een wijziging/uitbreiding van het aantal normen. De domeingroep heeft er daarom voor gekozen deze aanbevelingen niet opnieuw op te nemen. Tegelijkertijd merkt de domeingroep op dat de aanbevelingen relevant blijven. Met de uitbreiding op 'werking' krijgt de Totaalrapportage meer waarde en door de set normen te evalueren wordt ook bepaald of het doel van de verantwoording wordt bereikt. De domeingroep constateert ook dat het ministerie invulling geeft aan het interventieprotocol. Inmiddels krijgen een aantal gemeenten een vooraankondiging tot aanwijzing. Daarmee wordt aan de aanbevelingen die vorig jaar is gedaan invulling gegeven. Om die reden heeft de domeingroep deze aanbeveling ook niet meer opgenomen.

4) In algemene zin merkt de domeingroep op dat bevindingen over het bestaan (normafwijkingen) bij de verantwoording niet noodzakelijk betekent dat de informatiebeveiliging niet adequaat is. De registratie en afmelding van gebruikers kan bijvoorbeeld maandelijks plaatsvinden, maar als die niet beschreven is in een formeel vastgestelde procedure, is er toch sprake van een afwijking van een norm.

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

Conclusies

Afnemers met bevindingen in 2021 en voorgaande jaren

Er zijn drie niet- gemeentelijke-afnemers die voor het tweede jaar op rij bevindingen hebben. Hierbij wordt aangetekend dat niet-SUWI-afnemers niet onder de reikwijdte van het Interventieprotocol SUWI vallen. Er zijn 22 gemeenten die voor het tweede jaar op rij bevindingen hebben. Er zijn 7 gemeenten die voor het derde jaar op rij bevindingen hebben. Het ministerie handelt bij de gemeenten volgens het interventieprotocol.

Aantal afnemers met 0 bevindingen is licht gestegen

Het totale aantal afnemers met 0 bevindingen is het afgelopen jaar licht gestegen. Die stijging is toe te schrijven aan gemeenten (69,2% in 2020 en 71,6% in 2021). Het feit dat voor het tweede jaar op rij verantwoording wordt afgelegd over de 14 BIO-normen kan een verklaring zijn voor deze stijging.

Aantal bevindingen is gestegen

Het totale aantal bevindingen bij afnemers is gestegen. In 2020 was sprake van 389 bevindingen. In 2021 is sprake van 481 bevindingen.

Bevindingen die relatief vaak voorkomen

Bevindingen op norm 9.2.5 (beoordeling van toegangsrechten) en norm 7.2.2 (Bewustzijn, opleiding en training t.a.v. informatiebeveiliging) komen relatief vaak voor bij afnemers.

Verantwoording niet Suwi-taken bij gemeenten vs. aantal aansluitingen niet Suwi-taken

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.

Gebruik Suwinet zonder wettelijke grondslag

In 2018 rapporteerden 13 gemeenten dat zij gebruik hadden gemaakt van Suwinet 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.

Aanbevelingen

Op basis van de bovenstaande conclusies doet de domeingroep de volgende aanbevelingen aan het Ketenoverleg:

1. De domeingroep adviseert het ministerie om de beveiliging van de GeVS bij de niet-SUWI afnemers in het toezicht van het ministerie te betrekken. Deze afnemers verantwoorden zich nu voor het tweede jaar op rij en er is sprake van herhaling van bevindingen bij twee van deze afnemers.

Actie: De domeingroep gaat hierover in gesprek met het ministerie.

2. De domeingroep adviseert het BKWI te onderzoeken welke verklaringen er zijn voor het verschil tussen het aantal ontvangen verantwoordingen van gemeenten en het aantal gemeenten dat zich zou moeten verantwoorden bij het gebruik van Suwinet voor Belastingdeurwaarders, RMC en Burgerzaken.

Actie: Het BKWI onderzoekt mogelijke verklaringen voor het verschil in het aantal aansluitingen en verantwoordingen en met het ministerie en de VNG wordt op basis daarvan gezocht naar manieren om het proces, de communicatie en informatie hierover te verbeteren.

3. De domeingroep adviseert om verder te investeren in de verbinding met NOREA, VNG, ministerie en BKWI als het gaat om de vraag wat er nodig is om verbetering te realiseren op de normen die nu relatief veel voorkomen bij afnemers. De domeingroep merkt op dat de VNG al uitgebreide ondersteuning biedt aan gemeenten. Voor andere afnemers dient dit nog verder vorm te krijgen.

Actie: het BKWI zal het initiatief nemen om het gesprek hierover aan te gaan. Daarbij dient wel te worden opgemerkt dat de verdeling van verantwoordelijkheden verduidelijkt moet zijn (Zie punt 2 bij de algemene opmerkingen).