Conclusies en aanbevelingen van de Domeingroep Privacy & Beveiliging bij de Totaalrapportage Informatiebeveiliging GeVS 2020

Achtergrond

Dit jaar is voor het vierde jaar op rij een Totaalrapportage informatiebeveiliging GeVS opgesteld. Voor het eerst sinds het bestaan van de Totaalrapportage rapporteren alle afnemers over dezelfde normen en aan de hand van dezelfde verantwoordingsrichtlijn. Het is dit jaar dus voor het eerst mogelijk om andere afnemers dan gemeenten op dezelfde manier op te nemen in de Totaalrapportage als gemeenten en dus een beeld op te bouwen over het totaal van informatiebeveiliging GeVS.

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 SZW kan bij gemeenten zo nodig 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.

Conclusies

De conclusies in deze paragraaf zijn waar nodig voorzien van een duiding of enkele overwegingen. In algemene zin merkt de domeingroep op dat het bestaan van bevindingen (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.

Verder biedt het verantwoordingssysteem dat nu is ingericht organisaties een groot aantal waarborgen voor het tijdig in kaart brengen en herstellen van bevindingen en het terugbrengen van de risico's die daarmee samenhangen. Daarnaast biedt de Totaalrapportage de domeingroep de gelegenheid om algemene maatregelen voor te stellen.

Hoewel nog niet alle normen door alle afnemers worden nageleefd, is er wel een verantwoordingssysteem ontstaan dat zicht geeft op verbeterpunten en waarborgen bevat om de normnaleving te verbeteren.

De conclusies en aanbevelingen die nu volgen hebben betrekking op gemeenten en de andere afnemers.

Aantal gemeenten met 0 bevindingen is gedaald

Het valt op dat het aantal gemeenten dat geen bevindingen rapporteert het afgelopen jaar is gedaald van 82% naar 69,2%. In 2019 was nog sprake van lichte stijging. Het feit dat in 2020 14 normen in plaats van 12 normen zijn gecontroleerd kan hiervoor mogelijk een verklaring zijn. Ook het feit dat er voor het eerst op normen uit de BIO wordt gecontroleerd kan de daling verklaren. Een andere mogelijke verklaring kan zijn dat de gemeenten in de audit uitgebreider hebben gekeken naar de producten die zij afnemen en de taken waarbij zij die producten gebruiken. In 2020 heeft het BKWI immers een brief gestuurd naar alle gemeenten waarin is gemeld voor welke taken zij Suwinet - services gebruiken en welke services zij gebruiken. Uit een analyse blijkt bijvoorbeeld dat er in 2020 relatief veel gemeenten zijn met bevindingen op DKD-Inlezen.

Vergelijkbare bevindingen

Er lijkt sprake van bepaalde patronen als de bevindingen bij gemeenten en andere afnemers met elkaar worden vergeleken. Bevindingen op norm 12.4.1 (gebeurtenissen registreren) en norm 18.1.4 (privacy en bescherming van persoonsgegevens) komen zowel bij gemeenten als andere afnemers relatief vaak voor.

Aantal gemeenten met meer dan 4 bevindingen vrijwel gelijk

Het aantal gemeenten met 4 of meer bevindingen blijft de afgelopen drie jaar redelijk stabiel (2020 9,1%, 2019 8,2% en 2018 8,4%). Hierbij dient wel te worden opgemerkt dat er in 2020 sprake is van 14 normen. In de jaren daarvoor verantwoorden gemeenten zich over 12 normen.

Gebruik Suwinet zonder wettelijke grondslag

In 2018 rapporteerden 13 gemeenten dat zij gebruik hadden gemaakt van Suwinet bij de uitvoering van taken voor schuldhulpverlening of jeugdzorg. Voor dit gebruik bestaat geen wettelijke grondslag dus dat is onrechtmatig en de betreffende gemeenten zijn daarop gewezen. In 2019 was er nog maar één melding van onrechtmatig gebruik, in 2020 meldden 6 gemeenten dit. Het is niet duidelijk waarom dit aantal meldingen toe is genomen.

Aanbevelingen

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

Aanbevelingen m.b.t. gemeenten

1. Het is van belang dat het ministerie het interventieprotocol blijft toepassen. Er zijn dit jaar gemeenten die voor het derde opeenvolgende jaar bevindingen rapporteren.
2. In 2020 adviseerde de domeingroep om een groeipad te bepalen waarbij de eerste stap de uitbreiding met ‘werking’ bij gemeenten zou zijn. Over de uitbreiding is een gesprek gevoerd tussen de VNG, een afvaardiging van de domeingroep en het ministerie. Het groeipad is echter nog niet bepaald. De domeingroep constateert dat de Totaalrapportage zoals die nu er nu ligt toegevoegde waarde heeft. Deze toegevoegde waarde zou echter

groter kunnen zijn als 'werking' bij gemeenten onderdeel is van de verantwoording. Alleen dan wordt het gestelde doel van de rapportage, een compleet beeld van de informatiebeveiliging bij gemeenten, bereikt en kan het als middel dienen om een acceptabel niveau van informatiebeveiliging te bereiken bij gemeenten.

Actie: De domeingroep gaat opnieuw in gesprek met het ministerie. Bij het bepalen van het groeipad kan de impact worden bepaald. Afnemers kunnen ondersteunt worden bij het doorlopen van het groeipad, bijv. door het ENSIA-ondersteuningsteam van de VNG.

3. De domeingroep adviseert om aandacht te besteden aan het relatief hoge aantal bevindingen bij DKD-Inlezen bij gemeenten. Door in gesprek te gaan met een vertegenwoordiging van auditors kunnen Inlichtingenbureau, BKWI, VNG en de domeingroep onderzoeken of er een verklaring is voor deze bevindingen en gemeenten wellicht ondersteunen bij het terugdringen van de bevindingen.

   Actie: de domeingroep, Inlichtingenbureau, BKWI en het ENSIA-ondersteuningsteam van de VNG gaan in gesprek met auditors.

4. De domeingroep adviseert om de domeingroep en het ENSIA-ondersteuningsteam van de VNG in gesprek te laten gaan met auditors over de bevindingen bij normen
   - 9.2.5: beheer van toegangsrechten van gebruikers. Deze norm hangt nauw samen met norm 12.4.1
   - 12.4.1: gebeurtenissen registeren d.m.v. logbestanden
   - 7.22: bewustwording van informatiebeveiliging d.m.v. training en opleiding
   - 18.4.1: privacy en bescherming van persoonsgegevens in overeenstemming met relevante wet- en regelgeving.

   Wellicht kunnen gemeenten ondersteunt worden in het oplossen van deze bevindingen.

   Actie: de domeingroep en het ENSIA-ondersteuningsteam van de VNG gaan in gesprek met auditors.

Aanbevelingen m.b.t andere afnemers:

1. De domeingroep adviseert het ministerie om in de gesprekken die plaatsvinden in het kader van planning & control aandacht te besteden aan de volgende normen:
   - 12.4.1: gebeurtenissen registeren d.m.v. logbestanden
   - 18.1.4: bewustwording van informatiebeveiliging d.m.v. training en opleiding

   Deze normen komen relatief vaak voor.

Aanbevelingen m.b.t gemeenten en andere afnemers:

1. Ga in gesprek met het ministerie over de uitbreiding van het aantal normen. Ook dit is onderdeel van het groeipad en hierover zijn al gesprekken gevoerd met het ministerie. Het groeipad is echter nog niet bepaald. Door deze uitbreiding wordt het doel van de rapportage, een compleet beeld van de informatiebeveiliging bij gemeenten, bereikt en kan het als middel dienen om een acceptabel niveau van informatiebeveiliging te bereiken bij alle afnemers.