Conclusies en aanbevelingen bij de Totaalrapportage Informatiebeveiliging GeVS 2017 van de Domeingroep Privacy & Beveiliging

Achtergrond

In 2016 zijn de normenkaders voor de informatiebeveiliging van de GeVS herzien en in 2017 is de ENSIA-verantwoordingssystematiek voor informatiebeveiliging bij gemeenten ingevoerd. In de normenkaders is geregeld dat alle partijen ieder jaar een zogenoemde transparantierapportage over de informatiebeveiliging ter beschikking stellen aan BKWI. Gemeenten vullen dit in met de ENSIA-systematiek.

De transparantierapportages van gemeenten hadden voor 2017 betrekking op opzet en bestaan van interne beheersingsmaatregelen voor 11 uit het normenkader geselecteerde normen per 31 december 2017. Deze selectie is gemaakt door het ministerie van SZW als systeemverantwoordelijke voor de GeVS en afgestemd met het Ketenoverleg.

Voor de andere op de GeVS aangesloten partijen bestond voor 2017 nog geen verplichting tot het leveren van een transparantierapportage, omdat de herziene normenkaders voor hen nog niet van kracht waren. De Totaalrapportage voor 2017 heeft dus alleen betrekking op gemeenten.

BKWI voegt de afzonderlijke transparantierapportages samen tot een Totaalrapportage, zoals beschreven in het genoemde normenkader. 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..

Deze Totaalrapportage geeft een geaggregeerd beeld van de stand van de informatiebeveiliging van de GeVS. Op grond hiervan kan het Ketenoverleg, mocht daar aanleiding toe zijn, algemene, niet op individuele partijen gerichte maatregelen nemen om de informatiebeveiliging op het overeengekomen niveau te krijgen. De minister van SZW kan zonodig via de toepassing van het Interventieprotocol Suwinet maatregelen nemen gericht op individuele partijen.

Bevindingen

Met deze Totaalrapportage is voor het eerst in het bestaan van de GeVS een compleet beeld van de informatiebeveiliging bij gemeenten beschikbaar gekomen. Meer dan 99% van de gemeenten heeft al in het eerste jaar dat de ENSIA-verantwoordingssystematiek van kracht was een Transparantierapportage ingeleverd. Er is dus veel bereikt!

Wel blijkt uit de ervaringen van het eerste jaar dat er nog een aantal verbeteringen nodig is. Allereerst is de verantwoording over de informatiebeveiliging van niet-SUWI-taken[1] nog niet

[1] Het gaat om het gebruik van de GeVS door afdelingen Burgerzaken, gemeentelijke belastingdeurwaarders en RMCs, regionale meld- en coördinatiecentra vroegtijdig schoolverlaten, voor taken die niet in de SUWI-wetgeving zijn geregeld.

representatief. Hierbij kan een rol spelen dat dit onderwerp pas laat aan de verantwoordingssystematiek is toegevoegd. Ook is het gebruik van de GeVS voor niet-SUWI-taken veel minder frequent[2] dan dat van de SUWI-taken en doorgaans elders in de organisatie is belegd.

Een andere observatie is dat de normnaleving voor SUWI-taken nog niet maximaal is: voor 2017 meldt 54% van de gemeenten één of meer afwijkingen van de 11 geselecteerde normen[3] [4].

Duiding

Betrouwbaarheid

De Totaalrapportage geeft een representatief beeld van de stand van de informatiebeveiliging op basis van de geselecteerde normen bij gemeenten als het gaat om SUWI-taken. Het beeld van de niet-SUWI-taken is veel minder volledig en daarmee minder betrouwbaar. Daarbij moet worden opgemerkt dat de GeVS veel minder intensief gebruikt wordt voor niet-SUWI-taken (3,5% van de opvragingen door gemeenten).

Werking van het verantwoordingsysteem

Hoewel niet alle normen worden nageleefd, is er wel een verantwoordingssysteem ontstaan dat zicht geeft op verbeterpunten en waarborgen bevat om de normnaleving te verbeteren. Daartoe behoren de jaarlijkse zelfevaluatie, de Collegeverklaring en de getrouwheidsverklaring van een onafhankelijke IT-auditor, waarmee verantwoording wordt afgelegd aan de gemeenteraad en aan de minister van SZW. Daarnaast is er een interventieprotocol dat voorziet in het nemen van maatregelen door de minister van SZW indien van normen wordt afgeweken en verbetering te lang op zich laat wachten.

Oorzaken van niet-naleving

Waar de Totaalrapportage nog onvoldoende zicht op geeft, zijn de oorzaken van niet-naleving van normen.

Het is evident dat bepaalde afwijkingen met elkaar samenhangen. Om logging te kunnen controleren (norm C.06), moet die bijvoorbeeld wel beschikbaar zijn (C.05). Een afwijking op C.05 leidt dus automatisch tot een afwijking op C.06.

Er zijn ook correlaties denkbaar tussen de grootteklasse van een gemeente en bepaalde afwijkingen. Onderzoek kan dit soort verbanden zichtbaar maken en zo bijdragen aan effectieve interventies.

Risico's

Gebreken bij de verantwoording betekenen nog niet automatisch dat de informatiebeveiliging zelf in het geding is. De controle op autorisaties 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.

---

[2] De niet-SUWI-taken zijn goed voor ongeveer 3,5% van de gemeentelijke raadplegingen via de GeVS.

[3] Het in het rapport *SUWInet 2016 Stand van zaken na ontvangst in-control verklaringen gemeenten* van de Inspectie SZW beschreven onderzoek meldde geen afwijkingen, maar verschilde in belangrijke opzichten van het onderzoek waarop deze Totaalrapportage is gebaseerd. Zo zijn de onderzochte normen tussen beide rapportages ingrijpend herzien en is het aantal onderzochte normen uitgebreid (er waren er 7 en er zijn er 4 toegevoegd, onder andere op het gebied van controle van logging). Ook is de scope van het onderzoek uitgebreid naar niet-SUWI-taken en het gebruik van Suwinet- en DKD-Inlezen. Verder ging het bij het onderzoek van de inspectie om desk research bij een aselecte steekproef van gemeenten. Bij de voorbereiding van de Totaalrapportage is bij iedere gemeente onderzoek gedaan door een IT-auditors.

Zeker bij de introductie van een nieuwe verantwoordingssystematiek zullen dat soort situaties zich eerder voordoen en ligt het in de lijn van de verwachting dat die snel hersteld worden.

Verder biedt het verantwoordingssysteem dat nu is ingericht, zoals eerder aangegeven, een groot aantal waarborgen voor het tijdig in kaart brengen en herstellen van normafwijkingen en terugbrengen van de risico's die daarmee samenhangen.

Aanbevelingen

1. De betrouwbaarheid van de verantwoording over niet-SUWI-taken kan en moet beter. Zie erop toe dat de in de bijlage beschreven maatregelen worden genomen.
2. Geef de betrokken partijen eerst de gelegenheid om de rol te gaan spelen die ze in het systeem hebben, zoals de toezichthoudende rol van de Gemeenteraad, alvorens hierin aanpassingen aan te brengen.
3. Start onderzoek dat afwijkingen en samenhang van normen verklaart en zicht biedt op passende, effectieve interventies, waar die nodig zijn.

Conclusie

Met de ENSIA-systematiek en de Totaalrapportage is er voor het eerst een compleet overzicht in de stand van de informatiebeveiliging van de GeVS bij gemeenten. Daarmee is voor het eerst integrale stuurinformatie beschikbaar, in ieder geval voor de normnaleving bij SUWI-taken. Hiermee beschikt de SUWI-keten, hoewel er nog een aantal verbeteringen in mogelijk en nodig zijn, nu al over een belangrijk instrument om het gemeenschappelijke informatiebeveiligingsniveau te bewaken en risico's op dit vlak te beheersen

Bijlage: Verbetermaatregelen

Op basis van de ervaringen met de toepassing van ENSIA en de door gemeenten opgestelde en aan BKWI geleverde verantwoordingsinformatie zijn en worden de volgende maatregelen genomen.

Maatregelen in ENSIA-verband:

1. Verbeteren van de via de ENSIA-tooling ondersteunde zelfevaluatie betreffende de vragenlijst en de guidance daarbij (VNG in afstemming met SZW en BKWI: afgerond) (gemeenten zijn per 1 juli 2018 gestart met de zelfevaluatie over 2018).

2. Verbeteren van de algemene formats voor de Collegeverklaring en het Assurancerapport en de specifieke bijlage 2 Suwinet bij de Collegeverklaring (SZW, BKWI, VNG en beroepsvereniging NOREA: afgerond).

3. Verbeteren van de Handreiking ENSIA voor Gemeenten en het daarbij ontwikkelen van een spreadsheet voor het bij elkaar brengen van de verantwoordingsinformatie voor: SUWI-taken en evt. niet-SUWI-taken, inkijken en/of inlezen, eigen organisatie en/of organisatie(s) waaraan taken zijn uitbesteed (VNG in afstemming met NOREA, SZW en BKWI: afgerond).

4. Verdere communicatie/educatie voor gemeenten (VNG: communicatie via nieuwsbrieven, website, bijeenkomsten is doorlopende activiteit).

5. Verbeteren van de handreiking voor de IT-auditors waarbij is afgesproken dat de IT-auditors voortaan gaan beoordelen of de Collegeverklaring voldoet aan het afgesproken format en ook zelf het format van de Assuranceverklaring gaan naleven (NOREA in afstemming met VNG, SZW, BKWI: afgerond).

6. Verdere communicatie/educatie voor de groep ENSIA-auditors (NOREA: bijeenkomst in oktober en communicatie via website, nieuwsbrieven is een doorlopende activiteit).

Maatregelen SZW en BKWI op basis van via ENSIA al dan niet ontvangen verantwoordingsinformatie:

1. Benaderen van de 3 gemeenten over de nog ontbrekende ENSIA-verantwoording (BKWI en SZW).

2. BKWI stuurt brieven aan individuele gemeenten over onduidelijke en ontbrekende onderdelen van verantwoordingsinformatie met het verzoek om contact op te nemen met BKWI om dit door te spreken (BKWI in afstemming met SZW en UWV).

3. SZW informeert gemeenten via de algemene nieuwsbrief Gemeentenieuws over de opbrengst van het eerste jaar ENSIA (na ontvangst van de Totaalrapportage).