Informatiebeveiliging in Súdwest-Fryslân

Colofon

Rekenkamer Súdwest-Fryslân

drs. J.H. (Jet) Lepage MPA (voorzitter)

dr. M.S. (Marsha) de Vries (secretaris)

dr. R.J. (Rick) Anderson (lid)

Contactgegevens

Postadres: Postbus 10.000, 8600 HA Sneek

E-mail: rekenkamer@sudwestfryslan.nl

Website: www.gemeentesudwestfryslan.nl

Informatiebeveiliging in Súdwest-Fryslân

Plan van aanpak

April, 2018

Inhoud

1. Onderzoeksopzet

1.1 Achtergrond

In september 2017 heeft de visitatiecommissie Informatieveiligheid van de VNG een rapportage[1] gepubliceerd waarin zij concludeert dat gemeenten meer aandacht voor het thema informatieveiligheid hebben dan in het verleden, maar dat het tempo waarmee de aandacht toeneemt vaak nog te langzaam is. De commissie merkt op (2017, p.5): *"Gemeenten beschikken over een schat aan informatie van burgers en bedrijven en kunnen hierdoor een gericht doel van criminaliteit of spionage zijn. Dit besef moet bij diverse gemeenten nog dieper doordringen. […] Informatiebeveiliging draagt bij aan de kwaliteit en continuïteit van de gemeentelijke dienstverlening, maar het conflicteert soms met gebruikersvriendelijkheid of de functionaliteit. Informatieveiligheid vergt bovendien expliciete aandacht naast privacy en integriteit. Het leggen van de verbinding tussen deze onderwerpen en perspectieven helpt om de dilemma's onder ogen te zien en bewuste keuzes te maken"*. Daarnaast geeft de commissie aan dat de verantwoordelijkheid van gemeenten voor informatieveiligheid over de hele linie geldt, van inhuurkracht tot raadslid, voor leveranciers, met ketenpartners en samenwerkingsverbanden (2017, p.5): *"Het vergt een enorme inspanning om deze verantwoordelijkheid waar te maken. De aandacht voor informatieveiligheid moet structureel zijn en het kan goed zijn om incidenten te benutten"*.

In november 2013 is tijdens de Buitengewone Algemene Ledenvergadering van de Vereniging van Nederlandse Gemeenten (VNG) de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' bekrachtigd. Deze Resolutie houdt in dat iedere gemeente het informatiebeveiligingsbeleid vaststelt aan de hand van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Tevens zullen gemeenten informatieveiligheid zowel bestuurlijk als ambtelijk borgen en maken ze de invulling op informatieveiligheid transparant voor burgers, bedrijven en ketenpartners. Met de BIG kunnen gemeenten op een vergelijkbare manier efficiënt werken met informatiebeveiliging en hebben gemeenten een hulpmiddel om aan alle eisen ten aanzien van informatiebeveiliging te kunnen voldoen. Ook zorgen gemeenten er met de BIG voor dat informatiebeveiliging een integraal onderdeel is van de bedrijfsvoering en van de keuzes die het management maakt.[2] De horizontale verantwoording richting de gemeenteraad die met de komst van de BIG tot stand is gekomen bestaat uit een zelfevaluatie, een IT-audit, een verklaring van het College van B&W en een passage over informatieveiligheid in het jaarverslag. Daarnaast is er ook sprake van verticale verantwoording over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet). De horizontale verantwoording richting gemeenteraad vormt hiervoor de basis. De normen van de BIG en de specifieke normen van de BRP, PUN, Suwinet, BAG, BGT en DigiD zijn opgenomen in de zelfevaluatievragenlijst.[3] Deze integrale verantwoordingssystematiek wordt wel aangeduid als ENSIA (Eenduidige Normatiek Single Information Audit); bij het afleggen van verantwoording wordt het principe toegepast dat alle

[1] Eindverslag visitatiecommissie Informatieveiligheid 'Durven leren', september 2017.
[2] https://informatiebeveiliging-gemeenten.nl/baseline-informatiebeveiliging/; geraadpleegd op 5 februari 2018.
[3] https://ensia.nl; geraadpleegd op 16 april 2018.

informatie die noodzakelijk is voor verticale verantwoording ook onderdeel is van het horizontale verantwoordingsproces. ENSIA is in 2017 in alle Nederlandse gemeenten geïmplementeerd.

Met ingang van 25 mei 2018 wordt in Nederland de Algemene Verordening Gegevensbescherming (AVG) van toepassing. De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer, de BIG is inmiddels in lijn gebracht met de AVG. *"Door deze nieuwe Europese wetgeving, de technische mogelijkheden en de decentralisaties wordt het veld rond privacy voor gemeenten steeds complexer. Privacy is niet langer een onderwerp waar alleen juristen mee bezig zijn; privacy raakt de hele gemeentelijke organisatie"*, aldus de visitatiecommissie Informatieveiligheid (2017, p.7). De inwerkingtreding van de AVG heeft voor gemeenten allerlei gevolgen die onder meer te maken hebben met:

- Bewustwording binnen de organisatie
- Inzicht in en documentatie van datastromen
- Het aanstellen van een security officer
- Risicoanalyse
- Het op orde brengen van procedures

In het licht van voorgaande bevindingen van de visitatiecommissie en recente ontwikkelingen in wet- en regelgeving is het interessant de informatiebeveiliging in de gemeente Súdwest-Fryslân te bestuderen.

1.2 Verschillende invalshoeken

Verschillende rekenkamer(commissie)s[4] deden recentelijk onderzoek naar informatieveiligheid in hun gemeenten. Het onderzoeksthema wordt in rekenkameronderzoek met verschillende termen aangeduid, waaronder digitale veiligheid, informatieveiligheid, informatiebeveiliging, beveiliging gevoelige informatie en vernieuwing ICT, en wordt door verschillende rekenkamers expliciet gekoppeld aan het thema privacy. Ook kiezen sommige rekenkamers er voor om zich in het bijzonder te richten op informatieveiligheid en privacy in het sociaal domein, een verband dat ook al werd gelegd door de visitatiecommissie Informatieveiligheid.

Uit een inventarisatie van eerder rekenkameronderzoek komt naar voren dat in onderzoek naar informatiebeveiliging verschillende invalshoeken worden onderscheiden, met elk hun eigen (combinatie van) onderzoeksmethoden:

[4] Rekenkamer Den Haag (2014), rekenkamer Breda (2016), rekenkamercommissie Dordrecht (2017), rekenkamercommissie Neder-Betuwe (2017), rekenkamer Rotterdam (2017), rekenkamer Heerlen (2017), rekenkamer Arnhem (2017), rekenkamercommissie Eindhoven (2016), rekenkamer Zeist (2017) en rekenkamercommissie Haarlemmermeer (2016).

Tabel 1 Invalshoeken, aspecten en onderzoeksmethoden

Invalshoeken	Aspecten	Methoden
Mens	Kennis, houding, gedrag, bewustwording van ambtelijke organisatie, raad en college	Phishing emails/spear phishing tests, inlooptesten, USB sticks achterlaten, raadsverkenning, interviews
Techniek	IT landschap, fysieke werkomgeving	Pentests/hackpogingen (black box test, grey box test), kwetsbaarhedenscan, forensic readiness scan
Beleid & governance	Vastgelegde kaders, doelen, werkwijzen, taken en verantwoordelijkheden, leiderschap, processen, informatiestromen	Documentanalyse, interviews met informatie- en ICT-medewerkers, de verantwoordelijk wethouder en sleutelpersonen binnen afdelingen (zoals Concerncontrol, griffie), enquête afdelingshoofden, enquête onder partners (bijv. zorgaanbieders)

In dit onderzoek naar de informatiebeveiliging in de gemeente Súdwest-Fryslân worden de drie invalshoeken (mens, techniek en beleid & governance) meegenomen, waarbij expliciet aandacht besteed zal worden aan de gevolgen van de huidige informatiebeveiliging voor de wijze waarop de gemeente zich tot haar inwoners wil verhouden.

1.3 Doelstelling, onderzoeksvragen & onderzoeksmethoden

Het doel van dit onderzoek is om inzicht te geven in de huidige staat van de informatiebeveiliging bij de gemeente Súdwest-Fryslân en de gevolgen hiervan alsmede het – indien nodig - formuleren van concrete verbeteracties. De centrale vraag van dit onderzoek luidt dan ook:

"In hoeverre heeft de gemeente Súdwest-Fryslân de informatiebeveiliging doeltreffend ingericht, dat wil zeggen, op zodanige wijze dat geen oneigenlijke toegang tot informatie kan worden verkregen, en wat zijn de gevolgen van de huidige informatiebeveiliging voor de beoogde relatie tussen de gemeente en haar inwoners[5]?"

De onderzoeksvragen die uit deze centrale vraag voortvloeien luiden als volgt:

1. Welke normen kunnen worden gesteld aan de informatiebeveiliging in gemeenten?
2. Hoe zijn het informatiebeveiligingsbeleid en de informatiebeveiligingsfunctie in de gemeente Súdwest-Fryslân vormgegeven?

[5] De gemeente Súdwest-Fryslân wil zich op een andere manier gaan verhouden tot haar inwoners. Zo geeft het college in het Hoofdlijnenakkoord Bestuursperiode 2018-2022 van 29 december 2017 aan te willen gaan werken vanuit de bedoeling (2017, p.11): *"We willen de dienstverlening vormgeven volgens de uitgangspunten van 'de bedoeling': mensgericht, inwoner centraal, minder systemen en bureaucratie, doen wat nodig is en maatwerk leveren"*.

3. In hoeverre heeft de gemeente Súdwest-Fryslân zicht op de belangrijkste risico's op het gebied van informatiebeveiliging, in het bijzonder waar het gaat om gevoelige informatie zoals persoonsgegevens?
4. In hoeverre is het mogelijk om oneigenlijk toegang te krijgen tot gevoelige informatie die de gemeente in beheer heeft? Welke technische en fysieke kwetsbaarheden en risico's zijn er te constateren in de informatiebeveiliging bij de gemeente Súdwest-Fryslân?
5. Op welke wijze wordt aandacht gegeven aan het bewustzijn onder medewerkers, raads- en collegeleden op het gebied van informatieveiligheid? En hoe is het gesteld met dat bewustzijn?
6. Wat zijn de (mogelijke) gevolgen van informatiebeveiliging voor de dienstverlening aan burgers?
7. Op welke wijze wordt de gemeenteraad geïnformeerd over informatiebeveiliging en in hoeverre biedt dit handvatten om invulling te geven aan zijn kaderstellende en controlerende rol?
8. Hoe kan het gevoerde beleid en de praktijk van de informatiebeveiliging in Súdwest-Fryslân worden beoordeeld aan de hand van het normenkader? En welke aanknopingspunten voor verdere verbetering van de informatiebeveiliging komen naar voren?

Dit onderzoek vindt plaats in de periode april t/m september 2018. De onderzoeksmethoden die bij de verschillende onderzoeksvragen worden gehanteerd worden weergegeven in de volgende tabel.

Tabel 2 Onderzoeksmethoden

Deelvraag	Literatuuronderzoek	Analyse beleidsdocumenten	Fysieke/technische scans en tests	Interview portefeuillehouder	Interviews sleutelpersonen	Raadsverkenning	Interview griffie
1	X	X					
2		X		X	X		
3		X		X	X		
4			X				
5			X	X	X	X	X
6				X	X		
7				X		X	X
8				X			

2. Planning & taakverdeling

Het onderzoek wordt deels in eigen beheer uitgevoerd en deels uitbesteed aan een extern bureau. De planning en taakverdeling zien er als volgt uit:

Tabel 3 Planning & taakverdeling

Activiteit	**Door wie**	**Week**	**Aantal uur**
Uitwerken onderzoeksopzet en analyse van beleidsdocumenten	Marsha Jet Rick	15-17	8 4 2
Benaderen en selecteren extern bureau	Marsha Jet	19-21	4 4
Interviews met portefeuillehouder, sleutelpersonen ambtelijke organisatie en griffie	Marsha Jet	21-24	20 20
Deelonderzoek door extern bureau		24-29	
Raadsverkenning	Marsha Jet	37	6 6
Analyse, conclusies en aanbevelingen	Marsha Jet Rick	38	20 20 2
Verslaglegging en communicatie	Marsha Jet Rick	39	20 20 2
Totaal			**158**