Zoeken naar de pragmatische grens

Informatieveiligheid in de gemeente Súdwest-Fryslân

Colofon

Rekenkamer Súdwest-Fryslân

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

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

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

Contactgegevens

Postadres: Postbus 10.000, 8600 HA Sneek

E-mail: rekenkamer@sudwestfryslan.nl

Website: www.gemeentesudwestfryslan.nl

Zoeken naar de pragmatische grens

Informatieveiligheid in de gemeente Súdwest-Fryslân

4 maart 2019

Samenvatting

1. Aanpak

In de tweede helft van 2018 heeft de rekenkamer onderzoek gedaan naar de informatiebeveiliging in de gemeente Súdwest-Fryslân en naar de gevolgen hiervan voor de informatieveiligheid in de gemeente om uiteindelijk, indien nodig, concrete verbeteracties te kunnen formuleren. De centrale vraag van dit onderzoek luidde 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?"

Deze centrale vraag viel uiteen in de volgende deelvragen:

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? En in hoeverre voldoet de gemeente daarmee aan landelijke en Europese normen?
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. Op welke wijze wordt aandacht gegeven aan de bewustwording onder medewerkers, raads- en collegeleden op het gebied van informatieveiligheid? En hoe is het gesteld met die bewustwording?
5. Welke kwetsbaarheden en risico's zijn er te constateren in de informatiebeveiliging bij de gemeente Súdwest-Fryslân?
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?

In dit onderzoek werd vanuit drie invalshoeken (mens, techniek en beleid & governance) naar de informatieveiligheid in de gemeente gekeken, waarbij de nadruk ligt op de invalshoeken mens en beleid & governance. Voor het beantwoorden van de vragen is gebruik gemaakt van verschillende onderzoeksmethoden. Naast literatuuronderzoek en een analyse van beleidsdocumenten zijn er interviews gehouden met de portefeuillehouder, met verschillende sleutelpersonen vanuit de ambtelijke organisatie en met de griffier. Ook zijn er verschillende tests (social engineering, spear phishing en het versturen van een algemene phishing mail) uitgevoerd door een extern bureau.

2. Resultaten

Vormgeving informatiebeveiligingsbeleid en informatiebeveiligingsfunctie

De gemeente Súdwest-Fryslân beschikt over een beleidskader waarin onder meer de visie en uitgangspunten ten aanzien van informatieveiligheid en privacy en de taken en verantwoordelijkheden zijn beschreven. Deze taken en verantwoordelijkheden zijn vervolgens zichtbaar belegd binnen de ambtelijke organisatie. Zo zijn er zijn een CISO en een FG aangesteld en een beveiligingsadviescommissie en een werkgroep privacy ingericht. De uitgangspunten voor het beheer, het gebruik en de uitwisseling van (persoons)gegevens zijn nog niet volledig beschreven en vastgesteld; zo waren de convenanten voor de uitwisseling van persoonsgegevens met ketenpartners, de autorisaties van medewerkers en het, in het kader van de AVG verplichte, verwerkingsregister nog niet op orde ten tijde van dit onderzoek.

Zicht op risico's

De gemeente voert periodieke risicoanalyses uit waarbij fysieke, personele en technische dreigingen in beeld worden gebracht en, op basis van hun grootte (waarschijnlijkheid x effect), worden gewogen. Ook wordt de vertaalslag gemaakt naar de maatregelen die getroffen moeten worden om de verschillende risico's te beperken. Daarnaast laat de gemeente onderzoek verrichten om zicht te krijgen op risico's.

Kwetsbaarheden en risico's in de praktijk

De gemeente heeft de afgelopen jaren, en ook zeer recent nog, aandacht besteed aan het informatiebewustzijn van de medewerkers en de regels, de risico's en de plicht om problemen en datalekken door te geven. Er lijkt geen aandacht te zijn geweest voor het informatiebewustzijn van de leden van het college van B&W en de gemeenteraad.

Hoewel er een procedure is voor de wijze waarop incidenten gemeld moeten worden zijn er twijfels over het functioneren hiervan in de praktijk. Incidenten en een inschatting van risico's leidt tot het treffen van maatregelen door de gemeente, maar deze maatregelen, in het bijzonder de maatregelen die gericht zijn op het informatiebewustzijn, zijn onvoldoende effectief; het blijkt mogelijk om op eenvoudige wijze medewerkers, raadsleden en collegeleden te bewegen om acties te ondernemen die voor de organisatie schadelijk zouden kunnen zijn.

Gevolgen voor dienstverlening aan burgers

Volgens medewerkers maken informatiebeveiligingsmaatregelen en privacywet- en regelgeving hun werk gecompliceerder en leiden deze tot extra administratieve lasten. Desondanks bestaat binnen de gemeente de indruk dat zij de balans weet te vinden tussen informatiebeveiliging en privacybescherming enerzijds en een kwalitatief goede dienstverlening aan haar inwoners anderzijds. Met name het delen van informatie met ketenpartners in het sociaal domein blijkt wel een aandachtspunt dat ten koste kan gaan van de kwaliteit van de zorg en hulpverlening.

Informatievoorziening aan de raad

Het beleid, de gemaakte afspraken en geplande acties ten aanzien van informatieveiligheid en privacy worden getoetst, gecontroleerd en verantwoord. Raadsleden worden op verschillende manieren geïnformeerd over privacy, informatiebeveiliging en de informatieveiligheid in de gemeente, bijvoorbeeld structureel via de jaarstukken, waar het een vast thema is in de paragraaf over bedrijfsvoering, en via de zelfevaluaties en de rapportages in het kader van ENSIA. De gemeenteraad lijkt daarmee de informatie te ontvangen die nodig is om zijn kaderstellende en controlerende taak met betrekking tot informatieveiligheid en privacy adequaat te kunnen vervullen. Wel worden er verbeterpunten in de toegankelijkheid van de verstrekte informatie gesignaleerd. Of de gemeenteraad daadwerkelijk actief invulling geeft aan zijn kaderstellende en controlerende rol op het gebied van informatieveiligheid en privacy wordt betwijfeld; de betrokkenheid van raadsleden bij de thema's lijkt beperkt.

3. Conclusies & aanbevelingen

Vervolgens werden in dit onderzoek de volgende conclusies en aanbevelingen geformuleerd:

Conclusie 1

De gemeente Súdwest-Fryslân beschikt over een actueel strategisch informatieveiligheidsbeleid en privacybeleid waarin onder meer visie, uitgangspunten, maatregelen en taken en verantwoordelijkheden zijn beschreven.

Conclusie 2

De informatiebeveiligingsfunctie is zichtbaar belegd binnen de gemeentelijke organisatie. Er is een nauwe samenwerking rond de thema's informatiebeveiliging en privacy met een duidelijke verdeling van verantwoordelijkheden.

Conclusie 3

De gemeente Súdwest-Fryslân heeft de uitgangspunten voor het beheer, gebruik en de uitwisseling van (persoons)gegevens deels beschreven en vastgesteld. De uitwerking van de kaders voor de uitwisseling van persoonsgegevens met ketenpartners, de autorisaties van medewerkers voor gemeentelijke systemen en het invoeren van het verwerkingsregister behoeven nadere uitwerking.

Aanbeveling Zorg, mede in het licht van de vereisten die met de AVG aan gemeenten worden gesteld, dat de kaders voor de uitwisseling van persoonsgegevens met ketenpartners en de autorisaties van medewerkers voor gemeentelijke systemen worden uitgewerkt en vastgelegd en dat het verwerkingsregister op korte termijn wordt ingevoerd.

Conclusie 4

Informatiebeveiligingsmaatregelen en privacywet- en regelgeving maken de dienstverlening gecompliceerder en leiden tot extra administratieve lasten, zo is nu nog de ervaring in de uitvoeringspraktijk. Desondanks lijkt de gemeente de balans te vinden tussen

informatiebeveiliging en privacy enerzijds en een kwalitatief goede dienstverlening aan haar inwoners anderzijds. Binnen de gemeente bestaat een pragmatische houding ten aanzien van informatiebeveiliging en privacy. Dit is begrijpelijk vanuit het oogpunt van de dienstverlening aan inwoners, maar kan in de uitvoeringspraktijk risico's met zich meebrengen wanneer die pragmatische houding niet wordt vertaald van beleidsafspraken naar een eenduidige werkwijze in de uitvoering.

Aanbeveling Zorg ervoor dat de uitgangspunten en regels ten aanzien van informatiebeveiliging en privacybescherming van inwoners niet worden ondermijnd door een te pragmatische werkwijze in de uitvoering. Zorg dat de CISO en de FG zowel in financieel als functioneel opzicht effectieve doorzettingsmacht hebben inzake de toepassing en naleving van de afspraken over informatiebeveiliging en privacybescherming.

Conclusie 5

De gemeente Súdwest-Frsylân probeert op actieve wijze inzicht te krijgen in de risico's voor de informatieveiligheid in de gemeente en lijkt hierin te slagen. Deze inzichten worden vervolgens vertaald naar maatregelen die echter niet (altijd) effectief blijken, in het bijzonder waar het gaat om het informatiebewustzijn van de betrokkenen.

Aanbeveling Laat tenminste één maal per jaar de gemeentelijke informatiebeveiliging door een externe partij testen op kwetsbaarheden, neem dit op in de P&C-cyclus en handel naar de bevindingen.

Conclusie 6

De gemeente benoemt het informatiebewustzijn van de medewerkers als risico voor de informatieveiligheid en heeft hier de afgelopen jaren aandacht aan besteed. Er is onvoldoende aandacht geweest voor het informatiebewustzijn van de leden van het college van B&W en de gemeenteraad. Een belangrijk deel van de in dit onderzoek gevonden kwetsbaarheden is terug te voeren op het informatiebewustzijn, het gedrag en de betrokkenheid van ambtelijke organisatie, raad en college. Ook lijkt er binnen de ambtelijke organisatie onbekendheid te bestaan over welke incidenten aan wie en op welke wijze gemeld moeten worden.

Aanbeveling Blijf inzetten op een proces van bewustwording en bekwaamheid ten aanzien van informatiebeveiliging en privacy dat verder gaat dan vrijblijvend informeren en betrek ook college en raad hierin. Zorg op alle niveaus binnen de organisatie dat medewerkers zich daadwerkelijk verantwoordelijk gaan voelen voor de informatieveiligheid.

Aanbeveling Zorg dat alle medewerkers de benodigde kennis hebben over welke informatieveiligheidsincidenten gemeld moeten worden, aan wie en op welke manier.

Conclusie 7

De gemeenteraad wordt op verschillende manieren geïnformeerd over informatieveiligheid waarmee hij in staat wordt gesteld zijn kaderstellende en controlerende functie uit te oefenen. Wel kan de raad hierin beter gefaciliteerd worden door het aanleveren van toegankelijker informatie. Ook kan de raad zelf zijn rol op dit gebied actiever oppakken.

Aanbeveling — Stel als raad vast of u voldoende informatie ontvangt over de verschillende aspecten van het informatiebeveiligings- en privacybeleid, welke informatie u eventueel verder nodig acht over informatiebeveiliging en privacybescherming, op welke strategische punten en op welke momenten de raad een verantwoordingsverslag wenst te hebben en bespreken en welke documenten de raad zelf wenst vast te stellen.

Aanbeveling — Spreek als raad af welke kaders en eventuele leertrajecten de gemeenteraad zelf nodig heeft om veilig en bewust om te gaan met informatie(systemen) en welke informatie de raad hiertoe nodig heeft.

Inhoud

Hoofdstuk 1 Het onderzoek

1.1 Achtergrond

1.1.1 Belang van het thema

In september 2017 heeft de visitatiecommissie Informatieveiligheid van de VNG een rapportage 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*".

1.1.2 Relevante ontwikkelingen

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 wijze waarop zij dat doen 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.[1] 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

[1] https://informatiebeveiliging-gemeenten.nl/baseline-informatiebeveiliging/; geraadpleegd op 5 februari 2018.

en DigiD zijn opgenomen in de zelfevaluatievragenlijst.[2] Deze integrale verantwoordingssystematiek wordt wel aangeduid als ENSIA (Eenduidige Normatiek Single Information Audit); bij het afleggen van verantwoording wordt het principe toegepast dat alle informatie die noodzakelijk is voor verticale verantwoording ook onderdeel is van het horizontale verantwoordingsproces. ENSIA is in 2017 in alle Nederlandse gemeenten geïmplementeerd, zo ook in de gemeente Súdwest-Fryslân.

Sinds 25 mei 2018 is in Nederland de Algemene Verordening Gegevensbescherming (AVG) van toepassing. De Wet bescherming persoonsgegevens (Wbp) geldt vanaf dat moment 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 functionaris gegevensbescherming (FG)
- Analyse van privacyrisico's
- Het op orde brengen van procedures, waaronder het opstellen van een register voor verwerkingsactiviteiten

Onlangs pleitte een privacyjurist van de VNG ervoor dat raadsleden er goed op moeten toezien dat colleges de juiste maatregelen nemen bij het voldoen aan privacywetgeving. Ook zij wijst op het toenemend belang van privacy als gevolg van de nieuwe taken die gemeenten er in de afgelopen jaren met name in het sociaal domein bij hebben gekregen en de toename van de hoeveelheid persoonsgegevens die door gemeenten worden verwerkt als gevolg van het steeds meer digitaal werken.

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

1.2 Invalshoek

1.2.1 Keuze voor invalshoeken

Verschillende rekenkamer(commissie)s[3] deden de afgelopen jaren 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

[2] https://ensia.nl; geraadpleegd op 16 april 2018.

[3] 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).

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:

Tabel 1.1 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, 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 informatieveiligheid in de gemeente Súdwest-Fryslân worden de drie invalshoeken (mens, techniek en beleid & governance) tot op zekere hoogte meegenomen, waarbij de nadruk ligt op de invalshoeken mens en beleid & governance.

1.2.2 Informatieveiligheid en dienstverlening

In dit onderzoek wordt expliciet aandacht besteed aan de gevolgen van de huidige informatiebeveiliging voor de wijze waarop de gemeente zich tot haar inwoners wil verhouden. In een rapportage van de Informatiebeveiligingsdienst (IBD) (2018) wordt gesteld dat juiste, volledige en beschikbare informatie een belangrijke randvoorwaarde van de dienstverlening van gemeenten vormt. Beschikbaarheid, integriteit en vertrouwelijkheid van gegevens worden van groot belang geacht. *"Persoonlijke gegevens van inwoners over werk, inkomen, zorg en welzijn maar ook gegevens die om andere redenen dan privacy bescherming als vertrouwelijk moeten worden aangemerkt vormen de kroonjuwelen van de gemeentelijke informatievoorziening"*, aldus de IBD (2018, p.4-5). 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 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"*. Interessant is nu om te bezien hoe de eisen van beschikbaarheid, integriteit en vertrouwelijkheid en de maatregelen die worden getroffen om deze te beschermen zich verhouden tot de wens van de gemeente om de dienstverlening volgens de bedoeling in te richten en bijvoorbeeld systemen en bureaucratie minder leidend te laten zijn en te doen wat nodig is voor de inwoner.

1.3 Doelstelling & onderzoeksvragen

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?"

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? En in hoeverre voldoet de gemeente daarmee aan landelijke en Europese normen?
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. Op welke wijze wordt aandacht gegeven aan de bewustwording onder medewerkers, raads- en collegeleden op het gebied van informatieveiligheid? En hoe is het gesteld met die bewustwording?
5. Welke kwetsbaarheden en risico's zijn er te constateren in de informatiebeveiliging bij de gemeente Súdwest-Fryslân?
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?

Voor wat betreft de te hanteren begrippen wordt aangesloten bij het begrippenkader zoals de gemeente Súdwest-Fryslân dat zelf heeft vastgelegd in haar informatieveiligheidsbeleid (2018, p.6). Informatieveiligheid is het doel en hierbij gaat het om beschikbaarheid, vertrouwelijkheid en integriteit van alle vormen van informatie(systemen). Informatiebeveiliging is het middel om informatieveiligheid te bereiken. Het gaat om het geheel aan maatregelen, procedures en processen die de beschikbaarheid, integriteit en vertrouwelijkheid van alle vormen van informatie binnen een organisatie garanderen.

1.4 Onderzoeksmethoden

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

Tabel 1.2 Onderzoeksmethoden

Onderzoeksvraag	Literatuuronderzoek	Analyse beleidsdocumenten	Tests	Interview portefeuillehouder	Interviews sleutelpersonen	Interview griffie
1	X	X				
2		X		X	X	
3		X		X	X	
4			X	X	X	X
5			X			
6				X	X	
7				X		X
8	X					

1.4.1 Desk research: literatuuronderzoek en analyse beleidsdocumenten

Allereerst heeft er in het kader van dit onderzoek desk research plaatsgevonden. Relevante literatuur is bestudeerd, waaronder verschillende landelijke rapportages die betrekking hebben op informatieveiligheid van gemeenten. Daarnaast zijn er verschillende (beleids)documenten van de gemeente Súdwest-Fryslân bestudeerd, in het bijzonder het Implementatieplan Informatiebeveiliging 2016-2017, het Strategisch Informatieveiligheidsbeleid 2018-2020, het Privacybeleid gemeente Súdwest-Fryslân 2018-2020 en de risico-inventarisatie en evaluatie van de informatieveiligheid van 2017. Hiermee werd een antwoord verkregen op de onderzoeksvragen 1 en (deels) 2 en 3.

1.4.2 Tests

Daarnaast zijn er een aantal tests uitgevoerd door een extern bureau, Vitaen. Dit bureau heeft verschillende aanvallen uitgevoerd met als doel het achterhalen van informatie. Daartoe heeft Vitaen onderzoek gedaan in openbare bronnen naar persoonsgegevens en andere bruikbare informatie voor een twaalftal sleutelpersonen binnen college en ambtelijke organisatie. Onder deze openbare bronnen vallen bijvoorbeeld social media en het internet waarbij er ook wachtwoorden werden verzameld die te vinden waren op het dark web (social engineering). Op basis van de gevonden informatie werd er een gerichte mail verzonden naar vijf sleutelpersonen (spear phishing). Voor deze gepersonaliseerde aanval werd een legitiem lijkende email opgesteld met daarin een link (URL) die is voorzien van 'goedaardige' malware. Op deze wijze werd getoetst in hoeverre het mogelijk was om 'remote access' te verkrijgen. Hiermee kan een hacker controle over een computer verkrijgen. Ook werd er een algemene phishing mail gestuurd naar alle raadsleden, waarbij het doel was het achterhalen van wachtwoorden die worden gebruikt voor de gemeentelijke (email)accounts. Op deze wijze werd (deels) inzicht gekregen in het informatiebewustzijn onder medewerkers, raads- en collegeleden (onderzoeksvraag 4) en in eventuele kwetsbaarheden en risico's voor wat betreft de informatieveiligheid (onderzoeksvraag 5).

Aangezien Vitaen een opdracht heeft uitgevoerd die in het IT-domein van gemeente Súdwest-Fryslân zijn effect heeft, zijn in dit onderzoek niet alleen de rekenkamer als opdrachtgever, maar ook de CISO en de internet service providers betrokken. Vitaen heeft zoveel mogelijk geprobeerd de impact/inbreuk op de betrokkenen te minimaliseren en heeft voor deze opdracht een vrijwaring gekregen van zowel de rekenkamer als de gemeente Súdwest-Fryslân.

1.4.3 Interviews

Ook hebben er in het kader van dit onderzoek verschillende interviews plaatsgevonden (zie bijlage I). In april 2018 vond er een startgesprek plaats met de gemeentesecretaris, de toenmalige Chief Information Security Officer (CISO) en de Functionaris Gegevensbescherming (FG). Binnen de ambtelijke organisatie hebben er vervolgens interviews plaatsgevonden met de CISO, de FG, de kwaliteitsmedewerker van het TIC en de teammanager van het gebiedsteam Sneek-Noord. Met deze sleutelpersonen werd gesproken over het beleid en de uitvoering daarvan, de mogelijke risico's voor de informatieveiligheid in Súdwest-Fryslân, het informatiebewustzijn binnen de gemeente en de mogelijke gevolgen voor de dienstverlening door de gemeente. Ook met de portefeuillehouder werd hierover gesproken in een gecombineerd interview met de gemeentesecretaris. Daarbij kwam ook de informatievoorziening aan de raad aan de orde. Tot slot werd de griffier geïnterviewd over de informatievoorziening aan de raad, de bewustwording van raadsleden ten aanzien van informatieveiligheid en de rol van de griffie hierin. Hiermee werd een antwoord verkregen op de onderzoeksvragen 2, 3, 4, 6 en 7.

Vervolgens werden de inzichten die met behulp van de desk research, de tests en de interviews werden verkregen gecombineerd en werd een antwoord geformuleerd op de vraag hoe het gevoerde beleid en de praktijk van de informatiebeveiliging in Súdwest-Fryslân kunnen worden beoordeeld aan de hand van het normenkader en werden aanknopingspunten voor een verdere verbetering van de informatiebeveiliging beschreven (onderzoeksvraag 8).

1.5 Leeswijzer

In het volgende hoofdstuk, hoofdstuk 2, wordt het normenkader beschreven. Vervolgens wordt in hoofdstuk 3 het beleid ten aanzien van informatiebeveiliging beschreven en wordt ingegaan op de wijze waarop de informatiebeveiligingsfunctie vorm heeft gekregen in de gemeente Súdwest-Fryslân. In hoofdstuk 4 wordt ingegaan op de risico's voor de informatieveiligheid zoals die vanuit de gemeente zelf worden benoemd en wordt aandacht besteed aan het beveiligingsbewustzijn binnen de gemeente. In hoofdstuk 5 worden deze thema's vervolgens verder uitgewerkt met behulp van de uitkomsten van het onderzoek van Vitaen. In hoofdstuk 6 wordt verkend wat de (mogelijke) gevolgen van informatiebeveiliging zijn voor de dienstverlening aan burgers, waarna in hoofdstuk 7 wordt ingegaan op de raad en het thema informatieveiligheid. In hoofdstuk 8, tot slot, worden de resultaten van dit onderzoek geanalyseerd en worden conclusies getrokken en aanbevelingen geformuleerd verdere verbetering van de informatiebeveiliging in de gemeente Súdwest-Fryslân.

Hoofdstuk 2 Normenkader

In dit hoofdstuk worden, mede op basis van eerder rekenkameronderzoek, de normen beschreven die kunnen worden gesteld aan de informatiebeveiliging in gemeenten. Hiermee wordt een antwoord geformuleerd op de eerste onderzoeksvraag.

Tabel 2.1 Normenkader

Vraag	Thema	Normen
2	Vormgeving informatiebeveiligingsbeleid en informatiebeveiligingsfunctie	• De gemeente beschikt over een actueel overkoepelend informatiebeveiligingsbeleid dat bestuurlijk is vastgesteld • Taken en verantwoordelijkheden voor informatiebeveiliging en de bescherming van persoonsgegevens zijn zichtbaar belegd binnen de gemeente • De gemeente heeft een Chief Information Security Officer (CISO) benoemd • De gemeente heeft uitgangspunten voor beheer, gebruik en uitwisseling van (persoons)gegevens beschreven en vastgesteld
3	Zicht op risico's	• De gemeente heeft de risico's voor informatieveiligheid vastgesteld en geanalyseerd • In het informatiebeveiligingsbeleid is beschreven welke risico's beheerst dan wel geaccepteerd worden, inclusief de bijbehorende maatregelen
4, 5	Kwetsbaarheden en risico's in de praktijk	• Alle medewerkers, raads- en collegeleden dienen bewust en veilig om te gaan met papieren, mondelinge en digitale informatie • De gemeente zorgt ervoor dat iedere medewerker goed op de hoogte is van de regels, de risico's en de plicht om problemen en datalekken door te geven. • De toegangsbeveiliging, -beheer en -controles moeten op orde zijn, zowel van gebouwen, afdelingen, personen en apparatuur, als van systemen, informatie en gegevens • De gemeente heeft een procedure vastgesteld voor de wijze waarop incidenten en zwakke plekken worden beheerd en gerapporteerd • De gemeente leert van incidenten
6	Gevolgen voor dienstverlening aan burgers	• De gemeente vindt de balans tussen informatiebeveiliging enerzijds en een kwalitatief goede dienstverlening (d.w.z. toegankelijk, transparant, faciliterend) aan haar inwoners anderzijds

7	Informatievoorziening aan de raad	• Het beleid, de gemaakte afspraken en geplande acties worden getoetst, gecontroleerd en verantwoord • De gemeenteraad ontvangt de informatie die nodig is om zijn kaderstellende en controlerende taak met betrekking tot informatieveiligheid adequaat te kunnen vervullen

Hoofdstuk 3 Inrichting informatiebeveiliging

In dit hoofdstuk wordt een antwoord geformuleerd op de vragen: *Hoe zijn het informatiebeveiligingsbeleid en de informatiebeveiligingsfunctie in de gemeente Súdwest-Fryslân vormgegeven? En in hoeverre voldoet de gemeente daarmee aan landelijke en Europese normen?*

Eind 2016 is in de gemeente Súdwest-Fryslân het **Implementatieplan Informatiebeveiliging 2016-2017** opgesteld. De basis van dit implementatieplan was een nulmeting aan de hand van een standaardvragenlijst die was afgeleid van de BIG. Doel van deze nulmeting was in de eerste plaats om zicht krijgen op de mate waarin de gemeente Súdwest-Fryslân voldoet aan de door de BIG gestelde normen, een zogenaamde gap-analyse. Het resultaat van deze nulmeting was een overzicht van beveiligingsmaatregelen die wel, niet of deels waren geïmplementeerd of waarvan op dat moment de status onbekend of niet van toepassing was. Vervolgens is er een risico-impactanalyse uitgevoerd om onderscheid te kunnen maken in maatregelen die hoge, gemiddelde of lage prioriteit hebben. In het implementatieplan wordt opgemerkt (2016, p.3): *"De gemiddelde score uit de nulmeting is overigens 80% en is een goede basis als vertrekpunt"*. De gemeente bleek opvallend laag te scoren op het beheer van incidenten en continuïteitsbeheer. Het implementatieplan had een gemeentebrede aanpak en had daarmee betrekking op alle informatiesystemen van de gemeente Súdwest-Fryslân, waaronder dus ook de BRP, PNIK, BAG, Suwinet en DigiD. Hoewel voor deze systemen afzonderlijke zelfevaluaties en audits gelden streeft de gemeente Súdwest-Fryslân naar het voorkomen van een fragmentarische insteek op het gebied van informatiebeveiliging. De gap- en risico-impactanalyse hebben geleid tot het formuleren van verschillende actiepunten voor 2016 en 2017. In het implementatieplan wordt gepleit voor het op korte termijn borgen van het proces van informatiebeveiliging in de vorm van een Information Security Management System (ISMS). Een ISMS zou ervoor zorgen dat geïmplementeerde beveiligingsmaatregelen periodiek getoetst en waar nodig aangepast worden en dat ontbrekende beveiligingsmaatregelen geïmplementeerd worden volgens een daarvoor vastgesteld tijdschema.

Begin 2018 verscheen de beleidsnota **Achter de cyberdijken van de gemeente Súdwest-Fryslân. Strategisch Informatieveiligheidsbeleid 2018-2020**. In deze beleidsnota worden de visie op en grondslagen en uitgangspunten van de informatiebeveiliging in de gemeente Súdwest-Fryslân beschreven. Belangrijk uitgangspunt voor de komende jaren is het verhogen van informatieveiligheid en het creëren van bewustwording in de organisatie. De gemeente Súdwest-Fryslân kiest veelal voor een gecombineerde aanpak van privacy, integriteit en informatieveiligheid en ziet hierin als grootste winst het verbeteren van de factor mens. *"Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van burgers en ondernemers. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn"*, zo staat de in de beleidsnota te lezen (2018, p.6). De gemeente wil hiervoor het hiervoor reeds genoemde ISMS als proces tot uitvoering brengen. In het informatieveiligheidsbeleid staat verder beschreven dat het belangrijk is dat medewerkers beveiligingsincidenten kunnen herkennen en dat zij weten hoe zij incidenten moeten melden (2018, p.19): *"Meld beveiligingsincidenten, datalekken (lekken van persoonsgegevens) en onveilige situaties direct bij de Servicedesk (4222) van team ICT, of neem rechtstreeks contact op met onze CISO (…) van team Informatievoorziening"*.

Ook werd in 2018 het **Privacybeleid gemeente Súdwest-Fryslân 2018-2020** vastgesteld. Hierin staat beschreven dat informatiebeveiliging en de bescherming van persoonsgegevens onlosmakelijk met elkaar zijn verbonden; informatiebeveiliging is een randvoorwaarde voor de borging van privacy bij de verwerking van persoonsgegevens. Als doelstelling van het privacybeleid is geformuleerd (2018, p.7): *"[…] het beschrijven van kaders voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de privacyrechten van personen waarvan de gemeente persoonsgegevens verwerkt"*. In het beleid zijn maatregelen en uitgangspunten beschreven die ertoe moeten leiden dat persoonsgegevens rechtmatig, behoorlijk en transparant kunnen worden verwerkt volgens geldende wet- en regelgeving. Ook wordt in het privacybeleid gesproken over de werkwijze en rolverdeling bij een datalek. Hiervoor wordt verwezen naar het Protocol meldplicht datalekken gemeente Súdwest-Fryslân. In het privacybeleid wordt expliciet gewezen op de vereisten die de AVG met zich meebrengt voor gemeenten.

Zowel in het informatieveiligheidsbeleid als in het privacybeleid zijn rollen, taken en verantwoordelijkheden van de verschillende betrokkenen beschreven. Het gaat hierbij om het college van B&W, de gemeenteraad, onderdelen van de ambtelijke organisatie (directie, lijnmanagement, teams) en specifieke functies binnen de ambtelijke organisatie (CISO, FG). Daarnaast wordt ingegaan op de invulling en rol van twee gremia, te weten de Beveiligingsadviescommissie (BAC) en de werkgroep privacy. In een tabel in bijlage II is dit verder uitgewerkt.

Hoofdstuk 4 Zicht op risico's

In dit hoofdstuk wordt (deels) antwoord gegeven op twee onderzoeksvragen:

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?

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?

4.1 Risico-inventarisatie

Eind 2017 werd de **Risico-inventarisatie en evaluatie van de Informatieveiligheid** in de raad behandeld. Deze is opgesteld op basis van de jaarlijkse risicoanalyse waarin verschillende generieke bedreigingen voor de informatiebeveiliging worden onderscheiden en worden onderverdeeld in fysieke, personele en ICT technische bedreigingen. Vervolgens wordt in een analysematrix gebruik gemaakt van bedreigingen per kwaliteitsaspect (data-integriteit, beschikbaarheid, vertrouwelijkheid en controleerbaarheid) van de informatiebeveiliging. Niet alle bedreigingen zijn even groot en om toch een inschatting te kunnen maken van de ernst van de risico's worden door de gemeente twee factoren ingevoerd waarmee de risico's ten opzichte van elkaar worden gewogen, namelijk waarschijnlijkheid en effect. De belangrijkste bevindingen van de risico-inventarisatie en evaluatie van de informatieveiligheid in 2017 luidden (2017, p.18):

- Er moet een testomgeving hardware matig ingericht worden. Dit is onderdeel van het project OTAP (Ontwikkeling, Test, Acceptatie, Productie). Reeds 1 project opgestart en 1 project is gepland, maar de projecten zijn gestrand en zullen opnieuw worden geagendeerd in 2018;
- Risico's, zoals phishing, virussen en hacking zijn een continue aandachtspunt; er is nu een betere monitoring op deze processen d.m.v. aansluiting op de IBD; Aangezien beveiligingsbewustzijn een wezenlijk onderdeel vormt van informatiebeveiliging zal hier continue aandacht voor worden gevraagd;
- Er zal meer nadruk komen te liggen op logging van raadplegingen alsook van het gebruik kritische ruimten en het gebruik van het gehele informatiesysteem door o.a. technische applicatiebeheerders en systeembeheerders. Het toegangssysteem wordt gebruikt voor logging van b.v. de serverruimtes.

Daarnaast komt in de rapportage aan de orde dat er nog steeds te veel gegevens in Corsa zichtbaar zijn voor niet-geautoriseerde medewerkers. Verder wordt voor de risicoanalyse in 2018 onderzocht of een nieuw of aangepast format voor een gemeentebrede risicoanalyse kan worden ingezet. Vanwege de gemeentebrede opzet van informatiebeveiliging wordt de personele samenstelling van de Beveiligingsadviescommissie (BAC) aangepast en ook wordt het algemene informatieveiligheidsbeleid geactualiseerd.

In het Jaarverslag 2017 wordt over informatieveiligheid en privacy vermeld dat op meerdere terreinen de situatie in 2017 is verbeterd dan wel afgerond. Concreet worden genoemd (2017, p.51 e.v.):

- De succesvolle afronding van de jaarlijkse DigiD audit (voor veilige uitwisseling van informatie en continuïteit van de digitale dienstverlening).
- Het voldoen aan veiligheidsnormen bij gebruik van Suwinet in het Sociaal Domein.
- Voor alle collega's is een bewustwordingscampagne over het leren herkennen van phishingmails afgerond.
- Op 25 mei 2018 wordt de Europese Algemene Verordening Gegevensbescherming (AVG) van kracht. Deze verordening vervangt de huidige Wet bescherming persoonsgegevens (Wbp). Op de invulling van een verplichte Functionaris Gegevensbescherming is in 2017 vroegtijdig ingespeeld en deze is reeds vervuld.
- De implementatie van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) vordert.

De gemeente Súdwest-Fryslân heeft in 2017 zes datalekken gemeld bij de Autoriteit Persoonsgegevens (AP), waarvan twee middelgrote datalekken. In beide gevallen hebben de betrokken inwoners een excuusbrief ontvangen. Er zijn ook meerdere beveiligingsincidenten geweest met een relatief kleine tot middelgrote inbreuk, in totaal 59 meldingen. Het gaat hierbij bijvoorbeeld om virussen en zwakheden in applicaties. De gemeente merkt hier in het Jaarverslag over op (2018, p.52): *"We anticiperen zoveel mogelijk op datalekken en beveiligingsincidenten en hebben procedures bij calamiteiten. Het voorkomen hiervan bestaat helaas niet, maar we werken continue aan bewustwording en herkenning van verdachte zaken."* In de Programmabegroting 2018 neemt de gemeente zich voor verdere technische en organisatorische maatregelen te nemen om het risico op datalekken nog meer te verkleinen en behalve dat ook te voldoen aan de Europese Algemene Verordening Gegevensbescherming. Eén van die maatregelen is het verder uitrollen van mogelijkheden om op een veilige manier met belanghebbenden persoonsgegevens uit te wisselen.

De CISO geeft aan voornemens te zijn in najaar van 2018 te starten met eigen risicoanalyses. Dit zullen geen standaardanalyses zijn; er wordt specifiek gekeken naar waar de risico's voor de gemeente Súdwest-Fryslân zitten. Aan de hand van deze risicoanalyses komen de pijnpunten naar boven die aangepakt moeten worden. Het is van belang de risico's af te wegen tegen de middelen en de wensen in een organisatie en van daaruit kijken naar wat de beste oplossing is voor die betreffende organisatie. Daarbij wordt ook gekeken naar hoe andere gemeenten de informatiebeveiliging aanpakken. De CISO's van de gemeenten Súdwest-Fryslân, De Fryske Marren, Heerenveen, Harlingen en Waadhoeke hebben overleg met elkaar, maar wat voor de ene gemeente werkt hoeft weer niet voor de andere gemeente te werken, aldus de CISO.

4.2 Van bewustwording naar bewustzijn

4.2.1 Aandacht voor beveiligingsbewustzijn

Zoals in de voorgaande paragraaf reeds beschreven hebben er in het verleden verschillende activiteiten plaatsgevonden, zoals phishingacties en e-learning activiteiten, om het beveiligingsbewustzijn van medewerkers te vergroten. Ook heeft de FG voorlichting gegeven aan groepen medewerkers, in 2018 ruim dertig keer. Tijdens de voorlichting heeft de FG het

onder andere gehad over hoe persoonsgegevens rechtmatig mogen worden verwerkt, wat de AVG inhoudt en wat datalekken zijn. Zij is daarbij gestart met de groepen die het meeste contact hebben met burgers, zoals de gebiedsteams, burgerzaken en het klantcontactcentrum, en de managers. De FG geeft aan dat het van belang is om medewerkers handvatten te geven. De manier waarop zij omgaan met persoonsgegevens zegt iets over de kwaliteit die de gemeente levert en verantwoord omgaan met deze gegevens moet een automatisme worden.

Toch constateren de verschillende respondenten dat er nog altijd een verschil zit in het beveiligingsbewustzijn van medewerkers. De CISO geeft aan dat je risico's nooit helemaal afgedicht krijgt, maar dat je als organisatie zo bewust mogelijk met informatie moet omgaan en vervolgens de technische middelen moet hebben om het op te vangen wanneer er iets mis gaat. De technische maatregelen moeten op orde zijn en zijn dus de eerste ring voor informatieveiligheid. Zij zijn ondersteunend aan de processen. Het bewustzijn van medewerkers is de tweede ring en vangt de overige risico's af. De CISO geeft aan dat 100% risicovrij niet mogelijk is, maar dat je door zo bewust mogelijk te werken een acceptabel restrisico kunt behalen. Informatiebeveiliging vereist naar haar mening een cultuuromslag. Medewerkers moeten zich afvragen: wat betekent informatiebeveiliging voor mij, mijn team en mijn werk? *"De firewalls en dergelijke zijn best goed geregeld, de technische zaken zijn prima op orde in de gemeente Súdwest-Fryslân, maar het bewustzijn van de medewerkers is een groot risico"*, aldus de CISO. Eind september 2018 is er, naast de voorlichtingsbijeenkomsten door de FG, een extra, bredere bewustwordingscampagne voor medewerkers gestart. De campagne wordt gevolgd door een e-learning en een 0-meting die alle medewerkers moeten invullen. Ook is zijn verschillende locaties van de gemeente recentelijk bezocht door een mystery guest om zicht te krijgen op de mate waarin het mogelijk is om fysiek toegang te krijgen tot gebouwen van de gemeente en tot informatie die daar aanwezig is.

4.2.2 Actuele risico's

Er wordt vanuit de ambtelijke organisatie aangegeven dat de gemeente Súdwest-Fryslân nog niet volledig *in control* is waar het gaat om haar informatiebeveiliging. Respondenten vinden dat de informatiebeveiliging niet slecht geregeld is in de gemeente, maar geven tegelijkertijd aan mogelijkheden voor verbetering en soms zelfs risico's te zien. Het gaat dan om verbeteringen in systemen, processen en procedures, maar - in samenhang daarmee - ook om een verbetering van de bewustwording en het gedrag van medewerkers. Eén van de respondenten merkt hierover op: *"De medewerkers zijn nu nog grotendeels onbewust onbekwaam en dat moet naar onbewust bekwaam en er is nog wel een weg af te leggen"*.

Onduidelijkheid over de incident respons organisatie

Een eerste verbeterpunt betreft de incident respons organisatie. De gemeente heeft beschreven wat er moet gebeuren als zich een incident voordoet, maar deze beschrijving is nog te simpel, aldus de CISO. De FG en de CISO zijn nu bezig met bedenken hoe ze de incident respons organisatie verder willen inrichten en hopen dit in 2019 af te ronden. Het is de bedoeling dat de CISO en de FG hier ook een plek in krijgen. Er worden op dit moment (te) weinig beveiligingsincidenten, waaronder datalekken, gerapporteerd en dat bevreemdt beide functionarissen, omdat zij er zeker van zijn dat dergelijke incidenten zich regelmatig

voordoen. Zij schrijven dit toe aan een gebrek aan informatiebeveiligingsbewustzijn bij de medewerkers; medewerkers zouden niet altijd weten wat een beveiligingsincident is, zij denken daarbij vaak alleen aan privacyschendingen, terwijl integriteit en beschikbaarheid van informatie ook van belang zijn. Dit beeld wordt niet herkend door de respondenten die werkzaam zijn bij het TIC en bij een gebiedsteam. Wanneer zich een incident voordoet dan wordt dat in het geval van het TIC via de supervisors gemeld bij de CISO. Wanneer zich een incident voordoet in een gebiedsteam dan meldt de teammanager dat bij de FG. Beide respondenten geven aan dat er weleens iets misgaat met betrekking tot informatieveiligheid, als voorbeeld noemen zij beide een situatie waarin er sprake was van een schending van de privacy, maar zij hebben tegelijkertijd niet de indruk dat dit op grote schaal het geval is.

(Toegang tot) systemen nog niet op orde

Ook wordt door verschillende respondenten opgemerkt dat het verwerkingsregister dat met de inwerkingtreding van de AVG verplicht is geworden nog niet op orde is in de gemeente Súdwest-Fryslân. In het register geeft de gemeente aan welke verwerkingen zij uitvoert ten aanzien van persoonsgegevens, zoals met wie er gegevens worden uitgewisseld en hoe ze worden bewaard. De gemeente krijgt daarmee ook de risico's ten aanzien van persoonsgegevens in beeld en raakt meer in control. Het opzetten van het register is uitbesteed en is naar verwachting in maart 2019 gereed.

Daarnaast is in het sociaal domein een nieuw regiesysteem aangeschaft: Gidso. In dit systeem houden de medewerkers van de gebiedsteams onder meer bij wat zij in welke casus hebben gedaan. Vanuit de gebiedsteams wordt aangegeven dat de komst van Gidso wel de belangrijke vraag oproept wie inzicht krijgt in welke gegevens. Het TIC kan nu bijvoorbeeld niet in het regiesysteem, maar straks wel in Gidso, al wordt de toegang beperkt tot het voorportaal. Een aandachtspunt daarbij is dat de interne controle, dat wil zeggen de medewerkers die kijken of de gebiedsteams doelmatig en rechtmatig hulp hebben ingezet en die het voorwerk voor de accountant doen, toegang heeft tot alle informatie in het huidige regiesysteem. De gebiedsteammanager is het er niet mee eens dat de betreffende medewerkers niet alleen de motivatie zien, maar ook alle informatie over wat er met een inwoner aan de hand is. Dit is meerdere keren in het MT besproken, maar schijnt in het huidige systeem niet anders te kunnen, aldus de betreffende respondent. Met Gidso wordt er opnieuw gekeken wie toegang heeft tot welke informatie en zij verwacht dat dit onderwerp dan weer aan de orde komt.

Een ander aandachtspunt dat wordt genoemd, en wat ook reeds aan de orde kwam in de voorgaande paragraaf, is het risico dat gepaard gaat met het werken met Corsa. Corsa is het documentair informatiesysteem waarin onder andere alle telefoontjes en brieven die bij de gemeente binnenkomen worden vastgelegd. Wie er toegang heeft tot het systeem, maar ook de bewaartermijnen van informatie zouden beter geregeld moeten worden. De FG geeft aan dat andere gemeenten met hetzelfde dilemma zitten en dat zij verwacht dat leveranciers hier op zullen inspringen en verschillende niveaus zullen aanbrengen in systemen, toegang en autorisaties. Tot op heden is dit echter nog niet goed geregeld. Noemenswaardig is dat in het kader van de gemeentelijke dienstverlening de komst van Corsa vijf jaar geleden juist werd toegejuicht.

Beperkingen technische infrastructuur

Wanneer de technische infrastructuur nog niet volledig op orde is, dan ervaren medewerkers hinder van informatiebeveiliging en dan gebeurt het dat zij gaan werken via bypasses, zo blijkt uit de interviews. Een voorbeeld hiervan is de invoering van beveiligd mailen via Cryptshare, een module binnen Outlook. Het mailen naar personen buiten de gemeente zou beveiligd moeten gebeuren. Een respondent vanuit de gebiedsteams geeft aan dat de medewerkers van de gebiedsteams niet bij alle zorgaanbieders mensen kennen en dat zij wanneer zij dan van de beveiligde mail gebruik willen maken eerst moeten gaan bellen bij wie zij moeten zijn. Vervolgens moet de beoogde ontvanger van de mail een wachtwoord krijgen om de mail te kunnen openen. Dat mag niet via de mail, maar moet bijvoorbeeld via een SMS naar een mobiel nummer. Vervolgens blijken wachtwoorden in de praktijk regelmatig niet te werken. De medewerkers van de gebiedsteams hebben het al druk en kiezen dan toch voor een bypass. Zij bellen dan bijvoorbeeld eerst met een aanbieder voor ze hem mailen en bespreken tijdens het telefoongesprek de casus. Vervolgens verwijzen zij dan in een mail, die op reguliere wijze verzonden wordt, naar de zojuist besproken casus. Ze hoeven dan de beveiligde mail niet te gebruiken, want dat vinden ze teveel gedoe, aldus een gebiedsteammanager. Vroeger stuurden medewerkers van de gebiedsteams een mailtje en dan hoopten zij dat het goed kwam. Dat dat niet wenselijk is, daar zijn de medewerkers het wel over eens. Zij zijn er van doordrongen dat er in de basis zorgvuldig met persoonsgegevens omgegaan moet worden en dat er voor bepaalde zaken toestemming gevraagd moet worden begrijpen zij wel, zo geeft de betreffende respondent aan. Ook bij het TIC moeten de medewerkers beveiligd mailen. Eerder werd er gemaild vanuit de kennisbank van Kana, maar als gevolg van de komst van de AVG moet er nu gemaild worden met behulp van Cryptshare. Ook bij het TIC verloopt dit nog niet optimaal. Zo worden de emailadressen van de medewerkers nu nog meegestuurd naar de klant. Vanuit het TIC wordt aangegeven dat men nu weer tijdelijk is overgestapt op onbeveiligd mailen.

Risico's als gevolg van de overgang naar centrale huisvesting

Verschillende respondenten wijzen op de risico's voor de informatieveiligheid die het gevolg kunnen zijn van de inrichting van en de beschikbare faciliteiten na de centrale huisvesting. Na het invoeren van de centrale huisvesting kan iedereen overal gaan zitten en zaken met elkaar bespreken. De CISO geeft aan een voorstander te zijn van zonering in het pand zodat teams bij elkaar zitten, weten waar zij hun spullen kwijt kunnen en teambesprekingen kunnen houden. Er komen op de nieuwe locatie wel privacy werkplekken, maar die plekken kunnen medewerkers niet claimen. Vanuit het perspectief van informatieveiligheid is centrale huisvesting dus niet ideaal. De FG merkt in dit verband op dat de bewustwording van medewerkers van groot belang is. Zij moeten het gevoel hebben dat zij gesteund worden en dat hun professionaliteit groot genoeg is om dit aan te kunnen. Medewerkers moeten privacy niet als iets lastigs zien.

4.2.3 Zoeken naar de pragmatische grens

Zowel door de portefeuillehouder als vanuit de ambtelijke organisatie wordt aangegeven dat er pragmatisch omgegaan moet worden met informatiebeveiliging. De portefeuillehouder merkt op dat hij informatiebeveiliging een belangrijk onderwerp vindt, maar dat het niet te

ver gejuridificeerd moet worden: *"Dan wordt het heel eng en moeilijk om als organisatie te functioneren"*. Hij ziet dat medewerkers vaak het zekere voor het onzekere nemen en het hoogste informatiebeveiligingsniveau kiezen, maar, zo geeft hij aan: *"Je zou echter moeten zoeken naar de pragmatische grens"*. De CISO deelt zijn mening. De informatiebeveiliging in de gemeente Súdwest-Fryslân is volgens haar zeker niet slecht geregeld, maar het kan beter. Naar haar mening komt dat komt omdat er nog vaak wordt gedacht: Hoe kunnen we de informatiebeveiliging op de best mogelijke manier vormgeven? Hoe staat het in de norm? En vervolgens wordt dat dan de procedure, terwijl dat in de praktijk niet haalbaar is. In de gemeente is men snel geneigd processen over te nemen van bijvoorbeeld BMC, maar medewerkers werken in de praktijk niet zo, de beste manier is gewoon teveel werk. Wanneer een medewerker iets in één stap kan doen, bijvoorbeeld het afhandelen van een telefoontje, dan doet hij of zij dat niet in zes stappen. Het is beter om te zeggen hoe je het wel doet en daarover te rapporteren, omdat je het dan ook kunt uitleggen als er een keer iets fout gaat. De CISO geeft verder aan dat er voor bijvoorbeeld DigiD en Suwinet bepaalde verplichtingen zijn waar je als gemeente aan moet voldoen, maar dat er voor andere zaken meer vrijheid is om te bepalen hoe je als gemeente een en ander inricht.

4.2.4 Het budget lijkt geen belemmering

De middelen die beschikbaar zijn voor informatiebeveiliging en privacy worden door alle respondenten vanuit de ambtelijke organisatie en de portefeuillehouder als voldoende ervaren, waarbij opvalt dat geen van de respondenten kan benoemen wat de omvang is van de beschikbare middelen. De CISO heeft voor de besteding van het budget altijd toestemming nodig van de teamleider. Wanneer de teamleider het niet eens zou zijn met de keuze van de CISO dan kan hij deze tegenhouden. In praktijk is dit volgens de CISO geen enkel probleem, de CISO en FG mogen hun budget vrij besteden, en mocht dit wel een probleem zijn dan beschikken zij nog over een escalatielijn.

4.2.5 Verantwoordelijkheid nemen

De CISO geeft aan te hopen dat in de toekomst meer vanuit het management aangegeven gaat worden welke informatie zij over informatiebeveiliging wil ontvangen van de CISO. Het gaat dan om informatie in aanvulling op de zelfevaluaties van ENSIA. ENSIA zegt alleen iets over of het systeem van informatiebeveiliging vandaag werkt en niet over of het gisteren werkte of morgen zal werken. ENSIA gaat over de systemen en ook wel over de mens, maar dan in het bijzonder over de inrichting van processen. De CISO geeft aan: "*Informatiebeveiliging is voor het management ook een ver van mijn bed show*".[4] Dit omdat het iets abstracts is en soms lastig te begrijpen. Het moet toegankelijker worden gebracht, vertaald worden naar wat een norm in de praktijk betekent, aldus de CISO.

Haar ervaring is dat in de organisatie door medewerkers nog weinig verantwoordelijkheid wordt genomen voor informatiebeveiliging, terwijl vanuit de organisatie bepaald zou moeten worden welke systemen prioriteit hebben en welke niet. Nu bedenkt de CISO dat samen met de business continuity manager, maar dat zou niet zo moeten zijn. Medewerkers zouden moeten aangeven hoe snel de verschillende gemeentelijke systemen bij een incident weer beschikbaar moeten zijn, met andere woorden, vanuit de business moet worden aangegeven

[4] In het ambtelijk wederhoor geeft het management aan deze opmerking te bestrijden.

wat belangrijk en wat minder belangrijk is. Mogelijk onderschatten medewerkers de risico's, maar volgens de CISO is de belangrijkste verklaring hiervoor dat medewerkers (nog) geen verantwoordelijkheid voelen voor hun eigen systeem en dat is een kwestie van bewustwording. Zij zien de teamleider van het team informatievoorziening als verantwoordelijk voor de informatievoorziening. Op zijn minst de managers zouden de systemen die nodig zijn voor de uitvoering van hun processen als hun verantwoordelijkheid moeten zien, aldus de CISO.

Hoofdstuk 5 Kwetsbaarheden in de informatiebeveiliging

In het voorgaande hoofdstuk is beschreven hoe er vanuit de gemeente Súdwest-Fryslân wordt aangekeken tegen de informatieveiligheid in de gemeente en worden verschillende risico's beschreven die vanuit de ambtelijke organisatie en door de portefeuillehouder worden gesignaleerd. Het informatiebewustzijn en gedrag van medewerkers worden daarbij als belangrijk, misschien wel het belangrijkste, aandachtspunt benoemd door de verschillende respondenten. Zoals in het eerste hoofdstuk reeds is beschreven heeft de rekenkamer een extern bureau, Vitaen, gevraagd te toetsen waar de risico's en kwetsbaarheden in de informatiebeveiliging in de gemeente Súdwest-Fryslân zitten om daarmee de vijfde onderzoeksvraag te kunnen beantwoorden.

Vitaen heeft een drietal activiteiten uitgevoerd, namelijk social engineering, spear phishing en het uitzetten van een algemene phishing mail. Voor twaalf sleutelpersonen, leden van het college en vertegenwoordigers van de ambtelijke organisatie, is op het internet gezocht naar informatie die bruikbaar kon zijn voor een gerichte aanval. Bij twee van de twaalf personen is nagenoeg geen informatie gevonden, bij de overige tien personen zijn voldoende aandachtspunten naar voren gekomen om een gerichte aanval uit te kunnen voeren. Vijf van deze personen zijn per mail benaderd, drie van hen hebben vervolgens gereageerd. Van twee personen waarvan een wachtwoord bekend was op het internet is geen reactie verkregen. Dit kan mogelijk gekomen zijn doordat in de twee weken voorafgaande aan de aanval soortgelijke aanvallen massaal plaatsvonden en dat de detectie daarop mogelijk kan zijn aangepast. Het is Vitaen gelukt om te communiceren met raadsleden, collegeleden en medewerkers, om wachtwoorden te achterhalen en mensen acties te laten uitvoeren (klikken op een link). Eén raadslid heeft bemerkt dat de aangeboden url (link) niet correct was. Drieëntwintig wachtwoorden van raadsleden zijn bekend geworden. Gebleken is dat deze wachtwoorden vrij eenvoudig zijn en dat deze bij een aanval gericht op het achterhalen van wachtwoorden makkelijk te kraken zijn.[5] Gebleken is dat er door de gemeente geen technische maatregelen zijn getroffen om dit te voorkomen.

Op basis van deze resultaten concludeert Vitaen dat het mogelijk is om op eenvoudige wijze het merendeel van de actoren (medewerkers, raadsleden en collegeleden) te bewegen om acties te ondernemen die voor de organisatie schadelijk zouden kunnen zijn, bijvoorbeeld omdat hackers daarmee toegang kunnen krijgen tot de gemeentelijke systemen. In twee

[5] In het ambtelijk wederhoor wordt vanuit de griffie het volgende aangegeven:

- *"vermelden dat het hierbij ging om het wachtwoord van GriffyNet (…); Eind vorig jaar is er namelijk overgegaan naar een andere leverancier v.w.b. GriffyNet. Ten behoeve van het nieuwe GriffyNet hebben de raads- en commissieleden op 7 december 2018 een mail ontvangen met betrekking tot het inloggen en het instellen van een nieuw wachtwoord. Dit is dezelfde dag geweest als de verstuurde phishingmail. Voorgaande zou voor enige verwarring kunnen hebben gezorgd nu de raadsleden werden doorgelinkt naar een soort Griffynet;*
- *daarnaast is het zo dat er vanuit de griffie zoveel mogelijk via GriffyNet wordt gecommuniceerd of via het mailadres griffie@sudwestfryslan.nl. De betreffende mail was gestuurd vanaf het adres van de plaatsvervangend griffier. Dit heeft waarschijnlijk wel het vermoeden van importantie gewekt bij de betreffende raadsleden;*
- *n.a.v. mails van raadsleden heeft de Griffie op maandagochtend gelijk een mail gestuurd naar de ICT-servicedesk van de gemeente en is er vanuit de griffie een mail gestuurd naar de raadsleden dat wanneer zij de betreffende mail hadden ontvangen zij geen actie moesten ondernemen."*

weken voorafgaand aan de week dat door Vitaen de acties werden uitgevoerd, werd in alle media nagenoeg dagelijks melding gemaakt van beveiligingsincidenten bij organisaties op het gebied van phishing. Hierdoor was de verwachting bij Vitaen dat veel mensen op hun hoede zouden zijn. Uit de resultaten blijkt echter dat deze berichtgeving in de landelijke media niet een zodanig effect heeft gehad dat mensen niet in de phishing activiteiten zijn getrapt. Van veel betrokkenen is veel informatie vrijelijk op het internet te vinden. Hierdoor zijn er verschillende mogelijkheden om gericht een aanval op een persoon uit te voeren. Vitaen constateert dat uit de hoge mate van respons op de phishing activiteiten en de eenvoud van de wachtwoorden niet kan worden opgemaakt dat activiteiten van de gemeente, zoals het verstrekken van een folder met de resultaten van phishing in de gemeente Súdwest-Fryslân, effectief is geweest en het Security Awareness niveau van de medewerkers op gewenste niveau heeft gebracht.

Hoofdstuk 6 Informatiebeveiliging versus dienstverlening

In het kader van dit onderzoek is verkend wat de mogelijke gevolgen van informatiebeveiliging in de gemeente Súdwest-Fryslân zijn voor de dienstverlening aan inwoners. Hierover is onder meer gesproken met respondenten die zicht hebben op de praktijk van de dienstverlening door het team Centrale Dienstverlening en de gebiedsteams. Het beeld dat op basis van deze gesprekken is ontstaan wordt in de volgende twee paragrafen beschreven. Daarmee wordt in dit hoofdstuk een antwoord geformuleerd op de vraag wat de mogelijke gevolgen van informatiebeveiliging zijn voor de dienstverlening aan burgers. Hierbij moet worden opgemerkt dat de ketenpartners en de inwoners zelf niet zijn geraadpleegd.

6.1 Dienstverlening door het team Centrale Dienstverlening

6.1.1 Het werkproces in het kort

Alle contacten met inwoners via de telefoon, de post en aan de balie verlopen via het team Centrale Dienstverlening. Contacten via de post worden door de postkamer geregistreerd in Corsa. De telefonische klantcontacten en de klantcontacten via de balie worden geregistreerd in het klantvolgsysteem Kana wat gekoppeld is aan een kennisbank. Alle medewerkers van het team Centrale Dienstverlening kunnen dit systeem raadplegen. Daarnaast kunnen ook de bedrijfscontactfunctionarissen in het klantvolgsysteem, maar zij hebben een aparte ingang en kunnen niet bij de contacten van het team Centrale Dienstverlening. De bedrijfscontactfunctionarissen en het team Centrale Dienstverlening kunnen elkaars werkvoorraad niet zien, maar kunnen elkaars klantcontacten wel opvragen. Als een klantvraag binnenkomt die bij het gebiedsteam thuishoort dan wordt een meldingsformulier voor het gebiedsteam aangemaakt. De gebiedsteammedewerkers nemen dan vervolgens contact op met de klant.

De medewerkers van het team Centrale Dienstverlening hebben toegang tot verschillende gemeentelijke systemen, bijvoorbeeld GWS (voor een bepaald deel), Suite voor werk en inkomen, het reinigingssysteem en het BOA registratiesysteem. Daarbij is het wel zo dat alleen medewerkers toegang krijgen tot deze systemen die het daadwerkelijk voor hun werk nodig hebben.

6.1.2 Wet- en regelgeving leidt tot dilemma's in de uitvoering…

Als de werkwijze van het team Centrale Dienstverlening volledig moet voldoen aan de AVG dan kan de dienstverlening in de knel komen, verwacht de kwaliteitsmedewerker van het team Centrale Dienstverlening. Medewerkers zouden dat nu al merken in de praktijk. Zij registreren op klantniveau, maar kunnen niet meer alle informatie kwijt. Wanneer een klant belt over een bepaald onderwerp, dan mag dat onderwerp niet meer worden vermeld in het klantvolgsysteem. Meldingen worden doorgezet naar de backoffice, maar medische of andere privacygevoelige gegevens mogen niet in de kennisbank geregistreerd worden. Dat belemmert het werken voor de backoffice; hoe meer zij weten, hoe gerichter zij aan de slag kunnen. Het werk wordt lastiger, want wat heb je nog aan een klantvolgsysteem als je niet meer kunt terugkijken waar een klant voor gebeld heeft? De kwaliteitsmedewerker is, evenals de

respondenten die eerder in paragraaf 4.2.3 werden aangehaald, van mening dat de situatie wel werkbaar moet blijven en dat er vanuit de gemeente een afweging gemaakt moet worden tussen de eisen van de AVG en de wensen ten aanzien van de gehanteerde werkwijzen door de gemeente. Eenzelfde soort dilemma doet zich voor bij de telefoonnotities in Corsa. In deze notities mag nu minder vermeld worden dan in het verleden. Er is recentelijk afgesproken om klantgegevens te wissen uit de kennisbank. Een klantcontact leidt tot een product en wanneer een product afgegeven is, dan is dat klantcontact niet meer nodig. Mocht een medewerker iets willen nazoeken, dan kan hij of zij de benodigde informatie wel uit de backofficesystemen halen. Medewerkers zitten in werkgroepjes om hierover mee te denken, maar het blijft een lastige puzzel om te bepalen hoe ver je gaat, aldus de kwaliteitsmedewerker. Zij geeft aan dat medewerkers nu vaker zelf vragen of ze het wel goed doen.

6.1.3 … maar gaat niet ten koste van de dienstverlening

Desondanks geeft de betreffende kwaliteitsmedewerker aan niet het idee te hebben dat privacy en informatiebeveiliging op dit moment ten koste gaan van de dienstverlening aan inwoners. Het is meer de vraag wat er in systemen wordt geregistreerd over de inwoners. Medewerkers vragen nu aan de klanten of zij het goed vinden dat er bepaalde informatie over hen in het systeem wordt vastgelegd. Daarbij is het wel de vraag hoe die toestemming vervolgens geregistreerd moet worden. Er bestaat geen spanningsveld tussen de medewerker en de klant in die zin dat de medewerker meer informatie zou willen hebben die hij eigenlijk niet mag krijgen. Klanten doen daar volgens de betreffende respondent ook niet zo moeilijk over, want: *“Zij weten nog niet zoveel van de AVG af”*. Medewerkers zijn zich wel bewust van de wijze waarop zij klantgegevens registeren en weten dat deze informatie met de komst van de AVG ook weer door klanten opgevraagd kan worden.

6.2 Dienstverlening door de gebiedsteams

6.2.1 Spanningsveld tussen wet- en regelgeving en uitgangspunten in het sociaal domein

De vereisten die voortvloeien uit de AVG raken de visie en daaruit voortvloeiende werkwijze van de gemeente Súdwest-Fryslân in het sociaal domein. De gemeente heeft gekozen voor brede gebiedsteams van 0 tot 100 jaar. De gebiedsteams werken met brede vraagverheldering, dat wil zeggen dat op alle leefgebieden wordt uitgevraagd hoe het met inwoners gaat en waar zij tegenaan lopen. De gebiedsteammanager waar in het kader van dit onderzoek mee gesproken is geeft aan begrepen te hebben dat een dergelijke werkwijze vanuit de AVG gezien formeel niet mag, maar wel kan wanneer in het eerste gesprek aan de inwoner is uitgelegd waarom de gebiedsteams een dergelijke werkwijze hanteren en er toestemming is verleend door de inwoner. Dit is dan ook de werkwijze die de gebiedsteams op dit moment hanteren. Het advies van de FG aan de gebiedsteams is om zo transparant mogelijk te zijn; leg uit waarom je wat doet en leg dat vervolgens goed vast. Dit kan extra administratieve handelingen vragen en medewerkers hebben volgens haar soms het gevoel dat de dienstverlening aan de inwoners wordt belemmerd. Een dergelijke werkwijze draagt naar haar mening echter bij aan de professionele houding en kwaliteit van de dienstverlening. De gemeentesecretaris benadrukt ook hier het belang van een pragmatische insteek; er moet

naar zijn mening in het sociaal domein een goede balans worden gevonden tussen effectieve hulpverlening en informatiebeveiliging.

6.2.2 Moeizame informatiedeling met ketenpartners

Het grootste aandachtspunt in de uitvoering is volgens de gebiedsteammanager het tijdig kunnen delen van informatie met ketenpartners, zoals woningcorporaties en energieleveranciers, zodat de gebiedsteams ook preventief kunnen werken. De komst van de AVG heeft de samenwerking met ketenpartners echter bemoeilijkt. Gebiedsteams kunnen via ketenpartners signalen krijgen dat inwoners in de schulden dreigen te raken zodat zij vroegtijdig kunnen ingrijpen. Wanneer de gebiedsteams dergelijke signalen niet meer ontvangen dan wordt vroegtijdig ingrijpen lastig; het is al een aantal keer gebeurd dat er sprake was van een dreigende huisuitzetting en dan is het eigenlijk al te laat, aldus de respondent. Dergelijke signalen werden in het verleden makkelijker doorgegeven, maar verschillende ketenpartners geven nu aan dit niet meer te doen. De informatie-uitwisseling met ketenpartners moet met behulp van convenanten worden geregeld, maar deze convenanten zijn er nog niet en daar hebben de medewerkers van de gebiedsteams last van. De gebiedsteammedewerkers weten welke informatie zij met wie mogen uitwisselen, dit is recentelijk niet heel erg veranderd, maar de manier waarop zij informatie moeten uitwisselen is wel aanzienlijk veranderd. Niet alleen ketenpartners zijn terughoudender geworden bij het uitwisselen van informatie, de gebiedsteammedewerkers zelf ook. Er moet nu meer georganiseerd worden om informatie uit te kunnen wisselen. Daar zijn medewerkers zich van bewust en daar hebben ze soms ook last van.

6.2.3 Van inzicht naar eigen regie

Ook de gebiedsteammanager wijst op de toenemende mogelijkheden voor inwoners om zicht te krijgen op de gegevens die in de gemeentelijke systemen over hen zijn vastgelegd. Het is uiteindelijk de bedoeling dat inwoners zelf in het nieuwe regiesysteem Gidso kunnen kijken. De gebiedsteammanager vindt het heel belangrijk dat inwoners weten welke informatie de gemeente over hen heeft en vindt het goed dat hier nu stappen in worden gezet. Daar zitten inhoudelijke discussies aan vast en medewerkers moeten goed nadenken over hoe ze formuleren wanneer ze informatie over inwoners registreren. Daar is men nu al alert op, maar dat zal alleen nog maar meer nodig zijn wanneer het systeem wordt opengesteld voor inwoners. Wanneer een inwoner toestemming geeft is het van belang dat hij weet waarvoor hij toestemming geeft en weet dat hij ook *geen* toestemming kan geven. Wanneer Gidso wordt opengesteld voor inwoners dan kunnen gebiedsteammedewerkers en inwoner samen bekijken welke informatie aan wie verstrekt wordt en waarvoor toestemming wordt gevraagd. De eigen regie van de inwoner wordt daarmee versterkt. Tegelijkertijd moet de gemeente er wel alert op zijn dat niet iedere inwoner met een dergelijk systeem uit de voeten kan, aldus de gebiedsteammanager.

Hoofdstuk 7 Informatievoorziening raad

In dit hoofdstuk wordt ingegaan op de wijze waarop de gemeenteraad wordt geïnformeerd over informatiebeveiliging en op de mate waarin dit handvatten biedt om invulling te geven aan zijn kaderstellende en controlerende rol. Daarmee wordt een antwoord geformuleerd op onderzoeksvraag 7.

7.1 Raadsleden ontvangen openbare informatie

Raadsleden in de gemeente Súdwest-Fryslân hebben toegang tot iBabs, een systeem waarin alle vergaderstukken staan. Deze stukken zijn openbaar en zijn daarnaast ook op internet te vinden. Ook hebben raadsleden toegang tot intranet (GriffyNet) waarvoor zij een wachtwoord moeten gebruiken. De griffier geeft aan dat raadsleden bijna geen vertrouwelijk stukken ontvangen. Wanneer er geheimhouding ligt op stukken dan kunnen raadsleden deze inzien bij de griffie. En hoewel er gemeenten zijn waar met enige regelmaat vertrouwelijke raadsbijeenkomsten plaatsvinden, is dat in de gemeente Súdwest-Fryslân niet het geval. Raadsleden hebben geen directe toegang tot gemeentelijke informatiesystemen anders dan iBabs of GriffyNet. Wanneer inwoners via het post- of mailadres van de gemeente brieven of mails richten aan de raad dan krijgen raadsleden deze via GriffyNet te zien. Inwoners krijgen in dat geval bericht van de griffie dat hun brief of mail ter kennisname is gesteld aan de raad. Mailtjes aan individuele raadsleden worden doorgestuurd aan het betreffende raadslid en ook daar wordt de inwoner van op de hoogte gesteld.

In het kader van de AVG heeft de griffie samen met de FG gekeken naar de informatie die door de griffie wordt bijgehouden en zijn ook de werkprocessen van de griffie tegen het licht gehouden. Daar is niets vreemds uitgekomen, aldus de griffier. De gegevens van raadsleden staan op de website en zijn dus openbaar en dat weten raadsleden ook. Er is een protocol voor incidenten, bijvoorbeeld wanneer raadsleden lastig gevallen worden. De griffiemedewerkers gaan naar de bijeenkomsten over informatiebeveiliging en gaan dan na of zij met hetgeen zij daar horen nog iets moeten richting de raadsleden. De griffie kan wel in (een deel van) de gemeentelijke systemen. Zo kunnen griffiemedewerkers bijvoorbeeld zien welke collegestukken eraan zitten te komen.

De griffier is van mening dat, aangezien raadsleden alleen openbare stukken krijgen, er met hen ook niet over informatiebeveiliging gesproken hoeft te worden. Ook de gemeentesecretaris wijst op het overwegend openbare karakter van de informatie die raadsleden ontvangen en geeft aan dat de griffie bezig zou moeten zijn met de vraag hoe raadsleden met gemeentelijke informatie en informatie van inwoners omgaan. De campagne die in september is gestart is dan ook *niet* gericht op het informatiebewustzijn van raadsleden.

7.2 Interesse in informatieveiligheid lijkt beperkt

Raadsleden worden op verschillende manieren geïnformeerd over privacy, informatiebeveiliging en de informatieveiligheid in de gemeente. Dit gebeurt bijvoorbeeld structureel via de jaarstukken, waar het een vast thema is in de paragraaf over bedrijfsvoering, en via de zelfevaluaties en de rapportages in het kader van ENSIA.

Verschillende respondenten geven aan dat de belangstelling van raadsleden voor het thema informatieveiligheid beperkt lijkt. Zo merkt de griffier op dat raadsleden informatiebeveiliging meer zien als *"iets wat bij de bedrijfsvoering hoort en waarvan je als organisatie moet zorgen dat je het goed geregeld hebt"*. Raadsleden krijgen de verschillende rapportages onder ogen, maar het is geen thema waar zij vervolgens uitgebreid over spreken of waar zij vragen over stellen. Zij nemen het overwegend voor kennisgeving aan. Slechts enkele raadsleden stellen vragen over informatiebeveiliging en privacy, maar dat zijn er niet veel. De gemeentesecretaris geeft aan dat raadsleden hooguit een enkele keer vragen stellen over hoe een en ander is geregeld in de gemeente. Volgens hem spreekt daar het vertrouwen uit dat het geregeld is. De portefeuillehouder voegt hier aan toe dat in de raad wordt gesproken over hoofdlijnen en dat informatiebeveiliging op uitvoeringsniveau zit. Ook over het budget voor informatiebeveiliging en privacybeleid worden geen discussies gevoerd in de raad, aldus de betreffende respondenten.

De FG en de CISO blijken kritischer ten aanzien van de houding van de raad waar het gaat om privacy en informatiebeveiliging. De FG geeft aan dat zij aan de griffie en de wethouder heeft voorgesteld voorlichting te geven aan raadsleden, maar dat zij daar tot op heden nog geen reactie op heeft gehad, terwijl zij in andere gemeenten waar zij werkt of heeft gewerkt wel met de raad heeft gesproken. De raad lijkt zich niet bezig te houden met het onderwerp privacy of de AVG en dat is naar haar mening wel vreemd aangezien de raad ook brieven van de VNG ontvangt over het belang van de bescherming van persoonsgegevens en de taak daarin voor de raad. Geen enkel raadslid heeft nog gevraagd hoe dit is geregeld in de gemeente Súdwest-Fryslân. Haar ervaring is dat zowel de wethouder als de gemeentesecretaris zeer begaan zijn met het onderwerp. De CISO geeft ten tijde van het onderzoek aan dat zij nog niet weet of informatieveiligheid hoog op de agenda staat van het college en de raad. Zij had op dat moment nog niet kennisgemaakt met de portefeuillehouder en had vanuit de raad nog geen enkele vraag gekregen.[6] De ENSIA rapportage is wel naar de raad gegaan, maar dat rapport is erg technisch, abstract en moeilijk leesbaar. Daardoor kan zij goed begrijpen dat de raad dit niet goed kan lezen, terzijde legt en vertrouwt op de expertise van de ambtelijke organisatie.

Zij wil daarom vanaf 2018 een eigen rapportage over ENSIA maken die meer toegankelijk is. Zij heeft verder de indruk dat raadsleden niet geïnformeerd zijn over de wijze waarop zij moeten/mogen omgaan met hun Súdwest-Fryslânmail.

[6] In het ambtelijk wederhoor wordt door de gemeentesecretaris en de portefeuillehouder aangegeven dat er inmiddels een goed contact is tussen de portefeuillehouder, de gemeentesecretaris en de medewerkers die primair betrokken zijn bij informatieveiligheid en dat zowel de directie als het college het belang en organisatie van informatiebeveiliging evident vinden.

Hoofdstuk 8 Analyse, conclusies en aanbevelingen

In dit laatste hoofdstuk worden de resultaten van dit onderzoek geanalyseerd en worden conclusies getrokken en aanbevelingen geformuleerd verdere verbetering van de informatiebeveiliging in de gemeente Súdwest-Fryslân. Daarmee wordt een antwoord geformuleerd op onderzoeksvraag 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?*

8.1 Analyse

Vormgeving informatiebeveiligingsbeleid en informatiebeveiligingsfunctie

Met de beleidsnota's "Achter de cyberdijken van de gemeente Súdwest-Fryslân. Strategisch Informatieveiligheidsbeleid 2018-2020" en "Privacybeleid gemeente Súdwest-Fryslân 2018-2020" beschikt de gemeente over een beleidskader waarin onder meer de visie en uitgangspunten ten aanzien van informatieveiligheid en privacy en de taken en verantwoordelijkheden zijn beschreven. Deze taken en verantwoordelijkheden zijn vervolgens zichtbaar belegd binnen de ambtelijke organisatie. Zo zijn er zijn een CISO en een FG aangesteld en een beveiligingsadviescommissie en een werkgroep privacy ingericht. De uitgangspunten voor het beheer, het gebruik en de uitwisseling van (persoons)gegevens zijn nog niet volledig beschreven en vastgesteld; zo waren de convenanten voor de uitwisseling van persoonsgegevens met ketenpartners, de autorisaties van medewerkers en het, in het kader van de AVG verplichte, verwerkingsregister nog niet op orde ten tijde van dit onderzoek.

Zicht op risico's

De gemeente voert periodieke risicoanalyses uit waarbij fysieke, personele en technische dreigingen in beeld worden gebracht en, op basis van hun grootte (waarschijnlijkheid x effect), worden gewogen. Ook wordt de vertaalslag gemaakt naar de maatregelen die getroffen moeten worden om de verschillende risico's te beperken. Daarnaast laat de gemeente onderzoek verrichten om zicht te krijgen op risico's; zo heeft recentelijk een mystery guest twee locaties van de gemeente bezocht om risico's met betrekking tot de fysieke toegangsbeveiliging in beeld te brengen.

Kwetsbaarheden en risico's in de praktijk

De gemeente heeft de afgelopen jaren, en ook zeer recent nog, aandacht besteed aan het informatiebewustzijn van de medewerkers en de regels, de risico's en de plicht om problemen en datalekken door te geven. Er lijkt geen aandacht te zijn geweest voor het informatiebewustzijn van de leden van het college van B&W en de gemeenteraad.

Hoewel er een procedure is voor de wijze waarop incidenten gemeld moeten worden zijn er twijfels over het functioneren hiervan in de praktijk. Incidenten en een inschatting van risico's leidt tot het treffen van maatregelen door de gemeente, maar deze maatregelen, in

het bijzonder de maatregelen die gericht zijn op het informatiebewustzijn, zijn onvoldoende effectief; het blijkt mogelijk om op eenvoudige wijze medewerkers, raadsleden en collegeleden te bewegen om acties te ondernemen die voor de organisatie schadelijk zouden kunnen zijn.

Gevolgen voor dienstverlening aan burgers

Volgens medewerkers maken informatiebeveiligingsmaatregelen en privacywet- en regelgeving hun werk gecompliceerder en leiden deze tot extra administratieve lasten. Desondanks bestaat binnen de gemeente de indruk dat zij de balans weet te vinden tussen informatiebeveiliging en privacybescherming enerzijds en een kwalitatief goede dienstverlening aan haar inwoners anderzijds. Met name het delen van informatie met ketenpartners in het sociaal domein blijkt wel een aandachtspunt dat ten koste kan gaan van de kwaliteit van de zorg en hulpverlening.

Informatievoorziening aan de raad

Het beleid, de gemaakte afspraken en geplande acties ten aanzien van informatieveiligheid en privacy worden getoetst, gecontroleerd en verantwoord. Raadsleden worden op verschillende manieren geïnformeerd over privacy, informatiebeveiliging en de informatieveiligheid in de gemeente, bijvoorbeeld structureel via de jaarstukken, waar het een vast thema is in de paragraaf over bedrijfsvoering, en via de zelfevaluaties en de rapportages in het kader van ENSIA. De gemeenteraad lijkt daarmee de informatie te ontvangen die nodig is om zijn kaderstellende en controlerende taak met betrekking tot informatieveiligheid en privacy adequaat te kunnen vervullen. Wel worden er verbeterpunten in de toegankelijkheid van de verstrekte informatie gesignaleerd. Of de gemeenteraad daadwerkelijk actief invulling geeft aan zijn kaderstellende en controlerende rol op het gebied van informatieveiligheid en privacy wordt betwijfeld; de betrokkenheid van raadsleden bij de thema's lijkt beperkt.

Tabel 8.1 De normen versus de praktijk

Vraag	Thema	Normen	De praktijk
2	Vormgeving informatiebeveiligingsbeleid en informatiebeveiligingsfunctie	De gemeente beschikt over een actueel overkoepelend informatiebeveiligingsbeleid dat bestuurlijk is vastgesteld	Aan voldaan
		Taken en verantwoordelijkheden voor informatiebeveiliging en de bescherming van persoonsgegevens zijn zichtbaar belegd binnen de gemeente	Aan voldaan
		De gemeente heeft een Chief Information Security Officer (CISO) benoemd	Aan voldaan
		De gemeente heeft uitgangspunten voor beheer, gebruik en uitwisseling van (persoons)gegevens beschreven en vastgesteld	Deels aan voldaan

3	Zicht op risico's	De gemeente heeft de risico's voor informatieveiligheid vastgesteld en geanalyseerd	Aan voldaan
		In het informatiebeveiligingsbeleid is beschreven welke risico's beheerst dan wel geaccepteerd worden, inclusief de bijbehorende maatregelen	Aan voldaan
4, 5	Kwetsbaarheden en risico's in de praktijk	Alle medewerkers, raads- en collegeleden dienen bewust en veilig om te gaan met papieren, mondelinge en digitale informatie	Niet aan voldaan
		De gemeente zorgt ervoor dat iedere medewerker goed op de hoogte is van de regels, de risico's en de plicht om problemen en datalekken door te geven.	Deels aan voldaan
		De toegangsbeveiliging, -beheer en –controles moeten op orde zijn, zowel van gebouwen, afdelingen, personen en apparatuur, als van systemen, informatie en gegevens	Kan niet worden beoordeeld[7]
		De gemeente heeft een procedure vastgesteld voor de wijze waarop incidenten en zwakke plekken worden beheerd en gerapporteerd	Aan voldaan
		De gemeente leert van incidenten	Deels aan voldaan
6	Gevolgen voor dienstverlening aan burgers	De gemeente vindt de balans tussen informatiebeveiliging enerzijds en een kwalitatief goede dienstverlening (d.w.z. toegankelijk, transparant, faciliterend) aan haar inwoners anderzijds	Deels aan voldaan
7	Informatievoorziening aan de raad	Het beleid, de gemaakte afspraken en geplande acties worden getoetst, gecontroleerd en verantwoord	Aan voldaan
		De gemeenteraad ontvangt de informatie die nodig is om zijn kaderstellende en controlerende taak met betrekking tot informatieveiligheid adequaat te kunnen vervullen	Aan voldaan

8.2 Conclusies & aanbevelingen

Conclusie 1

De gemeente Súdwest-Fryslân beschikt over een actueel strategisch informatieveiligheidsbeleid en privacybeleid waarin onder meer visie, uitgangspunten, maatregelen en taken en verantwoordelijkheden zijn beschreven.

[7] De gemeente SWF heeft hier onlangs onderzoek naar laten doen door bezoeken van een mystery guest aan twee locaties van de gemeente. De bevindingen hiervan zijn nog vertrouwelijk en worden in februari 2019, samen met de resultaten van de 0-meting die plaatsvindt in het kader van de bewustwordingscampagne, bekend gemaakt.

Conclusie 2

De informatiebeveiligingsfunctie is zichtbaar belegd binnen de gemeentelijke organisatie. Er is een nauwe samenwerking rond de thema's informatiebeveiliging en privacy met een duidelijke verdeling van verantwoordelijkheden.

Conclusie 3

De gemeente Súdwest-Fryslân heeft de uitgangspunten voor het beheer, gebruik en de uitwisseling van (persoons)gegevens deels beschreven en vastgesteld. De uitwerking van de kaders voor de uitwisseling van persoonsgegevens met ketenpartners, de autorisaties van medewerkers voor gemeentelijke systemen en het invoeren van het verwerkingsregister behoeven nadere uitwerking.

Aanbeveling Zorg, mede in het licht van de vereisten die met de AVG aan gemeenten worden gesteld, dat de kaders voor de uitwisseling van persoonsgegevens met ketenpartners en de autorisaties van medewerkers voor gemeentelijke systemen worden uitgewerkt en vastgelegd en dat het verwerkingsregister op korte termijn wordt ingevoerd.

Conclusie 4

Informatiebeveiligingsmaatregelen en privacywet- en regelgeving maken de dienstverlening gecompliceerder en leiden tot extra administratieve lasten, zo is nu nog de ervaring in de uitvoeringspraktijk. Desondanks lijkt de gemeente de balans te vinden tussen informatiebeveiliging en privacy enerzijds en een kwalitatief goede dienstverlening aan haar inwoners anderzijds. Binnen de gemeente bestaat een pragmatische houding ten aanzien van informatiebeveiliging en privacy. Dit is begrijpelijk vanuit het oogpunt van de dienstverlening aan inwoners, maar kan in de uitvoeringspraktijk risico's met zich meebrengen wanneer die pragmatische houding niet wordt vertaald van beleidsafspraken naar een eenduidige werkwijze in de uitvoering.

Aanbeveling Zorg ervoor dat de uitgangspunten en regels ten aanzien van informatiebeveiliging en privacybescherming van inwoners niet worden ondermijnd door een te pragmatische werkwijze in de uitvoering. Zorg dat de CISO en de FG zowel in financieel als functioneel opzicht effectieve doorzettingsmacht hebben inzake de toepassing en naleving van de afspraken over informatiebeveiliging en privacybescherming.

Conclusie 5

De gemeente Súdwest-Frsylân probeert op actieve wijze inzicht te krijgen in de risico's voor de informatieveiligheid in de gemeente en lijkt hierin te slagen. Deze inzichten worden vervolgens vertaald naar maatregelen die echter niet (altijd) effectief blijken, in het bijzonder waar het gaat om het informatiebewustzijn van de betrokkenen.

Aanbeveling Laat tenminste één maal per jaar de gemeentelijke informatiebeveiliging door een externe partij testen op kwetsbaarheden, neem dit op in de P&C-cyclus en handel naar de bevindingen.

Conclusie 6

De gemeente benoemt het informatiebewustzijn van de medewerkers als risico voor de informatieveiligheid en heeft hier de afgelopen jaren aandacht aan besteed. Er is onvoldoende aandacht geweest voor het informatiebewustzijn van de leden van het college van B&W en de gemeenteraad. Een belangrijk deel van de in dit onderzoek gevonden kwetsbaarheden is terug te voeren op het informatiebewustzijn, het gedrag en de betrokkenheid van ambtelijke organisatie, raad en college. Ook lijkt er binnen de ambtelijke organisatie onbekendheid te bestaan over welke incidenten aan wie en op welke wijze gemeld moeten worden.

Aanbeveling Blijf inzetten op een proces van bewustwording en bekwaamheid ten aanzien van informatiebeveiliging en privacy dat verder gaat dan vrijblijvend informeren en betrek ook college en raad hierin. Zorg op alle niveaus binnen de organisatie dat medewerkers zich daadwerkelijk verantwoordelijk gaan voelen voor de informatieveiligheid.

Aanbeveling Zorg dat alle medewerkers de benodigde kennis hebben over welke informatieveiligheidsincidenten gemeld moeten worden, aan wie en op welke manier.

Conclusie 7

De gemeenteraad wordt op verschillende manieren geïnformeerd over informatieveiligheid waarmee hij in staat wordt gesteld zijn kaderstellende en controlerende functie uit te oefenen. Wel kan de raad hierin beter gefaciliteerd worden door het aanleveren van toegankelijker informatie. Ook kan de raad zelf zijn rol op dit gebied actiever oppakken.

Aanbeveling Stel als raad vast of u voldoende informatie ontvangt over de verschillende aspecten van het informatiebeveiligings- en privacybeleid, welke informatie u eventueel verder nodig acht over informatiebeveiliging en privacybescherming, op welke strategische punten en op welke momenten de raad een verantwoordingsverslag wenst te hebben en bespreken en welke documenten de raad zelf wenst vast te stellen.

Aanbeveling Spreek als raad af welke kaders en eventuele leertrajecten de gemeenteraad zelf nodig heeft om veilig en bewust om te gaan met informatie(systemen) en welke informatie de raad hiertoe nodig heeft.

Bronnen

Rapportages

Vereniging van Nederlandse Gemeenten, *Eindverslag visitatiecommissie Informatieveiligheid 'Durven leren'*, Den Haag: VNG, september 2017.

Vereniging van Nederlandse Gemeenten, *Resolutie Informatieveiligheid, randvoorwaarde voor de professionele gemeente*, 2013.

Informatiebeveiligingsdienst, *Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten*, Den Haag: IBD, 2018.

Beleidsdocumenten gemeente Súdwest-Fryslân

- Achter de cyberdijken van de gemeente Súdwest-Fryslân. Strategisch Informatieveiligheidsbeleid 2018-2020, februari 2018.
- Implementatieplan Informatiebeveiliging 2016-2017, november 2016.
- Jaarverslag 2017
- Privacybeleid gemeente Súdwest-Fryslân 2018-2020, april 2018.
- Programmabegroting 2018
- Risico-inventarisatie en evaluatie informatieveiligheid (BRP en Waardedocumenten), november 2017.

Bijlage I Respondenten

Datum	Naam	Functie
6-4-2018 *Startgesprek*	Pieter Zondervan Jelle Jan Burggraaff Carla Aden	Gemeentesecretaris CISO FG
21-9-2018	Erik Faber Pieter Zondervan	Portefeuillehouder Gemeentesecretaris
21-9-2018	Laura de Graaf	CISO
21-9-2018	Carla Aden	FG
11-10-2018	Grietsje Stegenga	Griffier
1-11-2018	Inge Jongejeugd	Kwaliteitsmedewerker TIC
1-11-2018	Ellen Both	Teammanager gebiedsteam Sneek-Noord

Bijlage II Rollen, taken en verantwoordelijkheden

	Informatieveiligheidsbeleid	**Privacybeleid**
College van B&W	• Het college van B&W stelt formeel het informatieveiligheidsbeleid vast, delegeert de uitvoering hiervan aan de directie en legt hierover verantwoording af aan de gemeenteraad door middel van ENSIA. • Binnen het college van B&W valt informatiebeveiliging onder de portefeuille van een van de portefeuillehouders.	• Het college van B&W is verantwoordelijk voor de verwerking van persoonsgegevens zoals bedoeld in de AVG. Het college van B&W stelt formeel het privacybeleid vast, delegeert de uitvoering hiervan aan de directie en legt hierover verantwoording af aan de gemeenteraad. • Binnen het college van B&W valt de bescherming van persoonsgegevens onder de portefeuille van een van de portefeuillehouders. • Het college van B&W stelt het beleid vast en doet de gemeenteraad voorstellen over in te zetten middelen (budget) en stelt specifieke regelingen en procedures vast. • Het college van B&W legt periodiek (1 x per jaar) verantwoording af aan de gemeenteraad over het gevoerde privacybeleid.
Gemeenteraad	Niet beschreven	• De gemeenteraad controleert het college van B&W op de uitvoering van de privacyregelgeving en het privacybeleid. De gemeenteraad wordt daartoe in staat gesteld door de verantwoordingsinformatie die het college van B&W jaarlijks verschaft.
Directie	• De directie is ambtelijk verantwoordelijk voor de beveiliging van informatie en de daarbij behorende algemene sturing. De directie adviseert het college van B&W formeel over het vast te stellen beleid. • De directie stuurt de organisatie aan op beveiligingsrisico's, controleert of de getroffen maatregelen overeenstemmen met de beveiligingseisen en of deze voldoende bescherming bieden en evalueert periodiek beleidskaders en stelt waar nodig bij. • De directie geeft sturing aan de uitvoering van het informatieveiligheidsbeleid en ziet erop toe dat naleving van dit beleid plaatsvindt. De taken die hieruit voortvloeien zijn belegd bij de CISO.	• De directie en teammanagers zijn verantwoordelijk voor de inrichting van de verdere privacyorganisatie. • Zij zijn naar de organisatie en medewerkers kaderstellend, sturend en monitoren de uitvoering van de privacyregelgeving en het beleid. • De directie en teammanagers gezamenlijk stimuleren kennisvergaring en de bewustwording van de medewerkers. Zij voorzien in faciliteiten voor bewustwording en training. • De teammanagers zijn eindverantwoordelijk voor het melden van beveiligingsincidenten en/of datalekken bij de Servicedesk, de CISO en de FG

	• Binnen de directie is de Concerncontroller belast met informatieveiligheid en namens de directie het aanspreekpunt voor de CISO. Controlerende taken op het gebied van informatiebeveiliging liggen zoveel mogelijk bij de Concerncontroller.	
Lijnmanagement/ Teammanagers	• Het (lijn)management is operationeel verantwoordelijk voor de integrale beveiliging van de organisatieonderdelen. • Het lijnmanagement stelt op basis van een expliciete risicoafweging beveiligingseisen vast volgens de classificatie voor zijn informatiesystemen, is verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit deze eisen, stuurt op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en bewustzijn) en meldt incidenten en rapporteert in hoeverre hun organisatieonderdeel compliance is aan het informatieveiligheidsbeleid van de gemeente Súdwest-Fryslân.	
Chief Information Security Officer (CISO)	• De CISO heeft een faciliterende en coördinerende rol en zorgt ervoor dat uitvoerende taken zoveel mogelijk belegd zijn bij het lijnmanagement. • De CISO organiseert tenminste tweemaal per jaar een overleg met de BAC. Tevens vindt er periodiek overleg plaats tussen de CISO en de BAC over de stand van zaken en nieuwe ontwikkelingen op het gebied van informatiebeveiliging. De resultaten hiervan neemt de CISO mee in zijn evaluatie. Hiernaast vindt er elk jaar een organisatiebrede risicoanalyse plaats. Het college van B&W ontvangt hiervan een rapportage.	• De CISO houdt toezicht op de informatiebeveiliging. Hij of zij ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de informatieveiligheid. • De CISO bewaakt de voortgang van aanbevelingen uit audits en andere onderzoeken en adviseert over het te voeren beleid. • Hij of zij is het centrale aanspreekpunt voor informatiebeveiliging en maakt, indien nodig, gebruik van het escalatiepad direct naar de directie. • De CISO organiseert tenminste tweemaal per jaar een overleg met de BAC.
Functionaris voor de Gegevensbescherming (FG)	Niet beschreven	• De FG is het aanspreekpunt voor de Autoriteit Persoonsgegevens en houdt intern toezicht op de naleving van de privacywetgeving en op het uitvoeren van het privacybeleid. • Taken en bevoegdheden van de FG op basis van de AVG: - informeert, signaleert en adviseert over de

		verplichtingen die de organisatie heeft met betrekking tot de bescherming van persoonsgegevens - ziet toe op de naleving van wet- en regelgeving en het beleid met betrekking tot de bescherming van persoonsgegevens - werkt samen met en treedt op als contactpersoon voor de Autoriteit Persoonsgegevens - geeft desgevraagd advies met betrekking tot de gegevensbeschermingseffect-beoordeling (PIA) en ziet toe op de uitvoering daarvan in overeenstemming met artikel 35 AVG
Teams/medewerkers	De teams Facilitair, ICT, HR en Informatievoorziening (bedrijfsvoering) zijn verantwoordelijk voor de uitvoering van: - de beveiliging van de informatievoorziening en implementatie van beveiligingsmaatregelen die voortvloeien uit de beveiligingseisen en bijbehorende risicoanalyse - alle beheeraspecten van informatiebeveiliging die betrekking hebben op ICT-aangelegenheden - maatregelen gericht op beveiliging van personeel - maatregelen gericht op beveiliging van gebouwen, publieke en werkruimte van de gemeente - activiteiten die gericht zijn op het inrichten en beheren van een ISMS	Alle medewerkers (inclusief inhuur/externen) zijn verantwoordelijk voor de bescherming van de privacy van betrokkenen. Dat betekent dat iedereen zorgt draagt voor een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens.
Beveiligingsadviescommissie (BAC)	• Belangrijke organisatieonderdelen hebben minimaal één aanspreekpunt voor de CISO. Hiervoor heeft de gemeente Súdwest-Fryslân een BAC ingesteld. • Het overleg heeft binnen de gemeente een adviesfunctie en richt zich met name op beleid en adviseert over informatiebeveiligingskwesties.	• Belangrijke organisatieonderdelen hebben minimaal één aanspreekpunt voor de FG. Hiervoor heeft de gemeente Súdwest-Fryslân een BAC ingesteld. • Het overleg heeft binnen de gemeente een adviesfunctie en richt zich met name op beleid en adviseert over privacy en informatiebeveiligingskwesties.
Werkgroep privacy	Niet beschreven	• Vanuit het sociaal domein is in 2015 de werkgroep privacy opgericht die zich met privacy binnen het sociaal domein

		bezighoudt. • De werkgroep is inmiddels uitgebreid met vertegenwoordiging van Burgerzaken en zal in 2018 uiteindelijk een gemeentebrede werkgroep worden. • Deze werkgroep organiseert de zaken die vanuit de AVG praktisch geregeld moeten worden en brengt deze tot uitvoering.

Bijlage III Bestuurlijke reactie

De reactie van het college van burgemeester en wethouders van de gemeente Súdwest-Fryslân op het rapport "Zoeken naar de pragmatische grens Informatieveiligheid in de gemeente Súdwest-Fryslân" van de rekenkamer van Súdwest-Fryslân.

	Rapport Rekenkamer	**Reactie college van burgemeester en wethouders.**
	Conclusies/Aanbevelingen	
1.	Conclusie De gemeente Súdwest-Fryslân beschikt over een actueel strategisch informatieveiligheidsbeleid en privacybeleid waarin onder meer visie, uitgangspunten, maatregelen en taken en verantwoordelijkheden zijn beschreven.	Mee eens. Uit onze recente zelfevaluatie BRP en ENSIA 2018 en de jaarlijkse evaluatie informatiebeleid en beveiligingsplan team Burgerzaken blijkt opnieuw dat onze plannen actueel en effectief zijn.
2.	Conclusie De informatiebeveiligingsfunctie is zichtbaar belegd binnen de gemeentelijke organisatie. Er is een nauwe samen-werking rond de thema's informatie-beveiliging en privacy met een duidelijke verdeling van verantwoordelijkheden.	Mee eens.
3.	Conclusie De gemeente Súdwest-Fryslân heeft de uitgangspunten voor het beheer, gebruik en de uitwisseling van (persoons) gegevens deels beschreven en vast-gesteld. De uitwerking van de kaders voor de uitwisseling van persoonsgegevens met ketenpartners, de autorisaties van medewerkers voor gemeentelijke systemen en het invoeren van het verwerkingsregister behoeven nadere uitwerking. Aanbeveling Zorg, mede in het licht van de vereisten die met de AVG aan gemeenten worden gesteld, dat de kaders voor de uitwisseling van persoonsgegevens met ketenpartners en de autorisaties van medewerkers voor gemeentelijke systemen worden uitgewerkt en vastgelegd en dat het verwerkingsregister op korte termijn wordt ingevoerd.	Conclusie Mee eens. Aanbeveling Het college neemt de aanbeveling over. Het verwerkingenregister is per 1 april 2019 gereed. De uitwisseling met ketenpartners is inmiddels opgepakt .

4.	Conclusie Informatiebeveiligingsmaatregelen en privacywet- en regelgeving maken de dienstverlening gecompliceerder en leiden tot extra administratieve lasten, zo is nu nog de ervaring in de uitvoeringspraktijk. Desondanks lijkt de gemeente de balans te vinden tussen informatiebeveiliging en privacy enerzijds en een kwalitatief goede dienstverlening aan haar inwoners anderzijds. Binnen de gemeente bestaat een pragmatische houding ten aanzien van informatiebeveiliging en privacy. Dit is begrijpelijk vanuit het oogpunt van de dienstverlening aan inwoners, maar kan in de uitvoeringspraktijk risico's met zich meebrengen wanneer die pragmatische houding niet wordt vertaald van beleidsafspraken naar een eenduidige werkwijze in de uitvoering. Aanbeveling (1) Zorg ervoor dat de uitgangspunten en regels ten aanzien van informatiebeveiliging en privacybescherming van inwoners niet worden ondermijnd door een te pragmatische werkwijze in de uitvoering. (2) Zorg dat de CISO en de FG zowel in financieel als functioneel opzicht effectieve doorzettingsmacht hebben inzake de toepassing en naleving van de afspraken over informatiebeveiliging en privacybescherming.	Conclusie Mee eens. Aanbeveling (1) Het college neemt de aanbeveling over. De balans tussen informatiebeveiliging en privacy enerzijds en een kwalitatief goede dienstverlening aan de inwoners anderzijds is essentieel. Daarom wordt in de bewustwordingscampagne ook benadrukt dat informatiebeveiliging en privacy een kwaliteitsaspect van onze dienstverlening zijn en daarom een goede dienstverlening niet in de weg staan. (2) Het college neemt de aanbeveling over. CISO en FG hebben maximale functionele doorzettingsmacht door rechtstreekse communicatie- en escalatielijnen met directie en bestuur. Door nog betere inbedding in veranderprocessen willen wij de effectiviteit verder verhogen. CISO en FG worden in de huidige situatie financieel volledig gefaciliteerd. De budgetverantwoordelijkheid bij CISO en FG neer leggen leidt daarmee alleen op papier tot meer onafhankelijkheid. Dit betekent dat CISO en FG ook financiële verantwoording moeten afleggen terwijl ze zich nu volledig op hun kerntaak kunnen richten.
5.	Conclusie De gemeente Súdwest-Frsylân probeert op actieve wijze inzicht te krijgen in de risico's voor de informatieveiligheid in de gemeente en lijkt hierin te slagen. Deze inzichten worden vervolgens vertaald naar maatregelen die echter niet (altijd) effectief blijken, in het bijzonder waar het gaat om het informatiebewustzijn van de betrokkenen. Aanbeveling Laat tenminste één maal per jaar de gemeentelijke informatiebeveiliging door een externe partij testen op kwetsbaarheden, neem dit op in de P&C-cyclus en handel naar de bevindingen.	Conclusie Niet mee eens. Het "informatiebewustzijn van betrokkenen" veranderen heeft tijd nodig. Het feit dat nog lang niet iedereen in elke situatie altijd even alert is, wil niet zeggen dat de maatregelen ter bevordering van het veiligheidsbewustzijn niet effectief zijn. Wij zien juist grote verbeteringen in de alertheid. Echter dit onderwerp vraagt steeds om herhaling en periodieke training net als bij fysieke veiligheid. Ook moeten we ons realiseren dat mensen fouten maken en daarom een 100% score lang niet altijd gehaald zal worden. Aanbeveling Het college neemt de aanbeveling niet over.

		De gemeente wordt al op verschillende manieren onderzocht over het voldoen aan de informatiebeveiligingseisen. Zo doet de accountant onderzoek en legt de gemeente via Ensia verantwoording af. Ensia is juist een methode om de belasting door allerlei onderzoeken door standaardisatie terug te brengen. Meer onderzoeken zijn daarom een tegenstrijdige beweging. Ze bevorderen ook niet het "informatiebewustzijn van betrokkenen".
6.	Conclusie De gemeente benoemt het informatiebewustzijn van de medewerkers als risico voor de informatieveiligheid en heeft hier de afgelopen jaren aandacht aan besteed. Er is onvoldoende aandacht geweest voor het informatiebewustzijn van de leden van het college van B&W en de gemeenteraad. Een belangrijk deel van de in dit onderzoek gevonden kwetsbaarheden is terug te voeren op het informatiebewustzijn, het gedrag en de betrokkenheid van ambtelijke organisatie, raad en college. Ook lijkt er binnen de ambtelijke organisatie onbekendheid te bestaan over welke incidenten aan wie en op welke wijze gemeld moeten worden. Aanbeveling (1) Blijf inzetten op een proces van bewustwording en bekwaamheid ten aanzien van informatiebeveiliging en privacy dat verder gaat dan vrijblijvend informeren en betrek ook college en raad hierin. Zorg op alle niveaus binnen de organisatie dat medewerkers zich daadwerkelijk verantwoordelijk gaan voelen voor de informatieveiligheid. (2) Zorg dat alle medewerkers de benodigde kennis hebben over welke informatieveiligheidsincidenten gemeld moeten worden, aan wie en op welke manier.	Conclusie Mee eens. De gemeente zet de afgelopen jaren continu in op bewustwording. In 2018 is het nieuwe IPI-traject (informatieveiligheid, privacy en integriteit) van start gegaan om het bewustzijn te verhogen. Dit traject loopt de komende jaren door. Hiervoor is ook het bestuur uitgenodigd. Verder is in 2018 dertig keer voorlichting gegeven door de FG aan de teams over privacy en de Algemene Verordening Gegevensbescherming (AVG). Ook voor 2019 zijn sessies gepland. Aanbeveling (1) Het college neemt de aanbeveling over. (2) Het college neemt de aanbeveling over..
7.	Conclusie De gemeenteraad wordt op verschillende manieren geïnformeerd over informatieveiligheid waarmee hij in staat wordt gesteld zijn kaderstellende en	Conclusie Mee eens. Aanbeveling (1) Deze aanbeveling krijgt vorm door dat de

	controlerende functie uit te oefenen. Wel kan de raad hierin beter gefaciliteerd worden door het aanleveren van toegankelijker informatie. Ook kan de raad zelf zijn rol op dit gebied actiever oppakken. <u>Aanbeveling</u> (1)Stel als raad vast of u voldoende informatie ontvangt over de verschillende aspecten van het informatiebeveiligings- en privacybeleid, welke informatie u eventueel verder nodig acht over informatiebeveiliging en privacybescherming, op welke strategische punten en op welke momenten de raad een verantwoordings-verslag wenst te hebben en bespreken en welke documenten de raad zelf wenst vast te stellen. (2)Spreek als raad af welke kaders en eventuele leertrajecten de gemeenteraad zelf nodig heeft om veilig en bewust om te gaan met informatie(systemen) en welke informatie de raad hiertoe nodig heeft.	Nederlandse gemeenten besloten hebben om vanaf 2017 het onderzoek op informatie-veiligheid te standaardiseren. Hiervoor is Ensia bedacht. Ensia is bedoeld om te voorkomen dat allerlei aparte onderzoeken en audits m.b.t. informatieveiligheid gedaan worden. De rapportage van Ensia gaat een keer per jaar als actieve informatie met de collegeverklaring naar de gemeenteraad. Aan de volgende gestandaardiseerde Ensia rapportage wordt een vertaling in begrijpelijke taal toegevoegd. De rapportage m.b.t. privacy wordt aan het jaarverslag van de gemeente toegevoegd en vanaf 2020 uitgebreid met een apart rapportage over privacy. (2) FG en CISO ondersteunen hier graag in en bieden aan een informatieve sessie voor de raad te geven over de onderwerpen.

Bijlage IV Nawoord rekenkamer

De rekenkamer constateert dat het college met instemming heeft kennisgenomen van haar bevindingen ten aanzien van de informatieveiligheid in de gemeente Súdwest-Fryslân. Wij zijn verheugd dat de aanbevelingen die wij in ons rapport hebben gedaan grotendeels worden overgenomen door het college, waarbij verschillende aanbevelingen reeds in gang zijn gezet.

Het is goed om te horen dat het verbeteren van het informatiebewustzijn binnen de gemeente Súdwest-Frsylân, het belangrijkste aandachtspunt dat uit ons onderzoek naar voren kwam, de aandacht blijft houden en gemeentebreed wordt opgepakt. Informatiebewustzijn moet er tenslotte niet alleen zijn bij de ambtelijke organisatie, maar ook bij de raad en het college.

Ook in dit onderzoek heeft de rekenkamer de medewerking vanuit de ambtelijke organisatie als zeer prettig ervaren, waarvoor wij onze dank uitspreken. Wij hopen met ons onderzoek een bijdrage te leveren aan het verbeteren van de informatieveiligheid in de gemeente Súdwest-Fryslân en zullen de verdere ontwikkelingen met betrekking tot dit onderwerp met belangstelling blijven volgen.

Drs. J.H. Lepage MPA

Voorzitter Rekenkamer Súdwest-Frsylân