Onderzoek informatieveiligheid en privacy

Gemeente Roosendaal

Eindrapportage

Februari 2019

Postbus 5000
4700 KA ROOSENDAAL

www.rekenkamerwestbrabant.nl

Inhoudsopgave

1. Inleiding en doel onderzoek

Toenemend belang digitale dienstverlening

Gemeenten investeren steeds meer in digitale dienstverlening, apps, portals en andere manieren om diensten te verlenen en met hun doelgroepen in contact te komen. Gemeenten worden daardoor steeds afhankelijker van een ongestoorde werking van hun ICT-voorziening om klanten/burgers goed en tijdig van dienst te kunnen zijn. Klanten en burgers verwachten op hun beurt een '24/7' beschikbaarheid van de digitale dienstverlening, gaan ervanuit dat de gegevens die zij daarbij verstrekken in veilige handen zijn én dat de gegevens altijd actueel, betrouwbaar en correct zijn. Gemeenten werken steeds meer samen in informatieketens (bijvoorbeeld in het sociaal domein/decentralisaties) en met ketenpartners, die op hun beurt ook eisen stellen aan de beveiliging van informatie. Wanneer ICT-voorzieningen uitvallen en/of data (onbedoeld) in verkeerde handen komen, leidt dat mogelijk tot financiële en imagoschade en een boete van de toezichthouder.

Informatiebeveiliging & Privacy

Vanuit wetgeving en overheidsbrede afspraken worden behoorlijke eisen gesteld aan de informatiebeveiliging en bescherming van persoonsgegevens in handen van gemeenten. Denk daarbij bijvoorbeeld aan eisen die gesteld worden aan de verwerking van persoonsgegevens vanuit de Wet Basisregistratie Personen (Wet BRP), de aansluitvoorwaarden DigiD en de door het forum Standaardisatie opgestelde 'Pas-toe-of-Leg-uit'-lijst met beveiligingsstandaarden[1].

Met het recentelijk goedkeuren door het Europees Parlement van de Europese Verordening 2016/679, beter bekend als de Algemene Verordening Gegevensbescherming (AVG), moet elke organisatie ervoor zorgen dat zij aan de AVG voldoet per 25 mei 2018. De AVG regelt onder meer de transparantie van de verwerking van persoonsgegevens, het (verplicht) aanstellen van een data protection officer/functionaris gegevensbescherming, het voldoen aan minimum inhoudelijk vereisten voor de verwerkersovereenkomst - anders loopt het bedrijf een risico op boete -, het recht om vergeten te worden, de verplichting tot gegevensbescherming bij het ontwerpen van producten en diensten (privacy by design) en het uitvoeren van een Data Protection Impact Assessment (DPIA)[2]. Als voorloper op de AVG is reeds de meldplicht datalekken in de Nederlandse wet opgenomen sinds 1 januari 2016. Bij een datalek is er sprake van verlies of onrechtmatige verwerking van persoonsgegevens en moet de verantwoordelijke een melding doen bij de Autoriteit Persoonsgegevens en de betrokkenen informeren.

[1] Door het forum worden verschillende standaarden op het gebied van veiligheid verplicht gesteld, zoals bijvoorbeeld NEN-ISO/IEC 27002. Zie voor meer informatie: https://www.forumstandaardisatie.nl/lijst-open-standaarden/in_lijst/verplicht-pas-toe-leg-uit

[2] Een DPIA is een instrument waarmee organisaties voorafgaand aan een gegevensverwerking de privacyrisico's daarvan in kaart kunnen brengen door met name de oorsprong, de aard, het specifieke karakter en de ernst van de privacyrisico's te evalueren. Vervolgens kunnen, indien nodig, maatregelen worden getroffen om de privacyrisico's te verkleinen. Zie: https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia.

Het onderwerp databeveiliging, in andere terminologie ook wel informatieveiligheid, heeft in toenemende mate aandacht van de gemeente Roosendaal. Ook op bestuurlijk niveau. Zo werd de gemeenteraad getriggerd door berichten van VNG over cybercrime en datalekken bij andere gemeenten. De gemeenteraad vraagt zich af hoe de gemeente op dit onderwerp ervoor staat. Om die reden heeft de gemeenteraad van Roosendaal, specifiek de auditcommissie, het onderwerp als onderzoeksthema aangemerkt en de Rekenkamer West-Brabant gevraagd dit onderzoek uit te laten voeren.

Deze rapportage bestaat uit een beschrijving van de onderzoeksvragen, een beschrijving van de onderzoekaanpak, een terugkoppeling van bevindingen en conclusies en aanbevelingen.

2. Onderzoeksvragen

Het onderwerp informatieveiligheid en privacy is onderzocht op een tweetal sporen:

1. De ambtelijke organisatie en wettelijke kaders

2. De bestuurlijke context en wisselwerking daarbinnen

Binnen de twee sporen stonden de volgende onderzoeksvragen centraal:

Spoor 1: De ambtelijke organisatie en wettelijke kaders

1. Bewustzijn informatieveiligheid op de werkvloer
Hoe is het gesteld met het bewustzijn ten aanzien van informatieveiligheid en privacy in de ambtelijke organisatie van gemeente Roosendaal?

2. Kaders en wettelijke verplichtingen
Geeft de gemeente Roosendaal vorm en inhoud aan het informatieveiligheidsbeleid en wettelijke kaders? En zo ja, hoe gebeurt dat?

3. Risico's
Heeft de gemeente in brede zin een goed beeld van de belangrijkste risico's op het gebied van de informatiebeveiliging en in het bijzonder de bescherming van de persoonsgegevens?

Spoor 2: De bestuurlijke context en wisselwerking daarbinnen

4. Wisselwerking
Hoe is de communicatie/afstemming/sturing met betrekking tot het informatieveiligheidsbeleid tussen het college en de ambtelijke organisatie?

5. Kaderstelling
Hoe is/wordt aan de kaderstellende en controlerende rol van de gemeenteraad met betrekking tot de informatieveiligheid vorm en inhoud gegeven?

3. Onderzoekaanpak

In dit hoofdstuk wordt de onderzoekaanpak nader geduid. Per spoor is duidelijk gemaakt welke stappen zijn ondernomen.

3.1. Spoor 1: De ambtelijke organisatie en wettelijke kaders

Zoals beschreven in de inleiding stelt de overheid wettelijke eisen en verplichtingen aan informatiebeveiliging en bescherming van persoonsgegevens bij gemeenten.
Sinds enkele jaren zijn 'best practices' op het gebied van informatiebeveiliging beschreven in internationaal erkende NEN-normen (ISO 27001). Binnen de overheid zijn deze vertaald en wordt er gewerkt met een voor gemeenten specifiek gemaakte Baseline Informatiebeveiliging Gemeenten (BIG). In deze best practices zijn voldoende handreikingen te vinden die helpen bij het treffen van maatregelen om de organisatie rond informatiebeveiliging en privacy in te richten. In elf hoofdstukken van de BIG[3] (vanaf hoofdstuk 5 t/m 15) zijn de belangrijkste maatregelen beschreven die een gemeente moet treffen om aan de BIG te voldoen.

Verschillende onderzoeksmethoden zijn toegepast om de vraagstelling vanuit meerdere invalshoeken te onderzoeken. Ten eerste is een documentenstudie uitgevoerd. Verschillende documenten (zie bijlage 1) zijn verzameld en bestudeerd. Hiermee is een eerste beeld verkregen van de kaders, de wettelijke verplichtingen en de risico's. Ten tweede is de QuickScan BIG ingezet om de papieren werkelijkheid met de praktijk te kunnen vergelijken. De QuickScan BIG is door het advies- en onderzoeksbureau Berenschot ontwikkeld en sluit goed aan bij de vragen die in spoor 1 relevant zijn. De QuickScan besteedt aandacht aan alle relevante hoofdstukken van de BIG, zoals in figuur 1 weergegeven. De hoofdstukken variëren met de klok mee van 'Beleid' tot 'Naleving'.

Figuur 1. Het framework van de QuickScan BIG

[3] https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2016/07/Tactische-Baseline-Informatiebeveiliging-Nederlandse-Gemeenten-v1.02.pdf

Deze QuickScan bestaat uit een vragenlijst die is afgenomen tijdens een interviewronde. In de interviewronde is gesproken met een aantal sleutelfiguren binnen de ambtelijke organisatie.
Door het gestructureerd doorlopen van een vragenlijst met betrokkenen uit de ambtelijke organisatie is een beeld verkregen van de huidige positie van de gemeente Roosendaal op de verschillende sub-thema's van de BIG. De vragenlijst bevat per hoofdstuk van de BIG alle elementen die de BIG voorschrijft. Aan de hand van de BIG-elementen is getoetst in welke mate de gemeente Roosendaal voldoet aan de criteria die de BIG voorschrijft. De vragenlijst bestaat uit gesloten vragen, die beantwoord zijn met ja of nee.

Op het thema 'organisatie' bevat de BIG bijvoorbeeld 10 richtlijnen voor gemeenten. Als de gemeente aan zes van de tien richtlijnen voldoet, dan zal ze een 3 (op een schaal van 0 tot 5) scoren op dit thema. De uitkomsten zijn geplot op een radardiagram en dienen daarmee als nulmeting, het vertrekpunt. In deze rapportage is vervolgens per relevant hoofdstuk uit de BIG beschreven op basis van welke argumenten de score tot stand is gekomen. De Quickscan brengt kwaliteiten, kwetsbaarheden en kansen voor verbetering van de informatiebeveiliging voor de gemeente Roosendaal boven water. Specifiek is er ook aandacht geweest voor het thema bewustzijn van medewerkers. Hier zijn concrete vragen over gesteld met betrekking tot gedragsvoorbeelden. Voorbeelden hiervan zijn: hoe gaan medewerkers om met onbekende e-mail, hoe gaan medewerkers om met gegevensdragers (zoals usb-sticks), worden computers vergrendeld bij afwezigheid, spreekt men elkaar aan indien men ongewenst gedrag ziet, weet men hoe te handelen bij incidenten, etc. Dit is meegenomen in deze rapportage in de hoofdstukken van de BIG die hier over gaan, zoals het hoofdstuk over naleving.

Buiten scope
Een gedetailleerde audit of tests naar de werking van de diverse informatieveiligheidsmaatregelen in de praktijk van de gemeente vielen buiten de scope van dit onderzoek. Zo zijn bijvoorbeeld geen penetratietesten[4] uitgevoerd en is het gedrag van medewerkers op de werkvloer niet onderzocht. Wel is waar mogelijk naar de werking gekeken door bijvoorbeeld mee te kijken in ICT-systemen en door te vragen naar concrete gedragsvoorbeelden.

3.2. Spoor 2: Verantwoording en wisselwerking

Voor een succesvolle kaderstelling en controle is het noodzakelijk dat de randvoorwaarden op orde zijn. Deze randvoorwaarden zijn deels vastgelegd in wetgeving (verordenende bevoegdheid, begrotingsrecht, budgetrecht) maar deels zijn gemeenteraden en colleges ook zelf verantwoordelijk voor het scheppen van deze kaders. De kaders dienen betrekking te hebben op prioritering (waarover wil de raad kaders stellen?), de spelregels waarbinnen het proces van kaderstelling kan plaatsvinden (duidelijkheid en consensus over rolinvulling en verantwoordelijkheden van raad, college, ambtelijke organisatie en verbonden partij) en een adequate

[4] Een penetratietest is een toets van een of meer computersystemen op kwetsbaarheden, waarbij deze kwetsbaarheden ook werkelijk gebruikt worden om in deze systemen in te breken. Een penetratietest heeft als doel de systemen juist beter te beveiligen.

informatievoorziening naar de raad (een goed geïnformeerde raad is in positie om actief invloed uit te oefenen op beleid).

Voor spoor 2 is aandacht besteed aan:

1. De wisselwerking tussen de raad en college van B&W

    a. In welke mate vindt expliciet verantwoording plaats over informatieveiligheid en privacy aan de gemeenteraad?

    b. Is de gemeenteraad in staat om te beoordelen of de informatieveiligheid en privacy binnen gemeente Roosendaal op orde is? Hiervoor is van belang dat de gemeenteraad op het juiste moment over voldoende informatie beschikt en hij voldoende kennis heeft over informatieveiligheid om de informatie te kunnen beoordelen.

2. De kaderstelling en controle door de gemeenteraad
   Hoe worden zowel de kaderstellende rol als controlerende rol door de gemeenteraad voor informatieveiligheid en privacy ingevuld?

De aanpak tijdens dit spoor bestond uit een documentenstudie, en interviewronde en een interactieve sessie. Eerst zijn voor de documentstudie diverse zowel publiek beschikbare verslagen als interne verslagen bestudeerd. In bijlage 1 is een complete lijst van bestudeerde documenten opgenomen. Na de documentstudie zijn de algemeen directeur en een portefeuillehouder gesproken in een interviewronde. Tot slot heeft een interactieve sessie met de auditcommissie plaatsgevonden. Middels deze sessie is een beeld verkregen vanuit het perspectief van de gemeenteraad over de rol van de gemeenteraad, de wisselwerking en verslaglegging tussen gemeenteraad, de ambtelijke organisatie en het college van B&W en het kennisniveau van de raadsleden. Het doel van deze sessie was om de rolverdeling tussen de gemeenteraad, de ambtelijke organisatie en het college van B&W in kaart te brengen, met een focus op de wisselwerking en verantwoording onderling.

3.3. Overzicht

De combinatie van spoor 1 en spoor 2 inclusief de spooroverstijgende activiteiten zoals hoor en wederhoor maakt de onderzoekaanpak als volgt:

Activiteiten		**Spoor 1: De ambtelijke organisatie en wettelijke kaders *'QuickScan en bewustzijn'***	**Spoor 2: De bestuurslaag *'Verantwoording en wisselwerking'***
1. Kick-off		x	x
2. Documentstudie		x	x
3. Interviewronde	3a. CISO	x	
	3b. Informatiemanager	x	
	3c. Concerncontroller	x	
	3d. Portefeuillehouder college B&W	x	x
	3e. Algemeen directeur	x	x
4. Interactieve sessie met de Raad			x
5. Ambtelijk hoor en wederhoor		x	
6. Bestuurlijk hoor en wederhoor		x	x
7. Terugkoppeling Rekenkamer West-Brabant		x	x

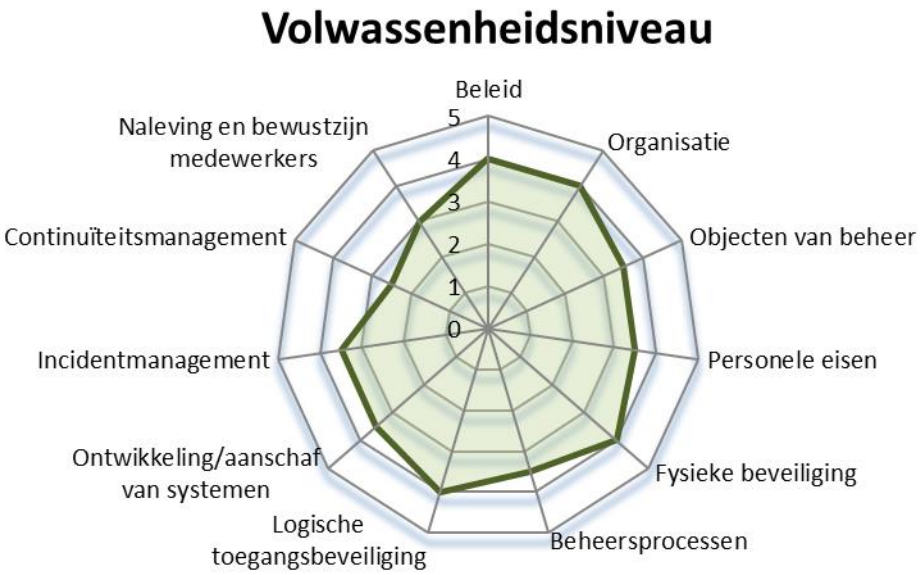
4. Bevindingen

4.1. Spoor 1: Ambtelijke organisatie

Het uitvoeren van de BIG-QuickScan binnen de ambtelijke organisatie heeft ons een beeld gegeven van de stand van zaken van verschillende onderwerpen uit de BIG. Deze paragraaf geeft per basisnorm de bevindingen weer, op basis van gesprekken met sleutelpersonen en de bestudeerde documentatie.

Hierbij is het goed om de context te schetsen van het informatiedomein van de gemeente Roosendaal. Het informatiedomein van de gemeente Roosendaal is (net als van andere gemeenten) complex. Deze complexiteit zit in de vele samenwerkingsverbanden die de gemeente heeft op verschillende vlakken. Zo werkt de gemeente op ICT-gebied bijvoorbeeld samen in een gemeenschappelijk regeling met vijf gemeenten, terwijl er op het sociale domein in het Werkplein West-Brabant wordt samengewerkt met vijf (deels andere) gemeenten. Dit betekent dus dat informatie van de gemeente op vele plekken in verschillende constructies vastgelegd wordt. Dit brengt qua governance en sturing uitdagingen met zich mee: uitdagingen die goed in beleid en werkprocessen verankerd dienen te zijn.

De BIG volwassenheidsscore op basis van de bevindingen uit spoor 1 (de resultaten van de QuickScan BIG) is weergegeven in het onderstaande radardiagram. In de paragrafen hierna wordt per hoofdstuk van de BIG toegelicht op welke feitelijke bevindingen deze score gebaseerd is.



Figuur 2. BIG volwassenheidsscore

4.1.1. Beleid

Wat betreft de basisnorm Beleid, worden in de QuickScan BIG vier van de vijf vragen beantwoord met een ja. Ten eerste blijkt dat een actueel informatieveiligheidsbeleid is vastgesteld voor de hele organisatie, in samenwerking met Bergen op Zoom, Etten-Leur, Moerdijk en Tholen, onder de naam ICT West-Brabant-West (ICT WBW). Hierin staat beschreven hoe ICT WBW (ofwel Gemeenschappelijke Regeling ICT, GR ICT WBW) werkt op het gebied van ICT. Het beleid is zo ingestoken dat er ruimte is om per gemeente te verschillen in governance. Dus onder een overkoepelende paraplu, leunend op veel expertise, is er een beleid, waarin ook ruimte is voor de lokale verschillen.

Ten tweede blijkt dat de gemeente Roosendaal een actueel informatiebeveiligingsplan onderhoudt voor de hele organisatie. Daarin zijn de prioriteiten geborgd en de posten voor de begroting opgenomen, zoals hardware en softwarekosten, de inrichting van het ISMS-systeem, en personele kosten voor de CISO of de FG. In lijn met de BIG is per beveiligingsmaatregel een eigenaar aangewezen die verantwoordelijk is voor de realisatie van die maatregel. Een voorbeeld hiervan is het Actieplan Informatieveiligheid 2017, waarin duidelijk omschreven wordt welke maatregelen er nog genomen dienen te worden door welke functionaris. Uit het interview met de CISO blijkt dat een aantal te nemen maatregelen die in dit actieplan informatieveiligheid 2017 worden aangekondigd ook daadwerkelijk gerealiseerd zijn of dat er nog acties lopende zijn.

Ten derde leidt het informatieveiligheidsbeleid tot het uitvoeren van een risicoanalyse op het gebied van informatieveiligheid. De risicoanalyse bestaat uit twee onderdelen:

1. De gapanalyse: Deze analyse is gestoeld op de BIG (vergelijkbaar met deze QuickScan BIG) en wordt in het 'Information Security Management System' (ISMS) bijgehouden. Deze risico's worden vervolgens geactualiseerd op het moment dat er een groot project of een grote wijziging optreedt. Dit gebeurt met diverse stakeholders uit de organisatie. In 2016 is deze analyse uitgevoerd door BMC. In 2018 heeft de ambtelijke organisatie deze analyse zelf uitgevoerd.
2. Risicoanalyse op basis van de MAPGOOD-methodiek[5]. Hiermee worden risico's voor de belangrijkste systemen en processen in kaart gebracht. In 2018 is deze risicoanalyse onder begeleiding van BMC uitgevoerd. In deze risicoanalyse worden niet alle systemen of processen meegenomen, zoals de BIG wel voorschrijft. Uit de gesprekken blijkt dat er prioriteiten toegekend zijn aan processen en systemen en ook is beschreven welke processen privacygevoelig zijn.

Daarnaast voert de gemeente Roosendaal jaarlijks (binnen de planning & control-cyclus ten behoeve van de begroting, bestuursrapportage en jaarrekening) een algemene risicoanalyse uit. Hierin worden met name financiële risico's gekapitaliseerd. Uit deze risico's wordt een top 10 geëxtraheerd die gedeeld wordt met het college. Deze top 10 kent doorgaans weinig informatiebeveiligingsrisico's (zoals het risico op

[5] MAPGOOD staat voor Mensen, Apparatuur, Programmatuur, Gegevens, Organisatie, Omgeving en Diensten. Dit zijn de verschillende invalshoeken om naar bedreigingen en risico's te kijken. Uitgangspunt van deze methode is dat risico's vanuit geselecteerde bedreigingen in relatieve vorm tot elkaar worden gewaardeerd. De geselecteerde bedreigingen voor informatieveiligheid zijn geselecteerd op basis van ervaringen uit andere gemeenten en op basis van ingeschakelde expertise. Aan deze bedreigingen is door de betrokkenen een risicowaardering toegekend. Vervolgens is beoordeeld welke risico's het zwaarst wegen en urgente beheersmaatregelen verdienen.

een datalek) omdat deze niet als grootste risico gezien worden door de gemeente. De maximale boete die men in het kader van de AVG opgelegd kan krijgen door de Autoriteit Persoonsgegevens (AP) bedraagt ongeveer 800.000 euro, waarmee deze boete niet in de top 10 komt. Andere schade die de gemeente door een datalek kan lijden is bijvoorbeeld imagoschade; deze is echter in de huidige planning & control risicoanalyse-methodiek niet te kapitaliseren. Daarnaast is er geen expliciete beleidsmatige verbinding tussen de twee vormen van risicoanalyse binnen de gemeenten. De 'algemene' (vanuit planning & control) risicoanalyse staat beleidsmatig los van de informatiebeveiligingsrisicoanalyse-methodiek, al zijn wel dezelfde functionarissen betrokken bij beide risicoanalyses.

4.1.2. Organisatie

Het hoofdstuk organisatie van de BIG gaat over of de verantwoordelijkheden op het gebied van informatieveiligheid duidelijk belegd zijn in de organisatie en of dit ook bij uitbestede informatiedienstverlening het geval is. Ook valt hier de sturing op incidenten onder.

Wat betreft de basisnorm organisatie worden voor gemeente Roosendaal in de QuickScan acht van de tien vragen beantwoord met een ja. Zo zijn in het kader van de organisatie van informatiebeveiliging en privacy verantwoordelijkheden expliciet gedefinieerd (in bijvoorbeeld het informatiebeveiligingsbeleid), is een Chief Information Security Officer (CISO) aangesteld met een duidelijke taakomschrijving en heeft ieder (privacygevoelig) informatiesysteem en iedere ICT-component een aangewezen eigenaar. Beveiligingsincidenten worden geregistreerd zoals voorgeschreven door de IBC. Dit gebeurt in Topdesk, een systeem waarin de GR-ICT alle incidenten bijhoudt en waar de gemeente Roosendaal toegang toe heeft. De onderzoekers hebben een lijst kunnen inzien van de geregistreerde incidenten in Topdesk. Hierbij valt op te merken dat dit alleen de digitale informatiebeveiligingsincidenten betreft; incidenten die betrekking hebben op het verlies van papieren informatie worden hier niet in geregistreerd. De IBC bewaakt de afhandeling van deze incidenten. Uit de gesprekken en documentstudie blijkt dat er echter geen stuurgroep is die rapportages over informatiebeveiligingsincidenten beoordeelt. De afhandeling van incidenten gebeurt situationeel; de CISO maakt een inschatting van het incident en besluit hoe er gehandeld moet worden en wie er bij betrokken moet worden. Wanneer het een datalek betreft, dan is er sprake van een stuurgroep in de vorm het kernteam privacy, waarin datalekken worden beoordeeld en een handelingsperspectief wordt opgesteld.

Bij uitbesteding van management en beheer van IT-voorzieningen zijn de beveiligingseisen niet vastgelegd in de betreffende Dienstverleningsovereenkomst (DVO) met de leverancier/beheerpartij. Omdat het hier niet een klassieke uitbesteding betreft (met leverancier-klant) maar een gemeenschappelijke regeling, zijn deze afspraken in het gezamenlijke informatiebeveiligingsbeleid vastgelegd en zijn nader uitgewerkt in de verwerkersoverkomst. Over de naleving hiervan wordt periodiek gerapporteerd. Ten aanzien van het uitbestede beheer is een opdracht verstrekt aan een onafhankelijke auditor voor het opleveren van een rapportage over opzet, bestaan en werking van getroffen beveiligingsmaatregelen. Ook zijn met interne ICT-

dienstverleners Service Level Agreements (SLA) afgesloten waarbij aandacht is besteed aan informatiebeveiliging.

Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke toegang (fysiek, netwerk of tot gegevens) de externe partij(en) moet(en) hebben om de in het contract overeengekomen opdracht uit te voeren en welke noodzakelijke beveiligingsmaatregelen hiervoor nodig zijn.

De rol van de portefeuillehouder en de algemeen directeur bij informatiebeveiliging en privacy is beperkt. Ze zijn uiteindelijk integraal verantwoordelijk voor het onderwerp, dat betekent toezien dat taken rondom informatieveiligheid uitgevoerd worden, en zich geregeld laten bijpraten over de actuele stand van zaken.

4.1.3. Objecten van beheer

Bij objecten van beheer gaat het over hoe de gemeente met bedrijfsmiddelen[6] en gegevens omgaat. Hierbij is het volgens de BIG bijvoorbeeld van belang dat je als organisatie een goed beeld hebt van welke middelen je gebruikt en dat je weet welke maatregelen je moet nemen om deze middelen goed te beschermen tegen oneigenlijk gebruik. De gemeente Roosendaal houdt een registratie bij van alle bedrijfsmiddelen die verband houden met informatiesystemen, zoals laptops en smartphones. Echter voor desktopvoorzieningen is de registratie minder actueel. Ook vereist de BIG dat gemeenten over een actueel documentair structuurplan (DSP) beschikken waarmee ze overzicht hebben van alle aanwezige informatie- en archiefbestanden van de organisatie in relatie tot de werkzaamheden. Gemeente Roosendaal beschikt over een actueel DSP. Aanvullend hierop gebruikt de gemeente een zaaktypecatalogus waarmee de gemeente ook op zaakniveau inzicht heeft op de aanwezige informatie. Met behulp van deze middelen heeft de gemeente haar informatie en de bedrijfsmiddelen geclassificeerd op de aspecten vertrouwelijkheid, betrouwbaarheid en beschikbaarheid.

Eind 2016 is door adviesbureau BMC onderzoek uitgevoerd naar de stand van zaken op gebied van privacy. Hierin wordt geconcludeerd dat het algemeen beeld is *dat de gemeente Roosendaal in administratief/juridisch opzicht op weg is naar een adequaat uitvoeringsniveau van de Wbp c.a., maar dat er ook nog werk ligt om dat niveau te bereiken.* Naar aanleiding van deze rapportage is de gemeente aan de slag gegaan met het uitvoeren van de geconstateerde gebreken. Voor een aantal van de aanbevelingen hebben onderzoekers kunnen constateren dat deze gerealiseerd zijn. Uit de interviews konden de onderzoekers afleiden dat de implementatie nog niet volledig voltooid is. Zo is de aanbeveling: "Een bewustwordingsproces privacy, zowel intern als extern in gang te zetten, te verbeteren en in stand te houden" nog niet volledig geïmplementeerd. De onderzoekers hebben daarnaast kunnen constateren dat de gemeente Roosendaal in een verwerkingsregister bijhoudt welke persoonsgegevens door wie gebruikt worden en heeft passende maatregelen getroffen in overeenstemming met de AVG voor de betreffende informatiesystemen. Er is een protocol voor datalekken. Tevens zijn er procedures vastgelegd rond verwerkingen

[6] Onder bedrijfsmiddelen worden goederen verstaan die gedurende een lange periode in een onderneming gebruikt worden zoals gebouwen, installaties of computers.

van persoonsgegevens, zoals een privacy-protocol. Deze zijn ook te vinden op de website van de gemeente Roosendaal[7].

4.1.4. Personele eisen

Het hoofdstuk personele eisen in de BIG doelt op het bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen en geschikt zijn voor de rollen waarvoor zij worden aangesteld. Verder heeft dit hoofdstuk als doel om het risico op diefstal, fraude of misbruik van faciliteiten te verminderen.

Bij de gemeente Roosendaal leggen nieuwe medewerkers bij indiensttreding een Verklaring Omtrent Gedrag (VOG) over en tekenen zij een integriteitscode. In het personeelsbeleid wordt niet ingegaan op tijdelijke medewerkers. Wel staat daar vermeld dat Ambtenarenwet 125a geldt en dat medewerkers die omgaan met bijzondere informatie een geheimhoudingsverklaring moeten tekenen. Door een medewerker van Personeel & Organisatie (P&O) wordt aangegeven dat dit ook daadwerkelijk gebeurt voor enkele specifieke functiegroepen, zoals ICT-medewerkers. Ook geeft P&O aan dat voor tijdelijke medewerker dezelfde eisen gelden. De gemeente onderscheidt twee groepen externe medewerkers: een groep die via externe partijen (intermediairs als uitzendbureaus, via Flex-Brabant) binnen komt en een groep die via de gemeente zelf binnen komt (zoals consultants, trainees en stagiaires). Voor de groep die rechtstreeks door de gemeente wordt ingezet, geldt dat niet standaard een geheimhoudingsverklaring ondertekend wordt, tenzij een medewerker daar expliciet om vraagt. Voor de groep die via Flex-Brabant wordt ingezet, geldt dat controles niet zelf worden uitgevoerd maar er wordt op externe partijen (zoals uitzendbureau, waarmee raamcontracten in Flex-Brabant verband zijn afgesloten) vertrouwd voor het uitvoeren hiervan. De gemeente Roosendaal houdt geen overzicht bij van de kwetsbare functies. Bij vervulling van een vacature voor een kwetsbare functie wordt een veiligheidsonderzoek uitgevoerd.

De gemeente Roosendaal heeft maatregelen getroffen die erin voorzien dat bij indiensttreding, dienstbeëindiging en wijziging van functie de daaraan gekoppelde logische en fysieke bevoegdheden voor het netwerk van de gemeente Roosendaal volgens een vaste procedure worden toegewezen of verwijderd. Voor applicaties is het minder structureel geregeld, echter kan men alleen gebruik maken van de applicaties als men toegang heeft tot het netwerk van de gemeente Roosendaal, waardoor bij uitdiensttreding ook onmiddellijk geen toegang meer verkregen kan worden tot applicaties. Ook maakt de gemeente Roosendaal gebruik van huisregels over het gebruik van faciliteiten, het melden van beveiligingsincidenten en het omgaan met informatie in het algemeen en persoonsgegevens in het bijzonder. Dit staat in de integriteitscode. Daarbij kan de gemeente niet met zekerheid zeggen of de huisregels ook aan extern personeel gecommuniceerd worden bij een aanstelling; men vertrouwt erop dat de uitzendbureaus dit voor hun rekening nemen. Ook besteedt de gemeente Roosendaal nog niet planmatig aandacht aan het actueel houden van kennis van medewerkers op het gebied van informatiebeveiliging, maar blijkt uit de gesprekken, dat dit wel op de planning staat.

[7] https://roosendaal.nl/privacyverklaring

4.1.5. Fysieke beveiliging

Het hoofdstuk fysieke beveiliging van de BIG heeft als doel om onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie te voorkomen. Het is dus van belang dat bijvoorbeeld de toegang tot computerruimtes of archiefkasten door onbevoegden wordt voorkomen, maar ook dat alleen de juiste personen toegang hebben tot informatie van de gemeenten (middels toegangsbeveiliging van apparatuur en autorisaties in software).

Voor de gemeente Roosendaal geldt dat voor elke vestiging een toegangsbeleid is beschreven waarin duidelijk is vastgelegd wie verantwoordelijk is voor de toegangsbeveiliging en het beheer van de daarvoor benodigde middelen.
Verder is het volgens de BIG van belang dat computerruimtes moeilijk herkenbaar gemaakt zijn. De meeste ICT-voorzieningen van Roosendaal worden gehost vanuit het gemeentekantoor, dat wil zeggen; de meeste servers zijn hier aanwezig. De computerruimte is niet als zodanig herkenbaar. Ook blijkt dat medewerkers die zelf niet geautoriseerd zijn alleen onder begeleiding van bevoegd personeel en als er een duidelijke noodzaak voor is, toegang mogen krijgen tot fysiek beveiligde ruimten waarin ICT-voorzieningen zijn geplaatst of waarin met vertrouwelijke informatie wordt gewerkt. Daarnaast staan er ook ICT-voorzieningen bij ICT-leveranciers. Over toegang zijn duidelijke afspraken in SLA's gemaakt. Ook is er een regeling voor het verwijderen en afvoeren van apparatuur en gegevensdragers. Uit de gesprekken blijkt dat de leverancier dit doet en dat laptops centraal worden verzameld. In het Informatiebeveiligingsbeleid staat dat het afvoeren of vernietigen per bedrijfseenheid geregistreerd wordt. Bij reparaties wordt niet specifiek rekening gehouden met beveiligingsrisico's, al wordt door de CISO hierbij aangegeven dat door de standaardbeveiligingsmaatregelen op telefoons en laptops (zoals encryptie) het risico op een incident zeer beperkt is.

Wat betreft de bescherming van apparatuur tegen calamiteiten, staat in het informatiebeveiligingsbeleid van de Gemeente Roosendaal beschreven dat beveiligde ruimten waarin zich bedrijfskritische apparatuur bevindt voldoende beveiligd moeten zijn tegen wateroverlast. Volgens dit beleid zijn ook gevaarlijke of brandbare materialen op een zodanige afstand van een beveiligde ruimte opgeslagen dat een calamiteit met deze materialen geen invloed heeft op de beveiligde ruimte. Uit de interviews blijkt dat het beleid met betrekking tot bedrijfskritische apparatuur in de praktijk wordt toegepast. Verder blijkt uit de gesprekken en documentatie dat de gemeente Roosendaal een cleardesk- en clearscreen beleid[8] hanteert en dat richtlijnen aanwezig zijn voor het gebruik van mobiele IT-voorzieningen binnen en buiten de organisatie. Volgens de richtlijnen van de BIG dient het gebruik van USB-poorten op pc's standaard geblokkeerd te zijn. De gemeente Roosendaal heeft gekozen om de toegang tot usb-poorten wel toe te staan, echter alleen in combinatie met het gebruik van een bitlocker (waarmee bestanden met encryptie en beveiligd worden weggeschreven op de usb-stick). Na het testen van deze maatregel blijkt dat het

[8] Cleardesk en clearscreen betekent dat er geen belangrijke informatie zichtbaar is of bereikbaar is voor mensen die deze informatie niet mogen zien.

afdwingen van bitlocker op een USB stick niet op laptops werkt. Dit wordt in 2019 opgepakt bij de implementatie van een Mobile Device Management tool (MDM)[9].

Wat betreft flexwerken zijn afspraken gemaakt binnen de gemeente. Deze zijn opgenomen in het informatiebeveiligingsbeleid. Bij flexwerken wordt gebruik gemaakt van een marktconform identificatie- en authenticatiemechanisme. Dit is gebaseerd op de Citrix technologie, waarmee de digitale werkplek op afstand beschikbaar wordt gesteld na een 2-factor authenticatie[10].

4.1.6. Beheersprocessen

Het hoofdstuk beheersprocessen heeft het waarborgen van een correcte en veilige bediening van IT-voorzieningen als doel. Dit betreft afspraken over omgaan met nieuwe software en onderwerpen als back-up en recovery van voorzieningen.

Bij de gemeente Roosendaal geldt dat procedures en verantwoordelijkheden voor het beheer van de bediening van alle ICT-voorzieningen zijn beschreven en vastgesteld. Ook zijn aparte (logisch gescheiden) omgevingen voor ontwikkeling, test, acceptatie en productie aanwezig voor kritische applicaties (indien gewenst: voor systemen die ingekocht worden is een ontwikkelomgeving niet noodzakelijk).

Uit het onderzoek blijkt dat bij acceptatie van nieuwe versies van systemen de eisen en acceptatiecriteria niet altijd duidelijk gedefinieerd, goedgekeurd, gedocumenteerd en getest zijn. Door functioneel beheerders wordt wel getest, maar soms mist een draaiboek om structureel en zorgvuldig te testen. De gemeente geeft zelf aan hier een verbeterpunt in te zien. Wel heeft de gemeente Roosendaal een formeel beleid met betrekking tot het naleven van programma-licenties en verboden gebruik van niet-geautoriseerde programma's.

In de interviews wordt aangegeven dat de gemeente Roosendaal continu een algemene back-up maakt. Daarnaast is een recoveryregeling getroffen ten behoeve van het herstel na calamiteiten. Deze worden ook getest, aldus de CISO. De werking in de praktijk hiervan hebben de onderzoekers niet kunnen vaststellen. In het informatiebeveiligingsbeleid is beschreven dat werkzaamheden van het ICT-beheer vastgelegd worden ten behoeve van rapportages en ook worden gelogd.

Voor het transporteren of delen van vertrouwelijke informatie en privacygevoelige informatie zijn extra maatregelen genomen. Ook is er een internet- en emailprotocol. Hiervoor worden extra beveiligde (boven de standaard) protocollen gebruikt. Daarnaast zijn verantwoordelijkheden en procedures voor het beheer van netwerken en apparatuur op afstand vastgelegd.
Verder eist de BIG dat de gemeente een actueel configuratieschema heeft van haar netwerk met al haar componenten. Op dit gebied wijkt de gemeente Roosendaal af van de BIG, omdat het netwerk grotendeels is uitbesteed aan de gemeenschappelijke regeling ICT West-Brabant West. Daardoor ligt de verantwoordelijkheid voor de

[9] Een oplossing voor Mobile Device Management (MDM) zorgt op mobiele apparaten zoals laptops, tablet en telefoons voor beveiliging, monitoring, beheer en ondersteuning door een IT-afdeling. Hiermee kunnen op afstand beveiligingsmaatregelen worden afgedwongen.
[10] Twee-factor authenticatie is een veilige methode om in te loggen, doordat het een tweede authenticatie vereist. Bijvoorbeeld naast het wachtwoord, een verificatie via sms.

veiligheid van het netwerk bij de Gemeenschappelijk Regeling. De gemeente houdt hier grip op middels contractafspraken met de gemeenschappelijke regeling.

4.1.7. Logische toegangsbeveiliging

Met het hoofdstuk logische toegangsbeveiliging doelt de BIG op het beheersen van de toegang tot informatie. Hiervoor moet beleid aanwezig zijn, moeten verantwoordelijkheden van gebruikers zijn gedefinieerd en de toegang tot netwerken goed worden geregeld.

De gemeente Roosendaal heeft een duidelijk en gedocumenteerd logisch toegangsbeleid waarin alle toegekende bevoegdheden in informatiesystemen adequaat worden beheerd. Daarbij zijn bevoegdheden alleen toegekend op basis van een 'need to use' en 'need to know' principe. Ook is iedere gebruiker uniek identificeerbaar en herleidbaar tot één persoon, al zijn hier een paar uitzonderingen op. Zo hebben de brandweer en politie bijvoorbeeld één account voor GIS en bestaan er algemene emailadressen. Per kritische applicatie worden periodiek de toegangsrechten gecontroleerd. Hiervoor is de functioneel beheerder verantwoordelijk. Er is echter niet een overall sturing op deze toegangscontrole voor alle applicaties, zoals de BIG voorschrijft.

Ook is er een duidelijk en stevig wachtwoordbeleid dat wordt afgedwongen[11]. Onderzoekers hebben tijdens een interview meegekeken in de computersystemen om te zien hoe dit werkt. Wachtwoorden hebben een beperkte levensduur. Netwerken zijn afdoende beveiligd. Zo is er sprake van netwerksegmentering. De digitale werkomgeving (Citrix) waarin medewerkers werken wordt automatisch geblokkeerd na 15 minuten inactiviteit. Verdachte of bijzondere gebeurtenissen worden gelogd. Medewerkers kunnen zelf geen applicaties installeren in de digitale werkomgeving (Citrix-omgeving). Op een laptop kunnen medewerkers wel zelf applicaties installeren. In de gebruikersovereenkomst die wordt aangegaan met de medewerker met een laptop staat dat de medewerker alleen legale applicaties mag installeren. Uit het interview met de CISO blijkt dat wanneer een medewerker een nieuw device krijgt, gezamenlijk met deze medewerker allerlei maatregelen ingesteld worden (zoals een pincode, een screenlock, encryptie en een virusscanner).

4.1.8. Ontwikkeling/aanschaf van systemen

De BIG doelt met het hoofdstuk ontwikkeling en aanschaf van systemen op het bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.

Bij de gemeente Roosendaal worden onderstaande informatiebeveiligingsaspecten meegenomen:

- *Wijzigingen op bestaande systemen*: uit gesprekken blijkt dat (incidenteel) bij major changes informatieadviseurs aanschuiven bij het

[11] Gebruikers worden door het systeem gedwongen wachtwoorden te kiezen, die aan bepaalde eisen voldoen en deze op gezette tijden te wijzigen (wanneer niet gewijzigd, geen toegang meer).

wijzigingsoverleg[12] van de GR ICT WBW om hier over te oordelen. Kleine wijzigingen worden niet expliciet op informatiebeveiliging beoordeeld.

- *Aanschaf van software of systemen*: vooral bij belangrijke systemen is dit een onderdeel. Zo geeft de CISO aan een bijdrage te leveren aan het opstellen van het programma van eisen voor nieuwe systemen. De gemeente Roosendaal ontwikkelt in principe nooit maatwerksystemen. Daarnaast werkt de gemeente met GIBIT[13]. Dit zijn inkoopvoorwaarden voor ICT-systemen die door de VNG zijn vastgesteld.

- *Testen van systemen en updates*: uit het gesprek met de CISO blijkt dat het testen en uitrollen van nieuwe systemen of updates verder geprofessionaliseerd kan worden. Momenteel zijn de testprocedures niet expliciet vastgelegd in een draaiboek.

- *In productie nemen van nieuwe software:* dit verloopt volgens de voorwaarden die de VNG daaraan stelt.

Met betrekking tot encryptie geldt voor Roosendaal dat dit wordt toegepast op mobiele gegevensdragers, zoals laptops en smartphones. De gemeente Roosendaal is voornemens om in 2019 een mobile device management tool (MDM) in te richten voor laptops, smartphones en tablets, waarmee de maatregelen ook technisch afgedwongen kunnen worden. Momenteel wordt, wanneer een medewerker een nieuwe laptop of smartphone ter beschikking krijgt, deze volgens de laatste veiligheidsvoorschriften geconfigureerd (dus met encryptie); echter de medewerker kan zelf op een later tijdstip deze instellingen ongedaan maken. Na installatie van een MDM-tool is dit niet meer mogelijk.

4.1.9. Incidentmanagement

Het hoofdstuk incidentmanagement in de BIG gaat over het bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.

Bij de gemeente Roosendaal is een procedure ingericht voor het melden en vervolgens rapporteren van digitale informatiebeveiligingsincidenten. Digitale informatiebeveiligingsincidenten die plaatsvinden bij de gemeente Roosendaal worden gemeld bij de servicedesk van de GR ICT WBW. Op basis van de bestudering van een lijst van incidenten kan vastgesteld worden dat deze incidenten structureel worden vastgelegd in de beheerapplicatie Topdesk. Indien noodzakelijk worden digitale informatiebeveiligingsincidenten doorgesluisd naar de CISO van Roosendaal. Het betreft alleen de digitale informatiebeveiligingsincidenten; de gemeente heeft hiermee geen registratie van de niet digitale informatiebeveiligingsincidenten, zoals bijvoorbeeld het verliezen van papieren informatie.

[12] Binnen het wijzigingen proces van de GR ICT WBW is dit een overleg. Dit overleg is verantwoordelijk voor beoordeling en planning van alle wijzigingen van meer dan geringe omvang. Alle betrokkenen en belanghebbenden zijn hierin vertegenwoordigd, zodat het hele wijzigingstraject beoordeeld en gepland kan worden.
[13] Zie https://www.vngrealisatie.nl/gibit

Uit verschillende interviews (zowel de Concerncontroller, de algemeen directeur als de CISO hebben een vergelijkbaar verhaal) blijkt dat er een niet-geformaliseerde escalatieladder tot aan de portefeuillehouder is. Wanneer zich incidenten voordoen, wordt de CISO ingelicht door de Gemeenschappelijke Regeling ICT West-Brabant West. De CISO besluit per situatie hoe te handelen, en hoe op te schalen afhankelijk van de ernst van het incident en de impact die het heeft op de dienstverlening van de gemeente. Wanneer de CISO het nodig acht wordt eerst de algemeen directeur ingeschakeld. In overleg met de algemeen directeur wordt eventueel de portefeuillehouder van het college bijgeschakeld. Informatie over beveiligingsrelevante handelingen, zoals loggegevens en foutieve inlogpogingen, worden echter niet regelmatig nagekeken en indien van toepassing niet gemeld aan de betreffende systeem- of proceseigenaar. In geval van een incident vindt altijd achteraf een evaluatie plaats, mede bedoeld om beheersmaatregelen te verbeteren. Ook zijn er afspraken met het IBD – NCSC (de informatiebeveiligingsdienst van gemeenten) over het melden van incidenten. De gemeente Roosendaal wordt andersom ook (wekelijks) geïnformeerd over dreigingen (onderzoekers hebben deze correspondentie kunnen inzien tijdens gesprek).

4.1.10. Continuïteitsmanagement

In de BIG is continuïteitsmanagement omschreven als het tegengaan van onderbreking van bedrijfsactiviteiten en de bescherming van kritische bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.

Bij de gemeente Roosendaal heeft een risicoanalyse plaatsgevonden over eventuele gebeurtenissen die de continuïteit van bedrijfsprocessen zouden kunnen schaden. Dit is onderdeel van de informatiebeveiligingsrisicoanalyse waarin beschikbaarheid één van de items is waarop gescoord wordt. Er is geen sprake van een actueel gemeentebreed continuïteitsbeleid. Alleen voor burgerzaken is er sprake van een continuïteitsplan. Hiervoor is bijvoorbeeld een noodaggregaat aangeschaft dat in geval van stroomuitval de systemen toch kunnen draaien.

Het aggregaat wordt (volgens de CISO) regelmatig getest, echter niet in samenhang met de processen van burgerzaken. Voor Burgerzaken zijn er verder ook uitwijkplannen en een ontruimingsdraaiboek beschikbaar. Voor andere processen binnen de gemeenten ontbreken uitwijkplannen en ontruimingsdraaiboeken.

Eén van de richtlijnen van de BIG is dat de organisatie over escrow-overeenkomsten[14] beschikt voor maatwerk-programmatuur waarvan de organisatie wel het gebruiksrecht bezit maar niet het eigendom. De gemeente heeft bewust de keuze gemaakt om hier geen gebruik van te maken, met uitzondering voor het zaaksysteem. Ten eerste omdat de gemeente als uitgangspunt heeft om met standaardpakketten te werken en niet met maatwerkpakketten. Ten tweede omdat het vaak met broncode alleen te complex is om de software zelf draaiend te houden. Mocht een leverancier bijvoorbeeld failliet gaan, dan is het vaak eenvoudiger om over te stappen naar een nieuwe leverancier, dan de bestaande software in de lucht te houden.

4.1.11. Naleving en bewustzijn van medewerkers

In de BIG staat naleving omschreven als het voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van enige beveiligingseisen.

De organisatie zet zich steeds meer in om medewerkers bewust te maken van de informatieveiligheidsrisico's. Zo staat er momenteel een programma in de steigers dat moet helpen om medewerkers bewust te maken van de gevaren, maar ook moet leren hoe ze hier mee moeten omgaan. Dit gebeurt onder andere middels e-learning. In eerste instantie zal deze niet verplicht zijn voor alle medewerkers. Daarnaast zijn er gedurende de zomer van 2018 verschillende workshops over de AVG voor medewerkers; deze worden goed bezocht. In de werkgroep privacy wordt de awareness van de medewerk(st)ers (op het gebied van privacy) periodiek geëvalueerd. Er zijn echter geen controle- of evaluatieprocessen ingericht op de naleving en het bewustzijn van medewerkers op het gebied van informatiebeveiliging.

[14] Een escrow-overeenkomst is een overeenkomst tussen de maker van software, zijn klanten en een escrow-agent. De overeenkomst garandeert dat de klant in bepaalde gevallen kan beschikken over de laatste broncode van het softwarepakket waarvoor de overeenkomst gesloten is.

Momenteel wordt er regelmatig gecommuniceerd met de medewerkers over risico's; op intranet zijn bijvoorbeeld verhelderende filmpjes te vinden en wordt geregeld gewaarschuwd voor phishingmail. Ook heeft men zelf wel eens phishingmails gebruikt om een beeld te krijgen van hoe de naleving daadwerkelijk in de praktijk plaatsvindt. De CISO geeft aan dat er behoefte is om meer te gaan meten in de toekomst.

Binnen alle geledingen van de organisatie is men zich ervan bewust dat de medewerkers een risico vormen voor de informatieveiligheid. In de dagelijkse praktijk worden door betrokkenen nog een aantal aandachtspunten voor de bewustwording rondom informatieveiligheid benoemd. Zo gaat het ene team beter om met de cleardesk- en clearscreen policy dan het andere team. Ook het vergrendelen van apparaten bij afwezigheid zou beter nageleefd kunnen worden. Het komt nog wel eens voor dat een computer bijvoorbeeld niet vergrendeld wordt bij het halen van koffie. Ook het bewustzijn op het gebied van privacy wordt door de organisatie nog als een aandachtspunt gezien. Niet alle medewerkers zijn zich bewust van de strenge eisen die de wetgever hieraan stelt. Als voorbeeld wordt genoemd dat onder sommige medewerkers de gedachte heerst dat er eenmaal toegang tot persoonsgegevens is verkregen, andere informatie ook automatisch ingezien mag worden.

De organisatie voert tweejaarlijks een gap-analyse[15] uit. Deze is gebaseerd op de BIG en wordt uitgevoerd door een externe onafhankelijke partij. Ook vinden verschillende (andere) audits plaats zoals de Basisregistratie Personen (BRP)-audit, een audit van Suwinet[16] en een audit van DigiD. In het kader van de AVG zijn er nog geen Data Protection Impact Analyses uitgevoerd.

Aan het management werd tot voor kort niet periodiek gerapporteerd over de status van informatiebeveiliging. Echter, het onderwerp kwam wel regelmatig ter tafel tijdens de zogenaamde college-plus vergaderingen, waardoor algemeen directeur en college geïnformeerd waren. Hier zijn echter geen verslagen van, waardoor het voor de onderzoekers niet is na te gaan wanneer er wat besproken is. Door de invoering van de Eenduidige Normering Single Information Audit (ENSIA)[17] is er momenteel wel sprake van verantwoording over dit onderwerp. Er zal jaarlijks naar het management van de gemeente en de raad gerapporteerd worden. Dit heeft in 2018 voor het eerst plaatsgevonden. Zo wordt in de audit op de ENSIA-collegeverklaring aangegeven dat in opzet en bestaan de Gemeente Roosendaal voldoet aan de beheersingsmaatregelen van de geselecteerde normen DigiD en SUWInet. Daarbij dient wel opgemerkt te worden dat bij een ENSIA-audit geen werkzaamheden worden uitgevoerd met betrekking tot de werking van interne beheersingsmaatregelen, waardoor er geen oordeel wordt gegeven over de werking van de maatregelen.

Ook wordt de ICT-infrastructuur van gemeenschappelijke ICT-regeling regelmatig door externe bureaus geaudit op kwetsbaarheden. Hier worden geen rapportages van ontvangen, behalve als er iets bijzonders aan het daglicht komt. De gemeente levert

[15] Met een Gap Analyse vergelijkt de organisatie de bestaande situatie met de gewenste situatie en wordt het verschil tussen identiteit (dat wat een organisatie wil uitstralen) en het imago (hoe er tegen een organisatie wordt aangekeken) in kaart gebracht.
[16] Via Suwinet Services kunnen overheidsorganisaties gegevens van burgers en bedrijven digitaal bij elkaar opvragen en naar elkaar sturen.
[17] De Eenduidige Normering Single Information Audit (ENSIA) richt zich op de gemeentelijke verantwoording rond de informatieveiligheid op basis van de Baseline Informatieveiligheid Gemeenten (BIG). ENSIA helpt gemeenten in één keer slim verantwoording af te leggen over informatieveiligheid gebaseerd op de BIG.

ook niet actief input voor deze audits, maar geeft aan dat als zij dat nodig acht dit wel mogelijk zal zijn. Op verschillende niveaus is er regelmatig afstemming met de gemeenschappelijk ICT-regeling en vindt sturing plaats.

4.2. Spoor 2: Bestuurlijke context en wisselwerking tussen raad en college

Op basis van een documentstudie, een interviewronde met de algemeen directeur, portefeuillehouder en Chief Information Security Officer (CISO) en een interactieve sessie met een afvaardiging van de raad, c.q. de auditcommissie, zijn inzichten opgedaan in de bestuurlijke context van informatieveiligheid en privacy bij de Gemeente Roosendaal en de wisselwerking tussen de raad en het college. In de onderstaande paragrafen worden de bevindingen toegelicht

4.2.1. De wisselwerking tussen de raad en college van B&W

Hoe is de communicatie/afstemming/sturing met betrekking tot het informatieveiligheidsbeleid tussen het college en de ambtelijke organisatie? Is de gemeenteraad in staat om te beoordelen of de informatieveiligheid en privacy binnen de gemeente Roosendaal op orde is? Hiervoor is van belang dat de gemeenteraad op het juiste moment over voldoende informatie beschikt en hij voldoende kennis heeft over informatieveiligheid om de informatie te kunnen beoordelen.

4.2.1.1 Voldoende en tijdige informatie

De wisselwerking tussen raad en college is op verschillende manieren te duiden. Een van de indicatoren voor een wisselwerking is de mate waarin expliciet verantwoording plaatsvindt over informatieveiligheid en privacy aan de gemeenteraad; dus beschikt de raad op het juiste moment over voldoende informatie. Hierin is gekeken naar twee zaken:

1. Objectief vast te stellen verantwoording; wat blijkt uit documenten?

2. Subjectief; hoe wordt de verantwoording beleefd?

<u>Objectief vast te stellen verantwoording</u>
Onderstaande tabel is het resultaat van de documentstudie. Het geeft weer of het onderwerp informatieveiligheid en privacy terugkomt in verantwoordingsdocumenten uit de jaarcyclus.

Beleid informatiebeveiliging				
Jaar	**Kadernota**	**Begroting**	**Jaarverslag**	**Opmerkingen**
2018	Niet genoemd	Niet expliciet	n.v.t	Ook niet in bestuursakkoord genoemd
2017	Niet genoemd	Niet expliciet	Wel genoemd	
2016	Niet genoemd	Niet genoemd	Niet genoemd	

Alleen in het jaarverslag van 2017 komt het onderwerp informatiebeveiliging expliciet terug. Hierin wordt melding gemaakt dat in 2017 intensief geïnvesteerd is in informatieveiligheid, en dat diverse maatregelen zijn geïmplementeerd. Ook wordt de ENSIA verantwoordingmethodiek aangekondigd. In de kadernota's en begrotingen komt het onderwerp informatieveiligheid en/of privacy verder niet terug. In 2017 en 2018 wordt in de begroting het onderwerp wel impliciet aangesneden, namelijk over de band van de gemeenschappelijk regeling aangestipt: "*Deze GR is opgericht met als doel het realiseren van een bedrijfszekere en veilige ICT-infrastructuur, zodat gemeenten zich kunnen blijven ontwikkelen richting een efficiëntere en digitale overheid"*.

Daarnaast is ook gekeken naar de schriftelijke vragen die door de raad zijn gesteld aan het college[18]; hoe vaak worden er door de raad vragen gesteld rondom informatieveiligheid en privacy? Onderstaande tabel geeft een overzicht van de vragen van 2017 en 2018.

Datum	Onderwerp raadsvraag
21-dec-17	Privacy
10-jan-18	Mailen naar de gemeente (privacygevoelige info)
10-jan-18	Mailverkeer (n.a.v. artikel in BNde stem)
5-mrt-18	Wifi in de Binnenstad, hoge kosten en beschermen persoonsgegevens
15-mrt-18	Algemene Verordening Gegevensbescherming
23-mei-18	AVG implementatie
29-aug-18	Privacywetgeving

Uit deze tabel blijkt duidelijk dat het onderwerp in 2018 meer aandacht krijgt van de raad. De vragen die gesteld worden gaan veelal over aan privacy gerelateerde onderwerpen, waar raadsleden zich zorgen over maken. Over het onderwerp informatieveiligheid worden minder vragen gesteld.

<u>Subjectieve beleving van verantwoording</u>
Uit de interactieve sessie blijkt dat de afvaardiging van de raad ontevreden is over de verantwoording van het college aan de raad rondom informatieveiligheid en privacy. De (afvaardiging van de) raad gaat er nu vanuit dat het college het onder controle heeft, zolang de raad niets hoort. Daarbij wordt benoemd dat zij willen weten wat het college eraan doet om informatieveiligheid en privacy te waarborgen, zoals het regelmatig toetsen van de veiligheid en afspreken wie wanneer rapporteert. De deelnemers van de interactieve sessie geven verder aan dat ze bij een frequentere verantwoording, waarover expliciete afspraken zijn gemaakt met het college, meer vertrouwen krijgen in de gemeente over het onderwerp informatieveiligheid.

De afvaardiging van de raad geeft aan behoefte te hebben aan een rapportage over informatieveiligheid in bijvoorbeeld de kadernota, de jaarrekening en de jaarrapportage. Ze geven daarbij aan dat dit volgens hen de basis vormt voor kaderstelling. Daarbij werd gesteld dat zolang zij niets horen, zij het idee hebben dat

[18] https://raad.roosendaal.nl/Documenten/Schriftelijke-vraag

er weinig te verantwoorden valt. Daarbij is het ook de vraag of alles wordt verantwoord wat níet goed gaat. Deelnemers geven aan dat het naleven van informatieveiligheid- en privacyprotocollen en het rapporteren hoe de gemeente dit doet, vooral van belang zijn.

In aanvulling op bovenstaande geven enkele raadsleden en geïnterviewden aan dat er altijd een spanningsveld zal zijn tussen college en de raad over welke dossiers en rapportages wel of niet openbaar gemaakt kunnen worden. Het college wil bepaalde onderwerpen niet altijd delen met de raad, bijvoorbeeld in het kader van gevoelige/bedrijfskritische informatie. Als gemeenteraad zou je erop moeten kunnen vertrouwen dat het college daar intern goede afspraken over maakt. De deelnemers geven aan dat zij er geen beeld van hebben of dit nu zo is. Het college en de algemeen directeur geven in de gesprekken aan dat ze vinden dat de raad te weinig gebruik maakt van andere instrumenten om voldoende op de hoogte te zijn van de stand van zaken op het gebied van informatiebeveiliging. In de ogen van de algemeen directeur wil de raad te vaak reactief (vooral bij landelijke incidenten) en vervolgens op detailniveau weten hoe een bepaald issue in elkaar zit, terwijl dit niet per se past binnen de controlerende rol. Het college is altijd bereid om raadsleden hierover te informeren. Soms worden in geval van dergelijke vragen bijeenkomsten georganiseerd voor raadsleden.

De beantwoording van de schriftelijke vragen die door de raad gesteld worden, leidt niet tot tevredenheid bij de afvaardiging van de raad. Als voorbeeld wordt de beantwoording van de vraag over de invoering van Wifi in de binnenstad gebruikt. De beantwoording was hier summier en te feitelijk in de ogen van de afvaardiging van de raad.

4.2.1.2 Kennis om informatie te begrijpen

Beschikt de gemeenteraad over voldoende kennis over informatieveiligheid om de informatie (die ze aangeboden krijgt) te kunnen beoordelen? Tijdens de interactieve sessie met een afvaardiging van de raad kwam het onderwerp 'rol en kennisniveau van de raad' met betrekking tot informatieveiligheid en privacy aan bod. De reacties op de vraag of de gemeenteraad in zijn geheel beschikt over voldoende kennis liepen uiteen. Een deel van de aanwezigen gaf aan het niet te weten, een deel vond van niet. Echter, de afvaardiging van de raad vraagt zich af in welke mate men over kennis zou moeten beschikken; het gaat hier om een controlerende taak, waarbij niet per definitie dieptekennis nodig is op dit onderwerp. Mocht het wel nodig zijn, dan kan men zich hier makkelijk in verdiepen, zoals voor veel onderwerpen geldt. Ook kan men het werk eventueel verdelen binnen fracties. Daarnaast geven raadsleden aan dat het wenselijk is dat dossiers die bij de raad terechtkomen (met betrekking tot informatieveiligheid en privacyaspecten) voldoende uitgelegd worden, in voor de raadsleden begrijpelijke taal en op het juiste detailniveau. De deelnemers geven aan het moeilijk te vinden om te zeggen of de andere raadsleden over voldoende kennis beschikken, maar dat ondanks het soms ontbreken van beschikbare kennis, het nut en de noodzaak wel duidelijk begint te worden.

4.2.2. Kaderstelling college en raad

Hoe wordt de kaderstellende rol door de gemeenteraad voor informatieveiligheid en privacy ingevuld?

Allereerst begint deze vraag met welke kaders er gezien worden zowel door de ambtelijke organisatie als door de raad. De volgende zaken worden door zowel de ambtelijke organisatie als het college en de raad benoemd als beleidsmatige kaders.

- Wettelijke kaders
  Vanzelfsprekend moet gemeente Roosendaal voldoen aan allerlei wet- en regelgevingen. De belangrijkste hiervan zijn de meldplicht datalekken en de Algemene Verordening Gegevensbescherming (AVG)

- Sectorbrede afspraken
  Door zowel de ambtelijke organisatie, het college als de raad worden sectorbrede afspraken (met andere gemeenten binnen VNG verband, of in afspraak met ministeries) als een belangrijk beleidsmatig kader gezien. Hierbij gaat het met name om de Baseline Informatiebeveiliging Gemeenten (BIG). Roosendaal is druk doende met het in praktijk brengen hiervan. Door iedereen wordt het als zeer zinvol ervaren om aan te sluiten bij ontwikkelingen in de sector, zoals de ENSIA.

Maakt de raad ook gebruik van zijn kaderstellende rol voor informatiebeveiliging? Vanuit de interviews met de algemeen directeur en de portefeuillehouder B&W blijkt dat de raad amper gebruikt maakt van zijn kaderstellende rol op dit gebied. Het ligt volgens de geïnterviewden ook niet per se in de lijn der verwachting dat de raad met kaders komt op dit onderwerp; voor bedrijfsvoeringonderwerpen is dit niet gebruikelijk.

Het beeld dat de raad weinig aanvullende kaders geeft voor informatieveiligheid en privacy wordt ook bevestigd in de interactieve sessie met een afvaardiging van de raad. Het college hanteert volgens hen alleen de wet- en regelgeving en de instructies vanuit VNG. Volgens hen zijn er verder geen inhoudelijke kaders. Pas als een incident heeft plaatsgevonden komt de raad op dit onderwerp met aanvullende kaders.

5. Conclusies

Dit onderzoek naar dataveiligheid bij de Gemeente Roosendaal bestond uit twee sporen. In het eerste spoor zijn de ambtelijke organisatie en het implementeren van de wettelijke kaders op het gebied van informatieveiligheid en privacy onderzocht. Dit spoor bestond uit drie delen, namelijk het bewustzijn van informatieveiligheid op de werkvloer, de kaders en wettelijke verplichtingen en de risico's op dit vlak. Hiervoor is de zogenaamde QuickScan BIG ingezet. De BIG (Baseline Informatieveiligheid Gemeenten) is het normenkader dat de beschikbaarheid, integriteit en exclusiviteit van gemeentelijke informatie(systemen) bevordert. De BIG is daarmee een richtlijn die een totaalpakket aan informatie beveiligingscontroles en -maatregelen omvat die voor iedere gemeente noodzakelijk is om te implementeren. Middels de QuickScan BIG is onderzocht of en hoe de gemeente Roosendaal zich aan deze richtlijnen houdt. In paragraaf 5.1 worden aan de hand van de QuickScan BIG de conclusies geformuleerd. In het tweede spoor is de bestuurlijke context en de wisselwerking tussen de raad en het college van B&W nader onderzocht. In dit spoor is aandacht besteed aan kaderstelling, communicatie, afstemming en sturing met betrekking tot het informatieveiligheidsbeleid. In paragraaf 5.2 worden de conclusies van spoor 2 beschreven. De conclusies van spoor 1 en spoor 2 leiden uiteindelijk tot de beantwoording van de vijf onderzoeksvragen in paragraaf 5.3.

5.1. Conclusies Spoor 1: QuickScan BIG

De QuickScan BIG bestaat uit een vragenlijst die is afgenomen tijdens een interviewronde met een aantal sleutelfiguren binnen de ambtelijke organisatie, zoals de Chief Information Security Officer (CISO) en de concerncontroller. Door de QuickScan is een beeld verkregen van de huidige positie van de gemeente Roosendaal op de verschillende subthema's van de BIG. De vragenlijst bevat per hoofdstuk van de BIG alle elementen die de BIG voorschrijft. De vragenlijst bestaat uit gesloten vragen, die beantwoord zijn met ja of nee, waardoor helder is of de gemeente op de betreffende richtlijn aan de norm voldoet. In onderstaande paragrafen beschrijven we per norm de conclusie, waarbij per norm expliciet wordt aangegeven waar de gemeente Roosendaal afwijkt van de norm en dit beperkt tot risico's leidt omdat er andere maatregelen zijn genomen, en waar de gemeente Roosendaal van de norm afwijkt zonder dat er aanvullende maatregelen zijn genomen.

5.1.1 Beleid

<u>Voldoen aan de norm</u>
Wat betreft de basisnorm beleid worden in de QuickScan vier van de vijf vragen beantwoord met een ja. Er is een actueel informatiebeveiligingsbeleid, waaruit een risicoanalyse voortvloeit. De maatregelen die nodig zijn om om te gaan met de risico's uit de risicoanalyse worden belegd in de organisatie, zowel qua rol als in de begroting.

<u>Afwijken van norm met beperkte risico's</u>
De vraag waar de gemeente Roosendaal afwijkt van de BIG-norm is dat er geen expliciete risicoanalyse per systeem of proces is, zoals de BIG wel voorschrijft. Dit betekent niet dat de Gemeente Roosendaal geen zicht heeft op de risico's die gelopen worden; er wordt een risicoanalyse uitgevoerd, en worden prioriteiten toegekend aan processen en systemen (op basis van privacygevoeligheid). Doordat de

aangekondigde maatregelen uit het document 'actieplan informatieveiligheid 2017' gerealiseerd zijn, is informatieveiligheid een structureler onderdeel van de Plan Do Check Act-cyclus (PDCA).

Afwijken van norm
Niet van toepassing op deze basisnorm.

Conclusie: de gemeente Roosendaal loopt op de basisnorm beleid geen verhoogde risico's.

5.1.2 Organisatie

Voldoen aan de norm
Wat betreft de basisnorm organisatie worden in de QuickScan acht van de tien vragen beantwoord met een ja. Dit betekent dat er verantwoordelijkheden zijn gedefinieerd voor informatiebeveiliging binnen de organisatie, er zijn duidelijke taakomschrijvingen, er zijn afspraken rondom de registratie en afhandeling van incidenten en er zijn afspraken met externe ICT-leveranciers over informatiebeveiliging.

Afwijken van norm met beperkte risico's
Een punt waar de gemeente Roosendaal afwijkt van de norm is dat er met de belangrijkste ICT-leverancier (de Gemeenschappelijke Regeling-ICT West-Brabant West) geen specifieke afspraken over informatiebeveiliging zijn vastgelegd in de dienstverleningsovereenkomst en er wordt niet periodiek gerapporteerd over informatiebeveiligingsincidenten. Wel zijn er afspraken over informatiebeveiliging opgenomen in het informatiebeveiligingsbeleid en in de verwerkersovereenkomst.

Afwijken van norm
De gemeente Roosendaal wijkt af van de BIG-norm omdat er binnen de gemeente geen stuurgroep is die rapportages over informatiebeveiligingsincidenten beoordeelt. Door de CISO wordt situationeel een inschatting gemaakt van het incident en besloten hoe het wordt afgehandeld en wie betrokken worden. Ook al heeft de gemeente Roosendaal wel een kernteam privacy dat datalekken beoordeelt, het voldoet niet aan de norm die vanuit de BIG gesteld wordt.

Conclusie; de gemeente heeft de organisatie van informatieveiligheid vrij goed geborgd Er zijn alleen aandachtspunten rondom de afhandeling van informatiebeveiligingsincidenten. Deze leiden niet direct tot risico's.

5.1.3 Objecten van beheer

Voldoen aan de norm
Wat betreft de basisnorm objecten van beheer worden in de QuickScan vijf van de zes vragen beantwoord met een ja. Dit betekent dat de gemeente Roosendaal in beeld heeft welke bedrijfsmiddelen (zoals laptops en telefoons) er gebruikt worden en dat bekend is welke maatregelen er genomen moeten worden om deze middelen goed te

beschermen tegen oneigenlijk gebruik. Ook is in beeld wie welke persoonsgegevens gebruikt.

Afwijken van norm met beperkte risico's
Op het gebied van de registratie van bedrijfsmiddelen is sprake van een hiaat: de registratie van desktops is namelijk verouderd. Dit leidt in de praktijk niet tot veiligheidsrisico's doordat de gemeente Roosendaal gebruik maakt van zogenaamde 'thin clients'. Hierdoor zijn er geen gevoelige gegevens of applicaties lokaal beschikbaar op desktops.

Afwijken van norm
Niet van toepassing op deze basisnorm

Conclusie; de geconstateerde afwijking van de norm leidt niet tot extra risico's voor de gemeente Roosendaal.

5.1.4 Personele eisen

Voldoen aan de norm
Wat betreft de basisnorm personele eisen worden in de QuickScan vijf van de acht vragen beantwoord met een ja. De gemeente Roosendaal zorgt ervoor dat werknemers hun verantwoordelijkheden op het gebied van informatiebeveiliging kennen. De gemeente heeft verschillende maatregelen getroffen om de risico's op diefstal, fraude of misbruik van faciliteiten te beperken.

Afwijken van norm met beperkte risico's
Niet van toepassing op deze basisnorm

Afwijken van norm
Tot op heden is er niet planmatig aandacht besteed aan het actueel houden van de kennis van medewerkers op het gebied van informatiebeveiliging. Dit staat op de planning van de gemeente voor najaar 2018.
Daarnaast houdt de gemeente Roosendaal geen overzicht bij van de kwetsbare functies bij de organisatie. Hierdoor kan de gemeente niet gericht maatregelen nemen om de kwetsbaarheid van deze functies te verminderen.
Er zijn wel afspraken met externe partijen die worden ingezet voor de inhuur van tijdelijke medewerkers (zoals uitzendbureaus) over het communiceren van de huisregels van de gemeente Roosendaal, maar het is onduidelijk of en op welke manier de huisregels van Roosendaal daadwerkelijk naar de tijdelijke medewerkers gecommuniceerd worden.

Conclusie: De gemeente wijkt af van de norm door niet aan alle eisen te voldoen. Gezien de constatering van de geïnterviewden dat het gedrag van medewerkers het belangrijkste risico vormt voor informatieveiligheid, verdient het voldoen aan deze norm juist prioriteit. Afwijken hiervan leidt tot onnodige risico's.

5.1.5. Fysieke beveiliging

Voldoen aan de norm
Voor de norm fysieke beveiliging worden in de QuickScan tien van de twaalf vragen beantwoord met een ja. Zo is er sprake van toegangsbeleid, is vastgesteld wie er voor verantwoordelijk is, zijn computerruimtes moeilijk herkenbaar gemaakt en hebben alleen geautoriseerde mensen toegang hiertoe. Ook zijn afspraken gemaakt over flexwerken, wordt zowel een toegangsbeveiliging als een cleardesk- en clearscreen beleid gehanteerd, zijn richtlijnen aanwezig voor IT-voorzieningen en is apparatuur voldoende afgeschermd en beveiligd. Over de werking in de praktijk van het cleardesk- en clearscreen beleid geeft men zelf aan dat dit soms te wensen overlaat.

Afwijken van norm met beperkte risico's
De gemeente Roosendaal wijkt af van de BIG-norm bij reparaties van laptops en telefoons door niet specifiek rekening te houden met alle beveiligingsrisico's. De genomen standaard beveiligingsmaatregelen (zoals encryptie van data) verminderen deze risico's deels.
De gemeente Roosendaal wijkt ook af van de BIG-norm door USB-poorten niet standaard te blokkeren. Dit is een bewuste keuze omdat men vindt dat men met extra beveiligingsmaatregelen (het verplichte gebruik van een bitlocker[19]) de risico's onder controle heeft. Er blijft echter een klein risico dat een eigen medewerker informatie moedwillig 'ontvreemdt' of op niet geautoriseerde apparaten gebruikt. Daarnaast werkt de bitlocker niet op laptops en de oplossing hiervoor moet nog geïmplementeerd worden.

Afwijken van norm
Niet van toepassing op deze basisnorm.

Conclusie: fysieke toegang tot informatie is bij de gemeente Roosendaal niet helemaal op orde. Dit leidt niet tot grote risico's, maar enkele aanpassingen in de beveiliging zijn wel gewenst.

5.1.6 Beheersprocessen

Voldoen aan de norm
Voor de norm beheersprocessen, waarbij het gaat om de correcte en veilige bediening van ICT-voorzieningen, worden in de QuickScan acht van de elf vragen beantwoord met een ja.

Afwijken van norm met beperkte risico's
Een van de vragen waar gemeente Roosendaal afwijkt van de BIG-norm is de aanwezigheid van aparte (logisch gescheiden) omgevingen voor ontwikkeling, test, acceptatie en productie. In het informatiebeveiligingsbeleid wordt gesteld dat dit aanwezig moet zijn, maar uit de interviews blijkt dat de gemeente hiervan afwijkt, omdat de gemeente zelf geen software ontwikkelt. Hierdoor is het niet noodzakelijk om over een ontwikkelomgeving te beschikken. De andere drie omgevingen zijn wel aanwezig voor de belangrijkste systemen. Afwijken van de norm leidt daarmee niet tot onnodige risico's.

[19] Met een bitlocker worden bestanden beveiligd en met encryptie weggeschreven op de usb-stick

Afwijken van norm
De gemeente wijkt af van de BIG-norm bij de acceptatie van nieuwe versies van systemen; de eisen vanuit informatiebeveiligingsperspectief en acceptatiecriteria zijn niet duidelijk gedefinieerd en gedocumenteerd. Hierdoor heeft informatiebeveiliging geen formele rol in updates of nieuwe systemen. Uit gesprekken blijkt dat informatiebeveiliging in de praktijk wel meegenomen wordt bij de aanschaf en uitrol van nieuwe systemen.

Conclusie; de afwijkingen op de norm leiden niet direct tot informatiebeveiligingsrisico's in de praktijk, echter het is niet duurzaam geborgd in de organisatie.

5.1.7. Logische toegangsbeveiliging

Voldoen aan de norm
Voor de norm logische toegangsbeveiliging worden in de QuickScan 23 van de 24 vragen beantwoord met een ja. De (ongeautoriseerde) toegang tot digitale informatie wordt onder andere voorkomen doordat er een logisch toegangsbeleid aanwezig is inclusief wachtwoordbeleid. Ook zijn verantwoordelijkheden van gebruikers gedefinieerd, waardoor gebruikers alleen toegang hebben tot informatie die voor hun taak/rol relevant is. De toegang tot netwerken is geregeld door netwerksegmentering.

Afwijken van norm met beperkte risico's
De gemeente wijkt af van de BIG-norm doordat overall sturing op toegangscontrole ontbreekt. De gemeente Roosendaal heeft ervoor gekozen om deze taak per applicatie te beleggen.

Afwijken van norm
Niet van toepassing op deze basisnorm

Conclusie; de geconstateerde afwijking vormt geen risico. De gemeente heeft de risico's rondom logische toegangsbeveiliging op orde.

5.1.8 Ontwikkeling en aanschaf van systemen

Voldoen aan de norm
Voor de norm ontwikkeling/aanschaf van systemen, waarmee geborgd wordt dat bij de ontwikkeling en aanschaf van systemen beveiliging integraal onderdeel uitmaakt van informatiesystemen, worden in de QuickScan vier van de zes vragen beantwoord met een ja.

Afwijken van norm met beperkte risico's
Niet van toepassing op deze basisnorm

Afwijken van norm
Het is niet structureel geborgd dat informatiebeveiliging bij grote wijzigingen in systemen en/of bij de aanschaf hiervan wordt meegenomen. Deze taak en rol is niet vastgelegd en geformaliseerd. Het is daarnaast geen expliciet onderdeel van test-

draaiboeken. De CISO of andere teamleden van informatiemanagement geven aan bij grote wijzigingen of aanschaf van belangrijke systemen wel mee te denken op het gebied van informatiebeveiliging.

Conclusie: door het niet structureel meenemen van informatieveiligheidsaspecten bij de aanschaf van systemen is Roosendaal niet helemaal in control op deze norm.

5.1.9 Incidentmanagement

Voldoen aan de norm
Voor de norm incidentmanagement worden in de QuickScan acht van de dertien vragen beantwoord met een ja.

Afwijken van norm met beperkte risico's
Niet van toepassing op deze basisnorm

Afwijken van norm
Gemeente Roosendaal wijkt met name af in de afhandeling en evaluatie van incidenten. Zo zijn de escalatieladder en de procedure niet geformaliseerd en worden er niet regelmatig analyses uitgevoerd op loggegevens en foute inlogpogingen. Door het niet formaliseren van de escalatieladder blijft de afhandeling van een incident gebaseerd op de inschatting van één sleutelspeler.

Conclusie: Incidentmanagement is binnen de gemeente Roosendaal niet voldoende geformaliseerd, waardoor de organisatie moet vertrouwen op het inschattingsvermogen van enkele sleutelspelers. Daarmee voldoet de gemeente Roosendaal niet aan de BIG-norm.

5.1.10 Continuïteitsmanagement

Voldoen aan de norm
Voor de norm continuïteitsmanagement worden in de QuickScan twee van de zes vragen met ja beantwoord.

Afwijken van norm met beperkte risico's
Hiermee is de score op deze norm voor gemeente Roosendaal lager dan op alle andere normen. Wat dit onderwerp betreft heeft de gemeente er bewust voor gekozen om geen gebruik te maken van escrow-overeenkomsten[20], waarmee ze afwijken van de norm. Echter andere maatregelen, zoals het werken met standaardsoftwarepakketten, zorgen ervoor dat risico's die daar uit voortvloeien beperkt zijn.

Afwijken van norm
Dit wordt vooral veroorzaakt doordat alleen voor burgerzaken volledig invulling wordt gegeven aan het continuïteitsbeleid en niet voor andere processen en/of systemen. Hierbij is geen ontruimingsdraaiboek of uitwijkplan beschikbaar. Wel heeft een

[20] Een escrow-overeenkomst is een overeenkomst tussen de maker van software, zijn klanten en een escrow-agent. De overeenkomst garandeert dat de klant in bepaalde gevallen kan beschikken over de laatste broncode van het softwarepakket

risicoanalyse plaatsgevonden over potentiële gebeurtenissen die de continuïteit van bedrijfsprocessen kunnen schaden

Conclusie: op deze norm scoort de gemeente Roosendaal onder de maat. Continuïteit van dienstverlening is onvoldoende geborgd en is onvoldoende helder gemaakt welke overwegingen ten grondslag liggen aan de gemaakte keuze om alleen voor burgerzaken invulling te geven aan continuïteitsbeleid, en niet voor andere processen.

5.1.11 Naleving en bewustzijn van medewerkers

Voldoen aan de norm
Voor de norm naleving en bewustzijn van medewerkers worden in de QuickScan drie van de zes vragen met ja beantwoord. Zo wordt tweejaarlijks een gap-analyse uitgevoerd door een externe, onafhankelijke partij, vinden verschillende audits plaats en zijn Data Protection Impact Analyses uitgevoerd.

Afwijken van norm met beperkte risico's
Niet van toepassing op deze basisnorm.

Afwijken van norm
De drie punten waar de gemeente afwijkt van de BIG-norm zijn:

1. Er is geen controle- en evaluatieproces ingericht om de naleving van de beveiligingseisen uit het informatiebeveiligingsbeleid te bewaken. Er is een plan hiervoor in ontwikkeling waarvan de uitvoering in het najaar 2018 van start moet gaan met als doel om medewerkers te leren omgaan met informatieveiligheidsrisico's.

2. Er wordt niet periodiek aan het management gerapporteerd over de status van informatiebeveiliging. Met de invoering van ENSIA[21] wordt verwacht dat verantwoording op dit onderwerp zal toenemen.

3. Er zijn geen controle- of evaluatieprocessen van naleving ingericht (behalve op privacy). Uit gesprekken blijkt dat men zich ervan bewust is dat het gedrag van medewerkers een risico vormt voor informatieveiligheid. Voorbeelden die genoemd worden door de geïnterviewden zijn naleving van het cleardesk- en clearscreen policy en het vergrendelen van apparaten bij afwezigheid. Volgens geïnterviewden verschilt de naleving hiervan per team.

   Conclusie: op deze norm scoort de gemeente Roosendaal onvoldoende. Dit onderwerp dient structureel meer aandacht te krijgen binnen de gemeente, zeker omdat hier de grootste risico's op gelopen worden.

[21] ENSIA (Eenduidige Normatiek Single Information Audit) heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus. Hierdoor heeft het gemeentebestuur meer overzicht over de stand van zaken van de informatieveiligheid en kan het hier ook beter op sturen.

5.1.12 Vergelijking met andere gemeenten

De afgelopen drie jaar is door het onderzoeksbureau ook bij vier andere gemeenten (vergelijkbaar qua omvang) de BIG-scan uitgevoerd. Vergelijken is, *door de kleine vergelijkingsgroep en door de verschillen in onderzoeksperiode (in drie jaar kan veel verbeteren),* risicovol en vraagt om een aantal voorbehouden. Over het algemeen kan gezegd worden dat in vergelijking met andere gemeenten Roosendaal een middenmoter is. Dat wilt zeggen; Roosendaal is overall geen koploper, maar hoort ook niet bij de slecht scorende gemeenten. Slechts weinig gemeenten scoren 100% op de BIG-norm. Ook punten waar Roosendaal afwijkt van de BIG-norm zijn vergelijkbaar met andere gemeenten; voor de andere gemeenten is naleving één van de hoofdstukken waar de meeste afwijkingen geconstateerd worden, net als voor Roosendaal. Het opstellen van documenten (zoals een informatiebeveiligingsbeleid) is immers ook makkelijker te voltooien dan het inregelen van nalevingsprocessen en daar structureel op te sturen. Continuïteitsbeleid is een onderwerp waarop de gemeente Roosendaal wel negatief afwijkt van andere gemeenten; veelal is bij andere gemeenten het continuïteitsbeleid breder ingestoken dan burgerzaken en is er sprake van een ontruimingsdraaiboek of uitwijkplan. Ook op incidentmanagement scoort Roosendaal net iets onder het gemiddelde; de escalatieladder en procedure is bij de meeste gemeenten wel geformaliseerd.

5.2. Conclusies Spoor 2: Bestuurlijke context en wisselwerking tussen raad en college

Om zicht te krijgen op de vragen in spoor 2 is gebruik gemaakt van interviews en een interactieve sessie met een afvaardiging van de raad.

5.2.1. De wisselwerking tussen de raad en college van B&W

Hoe is de communicatie/afstemming/sturing met betrekking tot het informatieveiligheidsbeleid tussen het college en de ambtelijke organisatie? Is de gemeenteraad in staat om te beoordelen of de informatieveiligheid en privacy binnen gemeente Roosendaal op orde is?
Als eerste is gekeken of de raad voldoende en tijdig informatie ontvangt van het college. In de verantwoordingsdocumenten van de gemeente, zoals de kadernota, de begroting en het jaarverslag, komt het onderwerp informatieveiligheid en privacy nauwelijks terug. Op basis van huidige informatievoorziening vanuit het college is het daarmee lastig om de controlerende rol te vervullen.
Een ander instrument van de gemeenteraad om ingelicht te worden over dit onderwerp is het stellen van schriftelijke vragen. Hier werden in 2017 weinig vragen over gesteld, maar we constateren wel een toename van schriftelijke vragen die gesteld worden door gemeenteraadsleden over dit onderwerp. De beantwoording van vragen door het college leidt lang niet altijd tot tevredenheid bij raadsleden. De informatievoorziening wordt door de afvaardiging van de gemeenteraadsleden als onvoldoende ervaren. Er is een behoefte aan frequenter ingelicht te worden over de stand van zaken van de gemeente op het gebied van informatiebeveiliging. Ze geven aan dat ze hier expliciete afspraken over willen maken met het college. Niet de hele raad denkt over voldoende

kennis over het onderwerp informatieveiligheid te beschikken om de aangereikte informatie goed te kunnen begrijpen. Dit wordt echter niet als problematisch ervaren, omdat men zich snel kan verdiepen in de materie als het niet begrijpelijk is.

De beperkte manier waarop de raad zowel proactief als reactief wordt ingelicht door het college leidt tot beperkt vertrouwen van de raad in de ambtelijke organisatie op het gebied van informatieveiligheid. Dit terwijl, gezien de feitelijke situatie in de gemeente en de voortgang die de ambtelijk organisatie heeft gemaakt op dit onderwerp, onnodig is. Betere informatieverstrekking zal het vertrouwen verbeteren. Er zijn daarbij meerdere instrumenten om deze informatievoorziening te organiseren. De raad maakt momenteel beperkt gebruik hiervan. Andere instrumenten, zoals een kennissessie, zouden enkele bezwaren van de ambtelijke organisatie (bijvoorbeeld het vertrouwelijke omgaan met dit onderwerp) wegnemen.

5.2.2. Kaderstelling college en raad

De gemeente Roosendaal hanteert voor informatiebeveiliging en privacy twee soorten kaders. Ten eerste worden wet- en regelgeving, zoals de meldplicht datalekken en de AVG als kader gebruikt. Ten tweede conformeert de gemeente zich aan landelijke afspraken, zoals de afspraak over het toepassen van de BIG-norm. Vanuit de gemeenteraad worden geen extra aanvullende kaders meegegeven aan de gemeente op dit onderwerp. De gemeenteraad functioneert op dit onderwerp meer reactief dan agenderend.
Gezien informatieveiligheid een bedrijfsvoering onderwerp betreft, lijkt het passend dat de gemeenteraad beperkt een agenderende rol aanneemt op het gebied van informatieveiligheid. De rol van de raad is immers om te sturen op beleidsvoornemens en niet op de details van de uitvoering. Ook zijn er geen directe aanleidingen (bijvoorbeeld aanwijzingen van verhoogde risico's) waardoor de gemeenteraad aanvullende kaders zou moeten stellen. Echter, informatie krijgt steeds meer een spilfunctie in de gemeentelijke dienstverlening. Hierdoor is het belang van goede informatieveiligheid toegenomen. Daarnaast werkt de gemeente op veel gebieden samen met andere partijen in het informatiedomein. Hierdoor neemt de complexiteit in sturing toe; een onderwerp wat de gemeenteraad wel degelijk aangaat.

5.3. Conclusies op de onderzoeksvragen

Met de conclusies uit spoor 1 en spoor 2 kunnen de vijf onderzoeksvragen beantwoord worden.

1. Hoe is het gesteld met het bewustzijn t.a.v. informatieveiligheid en privacy in de ambtelijke organisatie van gemeente Roosendaal?

   Bewustzijn van medewerkers is en blijft binnen de gemeente Roosendaal een belangrijk aandachtspunt. Zo scoort de gemeente op de BIG-norm 'naleving' slechts een 3 (schaal 1 t/m 5). Ook zijn niet alle aanbevelingen uit het adviesrapport van BMC[22] rondom privacy volledig geïmplementeerd,

[22] Persoonsinformatie en privacy, Roosendaal op weg naar Wbp-proof en

bijvoorbeeld het verhogen van privacybewustzijn in de hele organisatie. Uit gesprekken blijkt dat men zich duidelijk bewust is dat gedrag van medewerkers een belangrijk risico vormt op het gebied van informatiebeveiliging. Medewerkers die zich bezig houden met privacygevoelige informatie, zoals bijvoorbeeld in het sociale domein, zijn al extra getraind op het goed omgaan hiermee. Echter niet in alle geledingen van de gemeente is sprake van een vergelijkbaar bewustzijn hiervan. De gemeente zet in het najaar van 2018 dan ook in om dit te verbeteren. Het afwijken van de normen 'personele eisen' en 'naleving' door niet structureel het kennisniveau en bewustzijn rondom dit onderwerp van medewerkers hoog te houden, leidt tot onnodige risico's.

2. Geeft de gemeente Roosendaal vorm en inhoud aan het informatieveiligheidsbeleid en wettelijke kaders? En zo ja, hoe gebeurt dat?

   De gemeente geeft vorm en inhoud aan het informatiebeveiligingsbeleid. Dit beleid is gestoeld op wettelijke kaders (zoals de AVG) en op sectorale afspraken, zoals het toepassen van de BIG-norm. In het beleid zijn de voorgestelde maatregelen uit de BIG opgenomen. Nog niet op alle punten van de BIG-norm voldoet de gemeente. Soms wordt bewust afgeweken van de norm omdat men bijvoorbeeld andere maatregelen heeft genomen om de risico's te beperken. Op andere normen is men wel bewust van de afwijking, maar moet men nog maatregelen in de praktijk brengen. De gemeente heeft verschillende functionarissen aangesteld die de verantwoordelijkheid hebben voor informatieveiligheid binnen de gemeente, denk aan een Chief Informatie Security Officer (CISO) en een Functionaris Gegevensbescherming (FG). De gemeente voert regelmatig audits en evaluaties uit op het gebied van informatiebeveiliging om te toetsen waar ze staat en waar nodig verbeteringen aan te brengen. Het gebruik van een ISMS[23] zorgt voor meer structurele aandacht en grip op informatiebeveiliging. Informatiebeveiliging en privacy zouden nog structureler geborgd kunnen worden in de organisatie en ook binnen de verantwoordingslijnen van de organisatie; zo ontbreekt een formele escalatieladder en worden informatiebeveiligingsincidenten niet structureel geëvalueerd. Dit is cruciaal omdat het informatiedomein van de gemeente Roosendaal complex is; er is op tal van gebieden sprake van samenwerking met andere organisaties, waardoor de veiligheid van informatie niet binnen de eigen control valt. Dit leidt niet direct tot risico's, maar de borging van informatiebeveiliging in afspraken en werkprocessen met samenwerkingspartijen kan beter georganiseerd worden. Een voorbeeld is het meenemen van informatiebeveiligingsaspecten bij wijzigingen in systemen.
   De gemeente Roosendaal heeft de laatste jaren een aantal stappen gemaakt op het gebied van informatiebeveiliging. Als de score in dit onderzoek vergeleken wordt met de gap-analyse uit 2016 dan is er sprake van vooruitgang. In vergelijking met andere gemeenten is Roosendaal geen koploper, maar hoort het ook niet bij de slecht scorende gemeenten. Wanneer de gemeente inzet op het oplossen van de geconstateerde afwijkingen dan kan de gemeente haar informatiebeveiliging snel naar het benodigde niveau brengen. Uiteraard zal er

AVG voorbereid. Rapport inventarisatie persoonsgegevens en toetsing aan privacykader, BMC, november 2016
[23] Information Security Management System is een managementsysteem voor informatiebeveiliging. Een ISMS sluit aan bij het beleid en de strategie van de organisatie en dient geïntegreerd te worden in de werkprocessen. Het doel van een ISMS is (vertrouwelijke) informatie beter te beveiligen. Het is niet een tool, maar een manier van werken.

continue aandacht voor dit onderwerp nodig blijven om het bewustzijn in de organisatie op het juiste niveau te brengen en vooral ook te houden.

3. Heeft de gemeente in brede zin een goed beeld van de belangrijkste risico's op het gebied van de informatiebeveiliging en in het bijzonder de bescherming van de persoonsgegevens?

   De gemeente voert een risicoanalyse uit op het gebied van informatieveiligheid. Deze risicoanalyse is tweeledig: de gapanalyse en de MAPGOOD-methode. De zogenaamde gapanalyse is gestoeld op de BIG en wordt weer in het 'Information Security Management System' (ISMS) bijgehouden. Deze risico's worden vervolgens geactualiseerd op het moment dat er een groot project of een grote wijziging optreedt. Daarnaast is er nog een risicoanalyse gebaseerd op de MAPGOOD-methodiek waarin voor de belangrijkste systemen en processen de risico's in beeld worden gebracht. Echter, het ontbreekt aan een expliciete risicoanalyse voor alle systemen of processen, zoals de BIG wel voorschrijft. Vanuit de risicoanalyses zijn er prioriteiten toegekend aan processen en systemen en ook is beschreven welke processen privacygevoelig zijn. Op basis hiervan zijn voor de privacygevoelige processen extra maatregelen genomen, denk bijvoorbeeld aan de training van medewerkers in het sociale domein. Bij de risicoanalyse zijn veel stakeholders betrokken.
   Kortom: in de gemeente is goed zicht op de informatiebeveiligingsrisico's. Deze inzichten zijn niet breed gedeeld binnen de gemeente en daarnaast ook geen structureel onderdeel van de bedrijfsvoerings-risicoanalyse die in het kader van de beleidscyclus wordt uitgevoerd, waardoor ze binnen de ambtelijke top niet volledige prioriteit hebben.

4. Hoe is de communicatie/afstemming/sturing met betrekking tot het informatieveiligheidsbeleid tussen het college en de ambtelijke organisatie?

   Zowel het college als de ambtelijke organisatie leunen sterk op de expertise van enkele functionarissen in de organisatie die verantwoordelijk zijn voor informatiebeveiliging en privacy. Het onderwerp wordt wel eens besproken tijdens zogenaamde college-plus vergaderingen (college en MT). Daarnaast wordt het college bij grote informatiebeveiligingsincidenten ingelicht. Hier is geen protocol voor, maar gebeurt op basis van een situationele inschatting van de CISO. De rol van de portefeuillehouder en de directie bij informatiebeveiliging en privacy is beperkt. Ze zijn uiteindelijk integraal verantwoordelijk voor het onderwerp; dat betekent bij dit onderwerp toezien dat taken rondom informatieveiligheid uitgevoerd worden en zich geregeld laten bijpraten over de actuele stand van zaken. Kortom, er is sprake afstemming en sturing. Het onderwerp heeft aandacht in de verticale verantwoordingslijn tussen college en ambtelijke organisatie, echter is dit niet in voldoende mate geformaliseerd.

5. Hoe is/wordt aan de kaderstellende en controlerende rol van de gemeenteraad met betrekking tot de informatieveiligheid vorm en inhoud gegeven?

   De gemeenteraad geeft beperkt invulling aan zijn kaderstellende rol. Het is te typeren als reactief; wanneer een incident zich voordoet dan reageert de raad.

De gemeenteraad vindt het moeilijk om op het onderwerp informatiebeveiliging en privacy de controlerende rol goed in te vullen. Dit komt met name doordat de raad vindt dat het onvoldoende frequent en te summier qua inhoud wordt geïnformeerd over dit onderwerp. Er is behoefte aan meer zicht op de maatregelen die de gemeente neemt om de veiligheid te borgen. De raad maakt in toenemende mate gebruik van het middel van schriftelijke vragen, echter leidt de beantwoording van deze vragen door het college niet tot het gewenste vertrouwen van de raad in de gemeente op dit punt. Vanuit het college en de ambtelijke organisatie leeft juist het beeld dat de raad niet alle middelen gebruikt om voldoende geïnformeerd te zijn. Het onderwerp informatieveiligheid en privacy vraagt soms om een meer vertrouwelijke benadering (dan schriftelijke vragen stellen) en raadsleden zouden zich daarom beter op andere manieren kunnen laten informeren. Een voorbeeld hiervan zijn sessies georganiseerd door de gemeente.
De beperkte informatievoorziening van het college richting de raad met betrekking tot informatieveiligheid en privacy leidt tot een (onnodig) gebrek aan vertrouwen binnen de raad in de gemeente. Frequentere en uitgebreidere informatievoorziening zou de raad beter faciliteren in het vervullen van zijn rol.

6. Aanbevelingen

De bevindingen en de conclusies, zoals in hoofdstuk 4 en 5 beschreven, leiden tot de volgende aanbevelingen:

Spoor 1: Ambtelijke organisatie

- We stellen voor dat de gemeente zich conformeert aan de BIG-norm door wel per systeem of proces een expliciete risicoanalyse uit te voeren. Hierdoor ontstaat een completer beeld van de risico's.
- Stel een procedure vast voor het rapporteren van beveiligingsgebeurtenissen en borg deze in de organisatie. Hierin wordt rekening gehouden met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident. Daarnaast is het wenselijk dat er een stuurgroep ingericht wordt die rapportages over informatiebeveiligingsincidenten beoordeelt.
- Maak met de Gemeenschappelijke Regeling-ICT West-Brabant West specifieke afspraken over informatiebeveiliging (aanvullend op het gezamenlijke informatiebeveiligingsbeleid) en leg deze vast in de dienstverleningsovereenkomst. Zorg dat hier ook afspraken over periodieke rapportages in opgenomen zijn.
- Verbeter de registratie van bedrijfsmiddelen door ook de registratie van desktops te actualiseren.
- Het is belangrijk om te borgen dat tijdelijke medewerkers, die via externe partijen zoals uitzendbureaus worden ingezet bij de gemeente Roosendaal ook bekend gemaakt worden met de huisregels (specifiek rondom informatieveiligheid) bij de gemeente. Dit kan door bijvoorbeeld met enige regelmaat een steekproef te houden.
- Tot op heden is niet planmatig aandacht besteed aan het actueel houden van de kennis van medewerkers op het gebied van informatiebeveiliging. Dit staat op de planning van de gemeente voor najaar 2018. Het planmatig bewust maken van medewerkers en actueel houden van hun kennis is niet een eenmalige activiteit en dient regelmatig aandacht te krijgen.
- Maak een overzicht van kwetsbare functies binnen de gemeente zodat de gemeente in staat is daarop gericht maatregelen te nemen om de risico's voor deze functies te beperken.
- Maak aanvullende afspraken rondom reparaties van laptops en telefoons, zodat informatiebeveiligingsrisico's geborgd zijn.
- Zorg dat de informatiebeveiligingseisen voor systemen en de daarbij behorende acceptatiecriteria goed gedefinieerd en gedocumenteerd zijn, zodat bij de acceptatie van nieuwe versies van systemen hier rekening mee gehouden wordt.
- Zorg dat er periodiek gerapporteerd wordt aan het management over de status van informatiebeveiliging binnen de gemeente.
- Zorg dat er voor de cruciale processen Data Privacy Impact Analyses worden uitgevoerd.

Spoor 2 : Bestuurlijke wisselwerking

- De gemeenteraad wordt te weinig frequent en inhoudelijk te summier ingelicht door de ambtelijk organisatie. Het is belangrijk om afspraken (tussen college en raad) te maken over de manier waarop en de frequentie waarmee het college en de ambtelijke organisatie de gemeenteraad kan informeren, zodat zowel de informatiebehoefte van de gemeenteraad vervuld wordt, als dat er voldoende rekening gehouden wordt met de bezwaren (zoals vertrouwelijkheid) van de ambtelijke organisatie.
- De beantwoording van schriftelijke vragen wordt als summier ervaren. Omdat het onderwerp inhoudelijk soms ingewikkeld is, zou het college er goed aan doen om extra uitleg te geven bij de beantwoording van vragen.
- Het organiseren van een informerende themabijeenkomst kan helpen om de kennis van de raad met betrekking tot informatieveiligheid en privacy te verbreden. De bijeenkomst zou specifiek over de gemeente Roosendaal moeten gaan ('waarom doen we bepaalde dingen, welke afwegingen zijn gemaakt, hoe verloopt de samenwerking met ICT West-Brabant, waar zijn zij voor verantwoordelijk en zijn wij dan wel in control, etc.), met een laag instapniveau (bijvoorbeeld in de vorm van een kort inleidend college over het normenkader BIG) en daarna een verdieping op de specifieke situatie van de gemeente. Daarin zouden volgens de deelnemers maatregelen van de gemeente en de wisselwerking tussen raad en college aan bod moeten komen, met een toelichting op hoe bepaalde keuzes gemaakt worden door het college. Bijvoorbeeld het wel of niet delen van rapportages met de raad en de openbaarheid daarvan.

Overall: met het gebruik van een ISMS[24] is de gemeente op weg om informatieveiligheid goed te borgen. De uitdaging zit in het goed bijhouden hiervan zodat men grip heeft op alle risico's en maatregelen. Daarnaast is informatieveiligheid een kwestie van volharding. Het is meer dan naar aanleiding van een rapport actie ondernemen, want het vraagt om constante aandacht en hier zo transparant mogelijk over communiceren richting de gemeenteraad.

[24] Information Security Management System is een managementsysteem voor informatiebeveiliging. Een ISMS sluit aan bij het beleid en de strategie van de organisatie en dient geïntegreerd te worden in de werkprocessen. Het doel van een ISMS is (vertrouwelijke) informatie beter te beveiligen. Het is niet een tool, maar een manier van werken.

7. Reactie college op conceptrapportage

Op 17 januari 2019 heeft de Rekenkamer het conceptrapport aangeboden voor bestuurlijk hoor en wederhoor. Het college heeft op 12 februari hierop gereageerd. De inhoud van deze brief is onderstaand integraal verwoord.

Geachte leden van de Rekenkamer,

De Rekenkamer West-Brabant heeft in 2018 onderzoek verricht naar databeveiliging binnen de gemeente Roosendaal. Op de onderzoeksbevindingen hebben wij reeds via de ambtelijke reactie onze opmerkingen gegeven; deze zijn voor het merendeel door uw Rekenkamer overgenomen. Bij deze geven wij u onze bestuurlijke reactie op de conclusies en aanbevelingen van het rapport.

Ter wille van de overzichtelijkheid sluiten wij in onze reactie aan bij de indeling, zoals gehanteerd in het rapport.

Spoor 1: Ambtelijke organisatie
Wij onderschrijven de deelconclusies op de navolgende onderdelen:

5.1.1	Beleid
5.1.2	Organisatie
5.1.3	Objecten van beheer
5.1.5	Fysieke beveiliging
5.1.6	Beheersprocessen
5.1.7	Logische toegangsbeveiliging
5.1.10	Continuïteitsmanagement

Bij een vijftal andere deelconclusies willen wij enige nuancering aanbrengen.

5.1.4 Personele eisen
Conclusie: De gemeente wijkt af van de norm door niet aan alle eisen te voldoen. Gezien de constatering van de geïnterviewden dat het gedrag van medewerkers het belangrijkste risico vormt voor informatieveiligheid, verdient het voldoen aan deze norm juist prioriteit. Afwijken hiervan leidt tot onnodige risico's.
Reactie: Het belang hiervan erkennen wij. Sinds afgelopen jaar investeren we dan ook consequent in het bevorderen van de bewustwording en daarbij passend gedrag door het geven van workshops aan het college en ambtelijke organisatie en het beschikbaar stellen van een interactieve e-learning omgeving.

5.1.8 Ontwikkeling en aanschaf van systemen
Conclusie: Door het niet structureel meenemen van informatieveiligheidsaspecten bij de aanschaf van systemen is Roosendaal niet helemaal in control op deze norm.
Reactie: Wij streven naar een organisatie, waarin vertrouwen een belangrijke plaats inneemt naast de meer traditionele "harde" controlmaatregelen. Voor ons betekent in control zijn: het juiste evenwicht tussen formeel waar het moet en informeel waar het kan met als leidende gedachte "high trust, high penalty".

5.1.9 Incidentmanagement
Conclusie: Incidentmanagement is binnen de gemeente Roosendaal niet voldoende geformaliseerd, waardoor de organisatie moet vertrouwen op het inschattingsvermogen van enkele sleutelspelers. Daarmee voldoet de gemeente Roosendaal niet aan de BIG-norm.
Reactie: Wij verwijzen naar onze reactie op de vorige conclusie.

5.1.11 Naleving en bewustzijn van medewerkers
Conclusie: Op deze norm scoort de gemeente Roosendaal onvoldoende. Dit onderwerp dient structureel meer aandacht te krijgen binnen de gemeente, zeker gezien hier de grootste risico's op gelopen worden.
Reactie: Met de invoering van ENSIA maakt rapportage over de status van informatie-beveiliging deel uit van onze P&C-cyclus. De bewaking van de naleving van de beveiligingseisen vloeit logischerwijs voort uit de vervaardiging van de jaarlijkse verantwoording. Hiervoor actualiseren we momenteel de processen. Wij zijn ons terdege bewust van het belang van het gedrag van medewerkers (zie ook ons antwoord op deelconclusie 5.1.4).

5.1.12 Vergelijking met andere gemeenten
Wij herkennen ons niet in het beeld dat de gemeente Roosendaal een "middenmoter" zou zijn, gebaseerd op het gegeven dat formele procedures ontbreken en we daardoor niet aan de BIG-norm voldoen. De focus in onze organisatie ligt meer op het pragmatisch en adequaat oplossen van beveiligingsincidenten. Het management ziet het belang van informatieveiligheid in en stimuleert maatregelen op het gebied van mens, proces, gebouw en techniek om zodoende de beveiligingsrisico's en bedreigingen te minimaliseren. De organisatie transformeert geleidelijk van een reactieve naar een meer proactieve modus. Aandacht voor continuïteitsmanagement maakt daar nadrukkelijk onderdeel van uit.

Spoor 2: Bestuurlijke context en wisselwerking tussen raad en college

5.2.1 De wisselwerking tussen de raad en college van burgemeester en wethouders
Wij onderschrijven uw conclusie dat de ambtelijke organisatie de laatste tijd aanmerkelijke voortgang heeft geboekt op het gebied van informatieveiligheid. Dat de wijze van informatie-uitwisseling tussen raad en college geleid zou hebben tot beperkt vertrouwen in de organisatie, is een conclusie die wij niet delen. Wij nemen dit signaal echter serieus en zullen - zoals hierna aangegeven onder de aanbevelingen - met de raad ter zake afspraken maken.

5.2.2 Kaderstelling college en raad
Wij zijn het eens met uw analyse dat informatieveiligheid bedrijfsvoering betreft, waar de kaderstellende rol van de raad uit de aard van dit onderwerp beperkt is. Dat samenwerking met andere partijen in het informatiedomein leidt tot complexiteit in sturing doet daar ons inziens niet aan af.

Aanbevelingen

Spoor 1: Ambtelijke organisatie

Het merendeel van de aanbevelingen is reeds onderhanden (geldt voor aanbeveling 3, 4, 5, 6 en 10) dan wel staat voor dit jaar op de planning om geïmplementeerd te worden (aanbeveling 2, 7, 8, 9 en 11). Aanbeveling 1 hebben wij als volgt opgepakt: om redenen van efficiency voeren wij een diepgaande risicoanalyse uit op de belangrijkste systemen en processen in plaats van op ieder proces afzonderlijk.

Spoor 2: Bestuurlijke context en wisselwerking tussen raad en college

Wij willen in overleg met de raad bepalen op welke wijze en met welke frequentie de onderwerpen informatieveiligheid en privacy besproken kunnen worden. Inmiddels is een themabijeenkomst belegd, waarin de bespreking van dit rekenkamerrapport aan de orde komt en onze Chief Information and Security Officer (CISO) en Functionaris voor de Gegevensbescherming (FG) presentaties over informatieveiligheid en privacy zullen verzorgen.

Onze insteek bij de beantwoording van schriftelijke vragen is zo veel mogelijk "to the point" te blijven. Mocht naar aanleiding daarvan behoefte bestaan aan nadere uitleg, dan zijn wij daartoe uiteraard steeds bereid.

Hoogachtend,

Burgemeester en wethouders van Roosendaal,

De secretaris, De burgemeester,

Drs. M.C.J. Franken Mr. J.M.L. Niederer

8. Nawoord

De Rekenkamer heeft kennis genomen van de reactie van het College op het onderzoeksrapport. De reactie heeft betrekking op zowel de conclusies als de aanbevelingen.
Allereerst onderschrijft het College een groot aantal deelconclusies. Daarnaast wilt het College graag nuancering aanbrengen op een vijftal deelconclusies. Het gaat hier vooral om het toevoegen van het juiste perspectief waarin de conclusies gelezen moeten worden.

Een aantal kanttekeningen heeft betrekking op de voortschrijdende ontwikkeling van de gemeente op het vlak van informatiebeveiliging. Het College geeft bijvoorbeeld aan dat er recent investeringen zijn gedaan rondom bewustwording van het College en de ambtelijke organisatie. Informatiebeveiliging is een vakgebied dat zich snel ontwikkelt en ook de gemeente Roosendaal staat hierbij niet op stil. Het is dus goed mogelijk dat de gemeente verschillende verbeteringen reeds heeft doorgevoerd in het tijdsbestek tussen het uitvoeren van het onderzoek en de periode voor bestuurlijk hoor- en wederhoor.

Andere nuanceringen hebben betrekking op het sturingsprincipe van de gemeente. De leidende gedachte is 'high trust, high penalty'. De Rekenkamer heeft begrip voor deze gedachte en is zeker geen voorstander van nodeloze bureaucratie. Ook onderschrijft de Rekenkamer het belang van medewerkers die zelf verantwoordelijk handelen. Echter, de BIG-norm, waaraan de gemeente getoetst is, is er niet voor niets. Deze is gebaseerd op best practices op het gebied van informatiebeveiliging. Hiervan afwijken kan, maar het moet wel uitlegbaar zijn. De Rekenkamer blijft bij haar standpunt dat hiervoor een uitgebreidere motivering noodzakelijk is.

De Rekenkamer waardeert de positieve benadering van de aanbevelingen door het College. Veel aanbevelingen zijn reeds onderhanden of worden op korte termijn geïmplementeerd. Ook is de Rekenkamer verheugd dat het College de conclusies een aanbevelingen rondom de wisselwerking tussen raad en college serieus neemt en reeds actie heeft ondernomen door themabijeenkomsten in te plannen. Daarbij wil de Rekenkamer meegeven dat ook van de Gemeenteraad een proactieve houding nodig is om de wisselwerking te verbeteren.

BIJLAGE 1: BESTUDEERDE DOCUMENTEN

Achtergrondinformatie:

- Tactische baseline informatiebeveiliging Nederlandse gemeenten

Roosendaal specifiek:

- Informatieveiligheidsbeleid 2017-2020, Deel 1 t/m 3
- Informatieveiligheidsbeleid 2017-2020, adviesnota
- Actieplan informatieveiligheid 2017
- Stappenplan datalek 2017
- Beslisboom datalekken
- Persoonsinformatie en privacy, Roosendaal op weg naar Wbp-proof en AVG voorbereid. Rapport inventarisatie persoonsgegevens en toetsing aan privacykader, BMC, november 2016
- Informatieveiligheidsanalyse, gemeente Roosendaal, oktober 2016
- GAP-analyse Gemeente Roosendaal (okt 2016) incl. prioritering verbeteracties 2017
- Uittreksel en managementrapportage, Zelfevaluatie BRP van de gemeente Roosendaal, 2017
- ENSIA rapportage, inclusief bijlagen, april 2018
- Dienstverleningsovereenkomst ICT West-Brabant West (gemeenschappelijk regeling ICT)
- Verwerkersovereenkomst ICT West-Brabant West met Gemeente Roosendaal
- Rapport, Audit op de ENSIA, collegeverklaring 2017, SafeHarbour
- Privacyverklaring Gemeente Roosendaal (https://roosendaal.nl/privacyverklaring) bestaande uit volgende documenten:
  - Privacybeleid
  - Privacyreglement
  - Sociaal domein privacybeleid
  - Privacyprotocol gegevensverwerking jeugdhulp
  - Privacyprotocol gegevensverwerking maatschappelijke ondersteuning
- Lijst van incidenten
- Schriftelijk vragen van de raad: https://raad.roosendaal.nl/Documenten/Schriftelijke-vraag
- Kadernota's, begrotingen en jaarverslagen gemeente Roosendaal: https://raad.roosendaal.nl/Documenten/
- Risicoanalyse informatieveiligheid 2018