REKENKAMERCOMMISSIE BERGEN

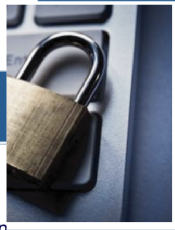
Quick scan Informatiebeveiliging

Computersystemen gemeente Arnhem gevoelig voor hackers
De beveiliging van computersystemen die de gemeente Arnhem gebruikt is zo lek als een mandje. Een ingehuurde hacker verkreeg heel gemakkelijk de rechten van een systeembeheerder en kon zo alle privacygevoelige informatie van burgers, ambtenaren en zelfs burgemeester en wethouders bewerken.

'Gemeente Rotterdam lekt privégegevens van probleemjongeren'
De gemeente Rotterdam heeft per ongeluk privégegevens van probleemjongeren gedeeld met andere probleemjongeren.

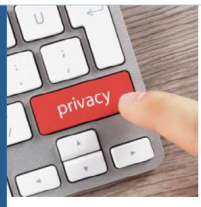
Gemeente Assen lekt gegevens van honderden inwoners met gebiedsverbod
De gemeente Assen heeft de persoonsgegevens van 530 inwoners met een gebiedsverbod gelekt. Het gaat daarbij om mensen met lopende en inmiddels verlopen gebiedsverboden en anderen die een waarschuwing hebben ontvangen.

Duizenden Nederlandse ID-bewijzen jarenlang openbaar door datalek
Kopieën van duizenden Nederlandse identiteitsdocumenten stonden jarenlang op een onbeveiligde dataserver, waardoor ze in te zien waren voor iedereen. Tussen de documenten zaten ook identiteitsbewijzen van Defensie.



Duizenden dossiers van kwetsbare kinderen gelekt bij Bureau Jeugdzorg
Dossiers van duizenden kinderen zijn gelekt door een fout bij Bureau Jeugdzorg Utrecht. Dat blijkt uit documenten in handen van RTL Nieuws.

'Nederlanders melden meeste datalekken in Europa'
Nederland maakte de meeste meldingen van datalekken sinds de invoering van de Europese privacywet (AVG). In totaal maakten Nederlanders 15.400 keer melding van een inbreuk op hun digitale gegevens, significant meer dan Duitsland (12.600) en het Verenigd Koninkrijk (10.600).



Toezichthouder krijgt twintigduizend klachten in eerste jaar privacywet
De Autoriteit Persoonsgegevens (AP) heeft van 1 januari tot 1 mei negenduizend klachten ontvangen over vermoedelijke privacyschendingen door bedrijven en organisaties. Dat meldt de toezichthouder vrijdag op zijn website.

gemeente BERGEN Limburg

Rekenkamercommissie
gemeente Bergen

d.d. 14 november 2019

REKENKAMERCOMMISSIE BERGEN

Aan de Raad van de gemeente Bergen (L)

Datum: 14 november 2019
Ons kenmerk: -

Onderwerp: ERRATUM bij het rapport
"Quick scan informatiebeveiliging"

Geachte leden van de gemeenteraad,

Helaas blijkt het rapport een onjuistheid te bevatten. Op pagina14 van het rapport staat:
*Indien de gemeenteraad tijdens de begrotingsbehandeling besluit over te gaan tot uitbesteding van ICT taken, blijft er sprake van een krappe tijdspanne om alle benodigde maatregelen te treffen om deze uitbesteding binnen de periode van november **2018** tot mei **2019** te kunnen realiseren.*
Deze zin moet luiden:
*Indien de gemeenteraad tijdens de begrotingsbehandeling besluit over te gaan tot uitbesteding van ICT taken, blijft er sprake van een krappe tijdspanne om alle benodigde maatregelen te treffen om deze uitbesteding binnen de periode van november **2019** tot mei **2020** te kunnen realiseren.*

Met vriendelijke groet,

De rekenkamercommissie van de gemeente Bergen (L),

W. Elemans, H. Meeuwsen, S. Joosten

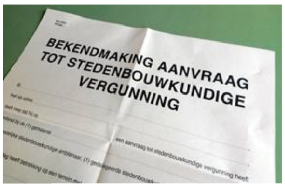
INHOUDSOPGAVE

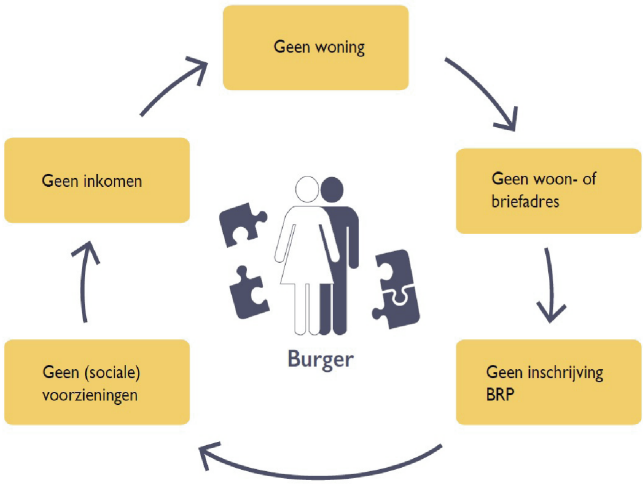
1 Aanleiding

Gemeenten verwerken en beschikken over steeds meer gegevens van burgers op een groot aantal uiteenlopende terreinen. Denk daarbij aan gegevens die nodig zijn voor bijvoorbeeld het verlenen van een parkeervergunning, de afgifte van identiteitsdocumenten, de aangifte van geboorte of overlijden of de aanvraag van bijzondere bijstand of een Wmo-voorziening. Gemeenten beheren en verwerken meer en meer persoonlijke en gevoelige data. Zeker sinds zij er zoveel taken in het sociale domein bij hebben gekregen.

Gegevensverwerking binnen een gemeente

Basisregistraties
Adressen en gebouwen (BAG) Grootschalige Topografie (BGT)





Basisregistratie Personen (BRP)

Paspoorten en Nederlandse identiteitskaarten

Basisregistratie Structuur Uitvoering Werk en Inkomen

Uit berichten in de media blijkt dat de gemeenten daarbij kwetsbaar zijn. Verlies van gegevens(dragers) zoals USB-sticks, inbraak in informatiesystemen en het onzorgvuldig of oneigenlijk gebruik van deze gegevens kan grote schade toebrengen aan overheden, burgers en/of bedrijven en instellingen. Dagelijks lezen we in de media over zaken die in dit kader fout zijn gegaan. Het kan daarbij gaan om een menselijke fout, een technische fout, maar ook om fraude met of diefstal van gegevens of opzettelijke manipulatie van data. Voor hackers is informatie letterlijk geld waard: er kan bijvoorbeeld misbruik worden gemaakt van dergelijke gegevens om goederen te bestellen op kosten van een ander, geld af te persen of identiteitsfraude mee te plegen. Ook informatie over voorgenomen besluiten van een gemeente kunnen voor derden veel geld waard zijn als deze voortijdig uitlekt. Verder zien we de laatste jaren een toename van het aantal cyberaanvallen.

Burgers, bedrijven, instellingen en organisaties in Bergen moeten erop kunnen vertrouwen, dat persoonsgegevens en andere gevoelige informatie in goede handen zijn bij de gemeente Bergen, dat deze gegevens correct zijn en op de juiste wijze worden verwerkt en bewaard. In dat kader is informatiebeveiliging van essentieel belang. Hierbij staan vertrouwelijkheid, integriteit en beschikbaarheid van de onderliggende (persoons)gegevens centraal.
Ook de gemeenteraad heeft hierin een rol. Hij zal willen weten hoe dat zit binnen de gemeente Bergen. Een logische vraag is dan ook: Hoe veilig zijn al deze persoonsgegevens en andere gevoelige informatie in handen bij de gemeente Bergen?

De Rekenkamercommissie Bergen (RKB) heeft besloten een quick scan uit te voeren naar de stand van zaken rondom Informatiebeveiliging binnen de gemeente Bergen (L). De onderzoeksopzet (zie bijlage) is in september 2018 voorgelegd aan het presidium. Dit heeft niet geleid tot wijzigingen in de opzet.

Leeswijzer
Deze notitie is als volgt opgebouwd. In hoofdstuk 2 zullen wij de opzet van deze quick scan omschrijven. In hoofdstuk 3 gevolgd door een korte toelichting op het onderzoeksonderwerp Informatiebeveiliging. In hoofdstuk 4 worden vervolgens de uitkomsten van het onderzoek toegelicht en we sluiten deze notitie af met conclusies hoofdstuk 5 en aanbevelingen in hoofdstuk 6.

2 Opzet quick scan

2.1 Doelstelling van de quick scan

De RKB wil met de quick scan een peilstok in de gemeentelijke organisatie steken, om zicht te krijgen op de actuele stand van zaken rondom informatiebeveiliging. Dit alles met als doel de informatieveiligheid op een (nog) hoger niveau te tillen.

Op de volgende vier deelvragen wil de rekenkamercommissie met de quick scan duidelijkheid verkrijgen:
1. Hoe staat het met de bekendheid van de Baseline Informatiebeveiliging Gemeenten[1] en de Algemene Verordening Gegevensbescherming binnen de gemeentelijke organisatie? Hoe is/wordt dit toegepast?
2. Is er een beveiligingsorganisatie en zo ja hoe is de organisatie op beveiligingsgebied ingericht?
3. Is de verantwoordelijkheid bestuurlijk en ambtelijk belegd en zo ja hoe?

[1] Vanaf 1 januari 2020 wordt de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de Baseline Informatiebeveiliging Gemeenten.

4. Is de organisatie qua informatieveiligheid klaar voor de toekomst? En daaraan gekoppeld is er voldoende duidelijkheid over rollen etc. van onder meer de security officer(s), de beveiligingscoördinator?

2.2 Het normenkader en de beoordelingscriteria

De bevindingen in dit onderzoek zijn getoetst aan een normenkader. Dit normenkader bestaat uit:

- De richtlijnen zoals opgenomen in de Wet bescherming persoonsgegevens en zijn opvolger de Algemene Verordening Gegevensbescherming, inclusief de meldplicht datalekken.
- De beveiligingsmaatregelen zoals omschreven in de Baseline Informatiebeveiliging Gemeenten.
- Specifieke normensets die door de Rijsoverheid zijn opgelegd aan gemeenten, zoals o.a. in de Eenduidige Normatiek Single Information Audit (ENSIA).

2.3 Werkwijze bij de uitvoering van de quick scan

Naast het bestuderen van de relevante documenten zijn met veertien sleutelfunctionarissen (groeps)interviews gepland[2]. Het betreft de volgende sleutelfunctionarissen[3]:

- De portefeuillehouder Informatiebeveiliging (het college van B&W is integraal verantwoordelijk voor de beveiliging van de informatie binnen de werkprocessen van de gemeente).
- De plaatsvervangend algemeen directeur (de directie is verantwoordelijk voor kaderstelling en sturing), tevens voorzitter van de werkgroep informatiebeveiliging.
- De voormalig Adviseur informatiebeveiliging[4] (verantwoordelijk voor het implementeren van en toezicht houden op het informatiebeveiligingsbeleid binnen de gemeente), tevens voormalige beveiligingsbeheerder (verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van informatieveiligheid van SUWINET) en voormalige functionaris gegevensbescherming (toezicht houden op de naleving van de privacywetten en –regels).
- Beveiligingsbeheerders verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van informatieveiligheid op het gebied van:
    - Informatie- en Communicatie Technologie.
    - Personeel & Organisatie.
    - Digitaal Informatie Management.
    - Gemeentelijke Basisadministratie/Basisregistratie personen.
    - Basisregistratie Adressen en Gebouwen.
- Communicatiemedewerker.
- Privacy officers/aspirant Privacy officers (verantwoordelijk voor het vormgeven en bewaken van het privacybeleid binnen de gemeente).
- Functionaris gegevensbeheer (toezicht houden op de naleving van de privacywetten en –regels, het inventariseren en behouden van gegevensverwerkingen en het afhandelen van vragen en klachten van mensen binnen en buiten de organisatie).

Verder hebben wij op basis van onze eigen waarnemingen vastgesteld hoe een en ander binnen de gemeente Bergen (L) georganiseerd is. Op basis van deze uitkomsten worden conclusies getrokken en aanbevelingen gedaan.

[2] Het interview met de portefeuillehouder heeft helaas tweemaal geen doorgang kunnen vinden, waarna deze de vragen schriftelijk heeft beantwoord.
[3] De griffie is niet betrokken in deze quick scan. Voor de publicatie van persoonsgegevens door de raad heeft de raad op 2 juli 2019 een gedragsprotocol vastgesteld.
[4] Officiële benaming van de adviseur informatieveiligheid is de Chief Information Security Officer (CISO)

2.4 Beperkingen van de quick scan

Het betreft hier een quick scan met een select aantal interviews op basis van een beperkte doorsnede door de gemeentelijke organisatie. Een quick scan is een beperkt onderzoek binnen een organisatie of van een bepaald product. Het doel is een globale evaluatie waarbij de belangrijkste kansen, knelpunten en verbetermogelijkheden worden benoemd.[5] Een quick scan is geen uitgebreid onderzoek waarin tot oordeelsvorming kan worden overgegaan. Wij geven slechts antwoord op de gestelde vragen en matigen ons geen oordeel over de kwaliteit en diepgang van alle interne beheersingsmaatregelen rondom informatiebeveiliging die de gemeente Bergen al dan niet heeft getroffen.

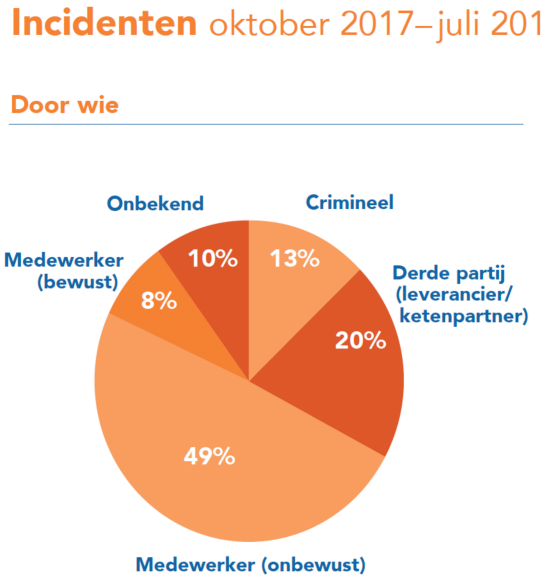
Wij wijzen erop dat, indien deze beperkingen niet van toepassing waren, wellicht andere aandachtspunten zouden zijn geconstateerd die voor rapportering in aanmerking zouden zijn gekomen.

3 Toelichting Informatiebeveiliging

Gemeenten beheren op vele manieren informatie en wisselen die uit binnen de organisatie, maar ook daarbuiten. Met inwoners, ondernemers, ketenpartners en medeoverheden. Hierdoor kunnen gemeenten onder andere hun dienstverlening beter organiseren, de veiligheid van inwoners verbeteren en meer mensen aan het werk helpen. Hierbij past dat de gemeente ook de beveiliging van informatie adequaat organiseert. Informatie moet beschikbaar, actueel, volledig en betrouwbaar zijn en mag alleen door bevoegden zijn in te zien.

3.1 Informatiebeveiliging is risicomanagement

Informatiebeveiliging is veel meer dan ICT alleen. Beveiliging van gegevens en systemen gaat om de mensen in de organisatie, om de manier waarop zij met risico's omgaan. Het gaat om de wijze waarop processen en procedures zijn ingericht, om kennis en bewustzijn. En in de laatste plaats pas om techniek. Dat blijkt uit de gemelde incidenten bij de IBD[6].



[5] De definitie komt uit www.Marketingtermen.nl
[6] IBD is de afkorting voor Informatiebeveiligingsdienst. De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum.

In de periode van oktober 2017 – juli 2018 heeft de IBD 429 incidenten vastgesteld, waarvan de impact in 84% laag was, 12% midden en 4% hoog.[7]
Verreweg de meeste incidenten worden nog steeds veroorzaakt door menselijk handelen doordat medewerkers zich onvoldoende bewust zijn van de gevolgen van kleine menselijke fouten (49%). Informatiebeveiliging begint met een bewuste medewerker.

3.2 Twee invalshoeken: techniek en privacy

Er kan vanuit twee invalshoeken naar bescherming van persoonsgegevens gekeken worden. In de eerste plaats is dat de meer technische invalshoek van de informatiebeveiliging. Hiermee wordt gedoeld op het waarborgen van een samenhangend pakket aan maatregelen bestaande uit beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van de gegevens in de organisatie.

- *Beschikbaarheid*:
  Het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers.
  Een voorbeeld van wat verkeerd kan gaan:
  Het niet beschikbaar zijn van systemen door een stroomuitval of virusaanval waardoor het netwerk 'plat ligt' en medewerkers niet kunnen werken.

- *Integriteit*:
  Het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.
  Een voorbeeld van wat verkeerd kan gaan:
  Gegevens van asielzoekers zijn in 300 verschillende bestanden verzameld. De kans op een verkeerde overname van gegevens wordt hierdoor zeer groot.

- *Vertrouwelijkheid*:
  Het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die daartoe geautoriseerd zijn.
  Een voorbeeld van wat verkeerd kan gaan:
  Het laten slingeren van een USB-stick waarop alle informatie van de cliënten en gezinnen voor de jeugdzorg staat vermeld.

De tweede invalshoek is die van privacy. Daarbij gaat het om regels en de toepassing van regels die bepalen hoe persoonsgegevens mogen worden verzameld en gebruikt. Bijvoorbeeld het vastleggen van de rechten van degenen op wie de informatie betrekking heeft: de burgers.

Privacybeleid en informatiebeveiligingsbeleid moeten er in samenhang voor zorgen dat persoonsgegevens niet in verkeerde handen komen en er geen schade aan burgers kan worden toegebracht.

3.3 Wet en regelgeving

Ten aanzien van Informatiebeveiliging speelt diverse wet en regelgeving een rol zoals:
- de Baseline Informatiebeveiliging Gemeenten (BIG);
- de Algemene Verordening Gegevensbescherming (AVG);
- de Wet datalekken;
- de Eenduidige Normatiek Single Information Audit (ENSIA);
- de organisatorische inbedding van een en ander.

[7] Informatiebeveiligingsdienst (IBD) (2018) Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2019/2020, VNG.

De Baseline Informatiebeveiliging Gemeenten (BIG)
Door de Vereniging Nederlandse Gemeenten (VNG) is op 29 november 2013 een richtlijn opgesteld voor informatiebeveiliging: de BIG. Deze richtlijn is gebaseerd op internationale standaarden voor het borgen van de veiligheid van informatie. Met de BIG hebben gemeenten een hulpmiddel om aan alle eisen ten aanzien van informatiebeveiliging te kunnen voldoen (doelen, resultaten, basisnormen en organisatie van de informatiebeveiliging) en kunnen zij daarmee een goed basisbeveiligingsniveau realiseren.

Vanaf 1 januari 2020 wordt de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines informatiebeveiliging voor Rijk, Gemeenten, Waterschappen en Provincies. De BIO is een 'update' van de nu bestaande BIG. De BIO legt meer nadruk op risicomanagement dan de BIG en de rol van de bestuurder en lijnmanager is ten aanzien van risicomanagement explicieter dan de BIG aangaf. Om daaraan invulling te geven wordt tegelijkertijd met de BIO een handreiking '10 bestuurlijke principes voor informatiebeveiliging' (zie bijlage) van kracht. In 2019 kunnen gemeenten zich voorbereiden op de overgang van de BIG naar de BIO.

Algemene Verordening Gegevensbescherming (AVG)
Per 25 mei 2018 is de AVG voor alle lidstaten van de Europese Unie van toepassing. Dat betekent dat er vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie. Tot 25 mei 2018 was de Wet bescherming persoonsgegevens (Wbp) van kracht. Deze is met het van toepassing worden van de AVG komen te vervallen. Ook de gemeente Bergen moet voldoen aan de AVG. Het kunnen voldoen aan de AVG vergt voor organisaties een gedegen en intensieve voorbereiding. De AVG verplicht de gemeente passende technische en organisatorische maatregelen te nemen om te waarborgen dat de opslag, verwerking en gebruik van persoonsgegevens in overeenstemming met de AVG wordt uitgevoerd.

Melden datalekken
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek constateren. En soms moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). Met ingang van 25 mei 2018 is deze wettelijke verplichting onderdeel van de AVG.

ENSIA
Eenduidige Normatiek Single Information Audit (ENSIA), ingaande 1 juli 2017, heeft tot doel het verantwoordingsproces over informatiebeveiliging bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning- & Controlcyclus. De BIG is nu de kern van de verantwoording over informatiebeveiliging aan de gemeenteraad. Met betrekking tot ENSIA verantwoordt het College zich vanaf 1 januari 2018 richting raad over de stand van zaken van de informatiebeveiliging. De verantwoordingssystematiek ENSIA zal ook worden bijgewerkt naar de BIO.

3.4 Verantwoordelijkheden in informatiebeveiliging

College van burgemeester en wethouders (beslissende rol)
Het college van burgemeester en wethouders is integraal verantwoordelijk voor de beveiliging van de informatie binnen de werkprocessen van de gemeente. Daarnaast stelt het college kaders vast voor informatiebeveiliging op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders.

De directie (sturende rol)
De directie is verantwoordelijk voor kaderstelling en sturing. Zij stuurt op concernrisico's, controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden. Ook evalueert de directie periodiek de beleidskaders en stelt deze waar nodig bij en ziet er op toe dat iedereen zich aan de afspraken houdt.

Lijnmanagement (vragende rol)
De lijnmanagers van de afdelingen binnen de gemeente zijn verantwoordelijk voor de integrale beveiliging van hun organisatieonderdeel. Dat doen zij door op basis van een expliciete risicoafweging betrouwbaarheidseisen voor informatiesystemen vast te stellen (classificatie). Daarnaast is de lijnmanager verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen. Hij stuurt op beveiligingsbewustzijn, betrouwbaarheidseisen en naleving van regels en richtlijnen (gedrag en risicobewustzijn). Tenslotte rapporteert hij over compliance aan wet- en regelgeving en specifiek beleid van de gemeente in managementrapportages.

De gemeentelijke Serviceorganisatie of gelijkwaardig (ICT, HR, bedrijfsvoering, etc.) (uitvoerende rol)
De organisatieonderdelen ICT, P&O, Bedrijfsvoering, Facilitaire zaken (gebouwenbeheer) zijn verantwoordelijk voor de uitvoering van beveiligingsmaatregelen.

De Chief Information Security Officer (CISO)
De CISO (ook wel beveiligingscoördinator genoemd) is dé spin in het web als het gaat om informatiebeveiliging binnen de gemeente. Hij is verantwoordelijk voor het implementeren van en toezicht houden op het informatiebeveiligingsbeleid binnen de gemeente. De CISO speelt een centrale rol in het beheren van alle processen die daarmee te maken hebben en moet daarbij voldoen aan de Baseline Informatiebeveiliging Gemeenten (BIG).

De Privacy Officer (PO)
De PO (ook wel juridisch adviseur privacy genoemd), is verantwoordelijk voor het vormgeven en bewaken van het privacybeleid binnen de gemeente. Daarnaast kan de PO ondersteunen bij het in kaart brengen van risico's door bijvoorbeeld een Privacy Impact Assessment (PIA)[8] uit te voeren. Ook kan hij een implementatieplan opstellen en speelt hij een belangrijke rol op de werkvloer. Net als de CISO heeft hij een adviserende rol richting de vakafdelingen en kan hij als vraagbaak dienen.

Functionaris Gegevensbescherming (FG)
Sinds het van kracht worden van de Algemene Verordening Gegevensbescherming op 25 mei 2018 zijn alle overheidsorganisaties verplicht een FG aan te stellen. De FG is verantwoordelijk voor het toezicht houden op de naleving van de privacywetten en –regels, het inventariseren en bijhouden van gegevensverwerkingen en het afhandelen van vragen en klachten van mensen binnen en buiten de organisatie. Daarnaast kan hij ondersteunen bij het ontwikkelen van interne regelingen, het adviseren over privacy op maat én het leveren van input bij het opstellen of aanpassen van gedragscodes.

[8] Een Privacy Impact Assessment (PIA) is een instrument om bij ontwikkeling van beleid, en de daarmee gepaard gaande wetgeving of bouw van ICT-systemen en aanleg van databestanden, privacy risico's in kaart te brengen.

4 Uitkomsten quick scan

4.1 Inleiding

Op de volgende vier deelvragen wil de rekenkamercommissie met de quick scan duidelijkheid verkrijgen:

1. Hoe staat het met de bekendheid van de Baseline Informatiebeveiliging Gemeenten en de Algemene Verordening Gegevensbescherming binnen de gemeentelijke organisatie? Hoe is/worden deze toegepast?
2. Is er een beveiligingsorganisatie en zo ja hoe is de organisatie op beveiligingsgebied ingericht?
3. Is de verantwoordelijkheid bestuurlijk en ambtelijk belegd en zo ja hoe?
4. Is de organisatie qua informatieveiligheid klaar voor de toekomst? En daaraan gekoppeld: is er voldoende duidelijkheid over rollen etc. van onder meer de security officer(s), de beveiligingscoördinator?

4.2 Bekendheid van de Baseline Informatiebeveiliging Gemeenten en de Algemene Verordening Gegevensbescherming

Hoe staat het met de bekendheid van de Baseline Informatiebeveiliging Gemeenten en de Algemene Verordening Gegevensbescherming binnen de gemeentelijke organisatie? Hoe is/worden deze toegepast?

Op basis van de door ons verzamelde informatie (documenten en interviews) kunnen we onderstaande feiten vaststellen met de beperkingen zoals eerder aangegeven:

- De medewerkers die dagelijks met persoonsgegevens werken zijn bekend met de Baseline Informatiebeveiliging Gemeenten[9] (BIG). Zij delen ook informatie met elkaar in het overleg veiligheid. Ook tijdens de interviews toonden deze sleutelfiguren een grote betrokkenheid bij het onderwerp en een positieve houding ten opzichte van het verder verbeteren van Informatiebeveiliging binnen de gemeente Bergen.[10]
- De beveiligingsbeheerders en de Adviseur informatiebeveiliging[11] vervullen een actieve rol in het verhogen van kennis en bewustzijn bij met name hun directe collega's. Door hen aan te spreken waar nodig en het goede voorbeeld te geven. De kennis en het bewustzijn op het gebied van de Baseline Informatiebeveiliging gemeenten bij de overige medewerkers is beperkt.
- Bij de start van onze quick scan (april 2019) heeft het college van burgemeester en wethouders het privacybeleid voor de gemeente vastgesteld waarin is opgenomen hoe de gemeente omgaat met persoonsgegevens en hoe de rollen, taken en verantwoordelijkheden zijn belegd. Aangezien de gemeente Bergen het privacybeleid in het kader van de AVG[12] pas recent heeft vastgesteld, is het logisch dat dit nog niet algemeen bekend is binnen de organisatie.
- De kennis en het risicobewustzijn onder de medewerkers worden in verschillende audits door de jaren heen genoemd als belangrijke aandachtspunten voor verbetering. Ook tijdens de gevoerde gesprekken worden deze als belangrijke verbeterpunten genoemd.

[9] BIG: Richtlijn voor Informatiebeveiliging opgesteld door de VNG.
[10] Dit blijkt bijvoorbeeld uit het feit dat na de interviews en vooruitlopend op het rapport van de rekenkamercommissies diverse maatregelen zijn getroffen. Bijvoorbeeld het advies op te volgen om het risico op beschadigde netwerkapparatuur te verkleinen door de patchkast op te ruimen, de er boven hangende airco periodiek te laten onderhouden en een lekbak te plaatsen. Maar ook voornemen om een ambassadeur per afdeling aan te wijzen, het inrichten van een maandelijkse rapportage op het gebied van privacy en toetsing clear desk policy met terugkoppeling aan het MT.
[11] In dit rapport wordt met Adviseur informatiebeveiliging de Chief Information Security Officer (CISO) bedoeld.
[12] AVG: Algemene verordening Gegevensbescherming.

- Volgens de BIG is informatiebeveiliging in de eerste plaats de verantwoordelijkheid van de lijnmanager. Uit documenten en gesprekken blijkt dat verantwoordelijkheid van lijnmanagers nog niet concreet is ingevuld en het belang van informatiebeveiliging beperkt wordt uitgedragen. Ook in de Ensia assurancerapporten Suwinet over 2017 en 2018 worden [13] aanbevelingen gedaan aan het management om te zorgen voor voldoende kennis en bewustzijn op het gebied van informatiebeveiliging.
- Op dit moment is er geen algemeen communicatieplan gericht op het vergroten van de kennis en bewustzijn van informatiebeveiliging. Wel is er sinds april 2019 een privacyreglement voor medewerkers en is gestart met een voorlichtingscampagne om medewerkers te informeren over de inhoud en eisen van de Algemene Verordening Gegevensbescherming, inclusief de werkwijze ten aanzien van het voorkomen van en het handelen bij datalekken.

4.3 Beveiligingsorganisatie

Is er een beveiligingsorganisatie en zo ja hoe is de organisatie op beveiligingsgebied ingericht?

Op basis van de door ons verzamelde informatie (documenten en interviews) kunnen we onderstaande feiten vaststellen met de beperkingen zoals eerder aangegeven:

- Gemeente Bergen beschikt over een integraal Informatieveiligheidsbeleid waarin niet alleen de strategische uitgangspunten en doelstellingen zijn opgenomen, maar waarin tevens de organisatie van de informatieveiligheidsfunctie, verantwoordelijkheden, taken en bevoegdheden zijn benoemd. Dit beleid is niet gebaseerd op een systematische analyse en assessment van de risico's. Een RI&E en GAP[14], informatieveiligheidsanalyse en actieplan zijn wel opgesteld maar eerst nadat het beleid is vastgesteld en zijn niet ter besluitvorming aan het college van burgemeester en wethouders voorgelegd. Over de tussenstand van het actieplan van januari 2017 is niet meer tussentijds gerapporteerd. Inmiddels is gestart met een GAP analyse en bestaat het voornemen om op basis daarvan het actieplan bij te stellen en het beleidsplan evalueren. Evaluatie en bijstelling van het integraal Informatieveiligheidsbeleid is gepland in de tweede helft van 2019.
- Het college van burgemeester en wethouders heeft in april 2019 het privacybeleid voor de gemeente Bergen vastgesteld. De AVG is per 25 mei 2018 van kracht wat betekent dat de gemeente Bergen in de tussenliggende periode niet aan de eisen van deze wetgeving voldeed. Personele wisselingen worden hiervoor als verklaring gegeven.
- De organisatie op beveiligingsgebied is op dit moment volop in beweging. Eerst op 16 april 2019 zijn de functieomschrijvingen van de Functionaris gegevensbescherming (FG) en Adviseur informatiebeveiliging (CISO) vastgesteld. Niet lang daarna zijn de FG, en de Privacy adviseur (PO)[15] benoemd. De functie van CISO is uit besteed bij ICT Noord- en Midden-Limburg.
- Over het algemeen blijkt uit de zelfevaluaties van de verschillende basisregistraties[16] dat de gemeente voldoet aan de veiligheidseisen op deze specifieke terreinen.

[13] Op basis van de resultaten uit de zelfevaluatie vragenlijst en de Collegeverklaring informatiebeveiliging wordt een IT-audit uitgevoerd en een Assurance rapport opgeleverd.
[14] RI&E staat voor risico-inventarisatie en –evaluatie. Met een risico-inventarisatie worden organisatierisico's op een rij gezet en de risico's voor personeel en organisaties worden teruggedrongen. Ook het financiële risico. Een GAP- en impactanalyse van de informatiebeveiliging geeft een algemeen inzicht in de aandachtsgebieden voor informatiebeveiliging en de mogelijke verbeterpunten op specifieke onderdelen.
[15] Officiële benaming voor Privacy adviseur is Privacy Officer (PO).
[16] Personen (BRP) en reisdocumenten, adressen en gebouwen (BAG), grootschalige Topografie (BGT) en Suwinet.

- De samenhang met het algemene veiligheidsbeleid is in de praktijk nog niet doorontwikkeld. Zo is er bijvoorbeeld geen gemeentebreed continuïteitsplan (bij uitval van kritische bedrijfsprocessen) en is de functie van Informatie adviseur (CIO)[17] op dit moment niet ingevuld.
- Binnen de gemeente Bergen is een beveiligingsorganisatie ingericht. Twee tot vier maal per jaar komt het overleg Informatieveiligheid bij elkaar. Daaraan nemen de sleutelfunctionarissen op ambtelijk niveau deel op het terrein van de BIG en AVG.
- Het laatste overzicht van de beveiligingsorganisatie dateert van 23 oktober 2018 (zie bijlage). Het schema moet nog worden bijgesteld. Zo ontbreekt de functie van de Functionaris gegevensbescherming en hebben personele wisselingen in de bezetting van rollen plaats gevonden. Daarnaast vervult het afdelingshoofd Bedrijfsvoering in de praktijk meer rollen in de beveiligingsorganisatie dan uit het schema blijkt. Een aantal daarvan overlappen met de verantwoordelijkheden die de Adviseur informatiebeveiliging heeft.
- Op het gebied van digitale beveiliging zijn veel stappen gezet. Adviezen op het terrein van informatiebeveiliging zijn voor het grootste deel opgevolgd, in uitvoering genomen of staan op de agenda. Het advies om Audit Policies in de Active Directory aan te zetten om b.v. mislukte aanmeldpogingen op te slaan is bewust het niet opgevolgd vanwege performanceproblemen .
- In 2019 wordt een informatiebeveiligingmanagementsysteem (ISMS) gebouwd waarin de rollen zijn beschreven.

4.4 Bestuurlijke en ambtelijke verantwoordelijkheden

Is de verantwoordelijkheid bestuurlijk en ambtelijk belegd en zo ja hoe?

Op basis van de door ons verzamelde informatie (documenten en interviews) kunnen we onderstaande feiten vaststellen met de beperkingen zoals eerder aangegeven:

- De uitgangspunten van de BIG zijn integraal opgenomen in het gemeentebrede informatieveiligheidsbeleid. Risicomanagement is de basis van een goede informatiebeveiliging. In afwijking van de BIG-richtlijnen is het beleidsplan niet gebaseerd op een systematische analyse en assessment van de risico's. Het college van burgemeester en wethouders heeft in het verleden geen keuzes gemaakt over welke risico's zij wel accepteert en welke niet. Er is niet gerapporteerd over de beheersing van deze risico's. Deze informatie is voor de gemeenteraad belangrijk om zijn kaderstellende en controlerende rol inhoud te geven en afspraken te maken over het informatieveiligheidsbeleid met het college van burgemeester en wethouders.
- De zelfevaluaties conform de ENSIA inclusief daarbij behorende Ensia-assurance rapporten worden aan het college van burgemeester en wethouders voorgelegd. Informatiebeveiliging is binnen het college van burgemeester en wethouders niet als specifieke portefeuille bestempeld maar wordt uitgevoerd binnen de portefeuille Informatie en automatisering (inclusief website). Informatiebeveiliging is niet expliciet benoemd als strategisch agendapunt voor het college.
- Op dit moment wordt in de P&C-cyclus niet jaarlijks gerapporteerd over informatiebeveiliging aan de gemeenteraad door bijvoorbeeld een paragraaf Informatieveiligheid op te nemen in het jaarverslag onder Bedrijfsvoering en het onderwerp "informatiebeveiliging" in de gemeenteraad te bespreken. De rapportage aan de gemeenteraad is wel op korte termijn gepland zodat de gemeenteraad beter in staat zal worden gesteld om de kaderstellende en controlerende rol uit te voeren. De ENSIA-verantwoordingsystematiek is nog niet toegelicht in de raad en/of raadscommissie.

[17] De officiële benaming voor Informatie adviseur is Chief Information Officer. De chief information officer (CIO) is binnen een organisatie de hoogste verantwoordelijke op het gebied van de ICT.

- Volgens de BIG is informatiebeveiliging een verantwoordelijkheid van het lijnmanagement (alle afdelingshoofden tezamen) en moeten de kennis en expertise op dat niveau aanwezig zijn. Op dit moment is de kennis en expertise op managementniveau geconcentreerd bij het afdelingshoofd Bedrijfsvoering vanuit zijn centrale rol. Het lijnmanagement in Bergen vervult in de dagelijkse praktijk nog niet de rol die aan hen ook in het beleidsplan informatieveiligheidsbeleid is toebedeeld. De lijnmanagers voelen zich niet verantwoordelijk voor de integrale beveiliging van hun organisatieonderdeel en systemen en sturen nog niet actief op beveiligingsbewustzijn, betrouwbaarheidseisen en naleving van regels en richtlijnen (gedrag en risicobewustzijn) binnen hun afdeling. Uiteraard geldt in dit geval ook voor zover wij dit in deze quick scan hebben kunnen vaststellen. Het voornemen bestaat om dit eigenaarschap voor het einde van 2019 in overleg met de lijnmanagers nader uit te werken en in te vullen.
- Clean desk policy (het schoonhouden van bureaus en vertrouwelijke documenten opbergen), clear screen policy (computersessies niet open laten staan tijdens afwezigheid) zijn gecommuniceerd maar niet iedereen houdt zich daaraan; handhaving door het management is een aandachtspunt.[18] Daarnaast hebben wij uit eigen ervaring geconstateerd dat de alertheid op het binnenlopen en aanwezig zijn van onbevoegden in het gemeentehuis nog geen gemeengoed is binnen de organisatie.
- In het verleden was de rol van de Adviseur informatiebeveiliging redelijk smal ingevuld. Hij was met name belast met het coördineren van de zelfevaluaties en het nemen van gepaste maatregelen op het gebied van de ICT. Hij onderhield geen rechtstreekse contacten met het college of het managementteam. Inmiddels wordt de functie uitgevoerd via inhuur bij ICT- Noord- en Midden-Limburg (8 uur per week) en is er een functieomschrijving vastgesteld waarin onder meer het adviseren van het (lijn)management als specifieke taak is opgenomen.
- Het afdelingshoofd Bedrijfsvoering vervult een centrale rol in de beveiligingsorganisatie. Hij is de voorzitter van de werkgroep Informatiebeveiliging, is de linking pin naar het college van burgemeester en wethouders en het managementteam, is verantwoordelijk voor de uitvoering van de audits en zelfevaluaties en de direct leidinggevende van de meeste medewerkers in de beveiligingsorganisatie. Daarnaast fungeert hij samen met de Adviseur informatiebeveiliging als vertrouwenspersoon bij de melding van incidenten. Het onderbrengen van verschillende rollen bij één persoon is risicovol en tevens omvat het rollen die normaliter tot de verantwoordelijkheid van de Adviseur informatiebeveiliging horen.

4.5 Klaar voor de toekomst?

Is de organisatie qua informatieveiligheid klaar voor de toekomst? En daaraan gekoppeld is er voldoende duidelijkheid over rollen etc. van onder meer de security officer(s), de beveiligingscoördinator?

Op basis van de door ons verzamelde informatie (documenten en interviews) kunnen we onderstaande feiten vaststellen met de beperkingen zoals eerder aangegeven:

- Een grote bedreiging voor de toekomst ten aanzien van informatiebeveiliging in Bergen ligt op het gebied van de ICT. Hoewel op het gebied van digitale beveiliging veel stappen zijn gezet, wordt ook door de accountant KSG in de managementletter 2018 geconstateerd dat de generieke beheersmaatregelen te wensen over laten. Een aantal adviezen die niet veel tijd kosten en het risico op beschadigde netwerkapparatuur kunnen voorkomen, is niet uitgevoerd. Maar met name het feit dat Microsoft vanaf 14 januari 2020 stopt met de ondersteuning van

[18] Inmiddels hebben wij kunnen constateren dat in de periode tussen de gevoerde interviews en de oplevering van dit rapport een clean desk onderzoek heeft plaats gevonden. De PO heeft de opdracht het MT hier een keer per kwartaal over te informeren.

windows 7 en windowsserver 2008 R2, gecombineerd met de beperkte technische performance van de huidige hardware vormt al op korte termijn een verhoogd risico in het kader van informatieveiligheid. Dit wordt nog een keer uitvergroot doordat de mogelijke uitbesteding aan ICT NML vertraagd[19] is. Dit betekent dat, anno nu, de informatiebeveiliging vanaf 2020 (ernstig) gevaar loopt. Inmiddels wordt de uitbesteding van de ICT meegenomen in de begroting van 2020. [20]

- Medio april 2019 is het privacybeleid voor de gehele gemeente vastgesteld. Hoewel dit laat is (de gemeente diende al vanaf 25 mei 2018 aan de AVG te voldoen) is hiermee een belangrijke stap gezet richting AVG-proof zijn als gemeente. De indruk is dat dit onderwerp nu voortvarend wordt opgepakt en er een goed inzicht bestaat in de nog te ondernemen acties.
- De organisatie op beveiligingsgebied is volop in beweging. Dat betekent nieuwe functies en nieuwe mensen. Daarnaast kan op dit moment nog niet worden vastgesteld of het aantal uren dat men aan de uitvoering van de functies kan besteden voldoende is. De drie sleutelposities in het informatiebeveiligingsbeleid zijn pas zeer recent ingevuld (mei 2019). De functie van CISO is uitbesteed bij ICT Noord- en Midden-Limburg, de Functionaris gegevensbeheer heeft weinig tot geen ervaring binnen de gemeentewereld en de privacy-adviseur is ook niet ervaren op dit terrein. Deze laatste twee worden gecoacht door de externe ondersteuning die is ingehuurd in het kader van het AVG-proof maken van de organisatie. Ook zal ingezet worden op opleiding van de medewerkers.
- Bergen is in het bezit is van alle registers en procedures die verplicht zijn gesteld onder de AVG maar nog niet AVG-proof. Hier wordt in 2019 flink op ingezet. Hierbij kan gedacht worden aan een voorlichtingscampagne, het opstellen van domein specifiek privacybeleid, inrichten van werkprocessen, register van verwerkingsactiviteiten, bekendheid en toepassen van het meewegen van privacybelangen in de besluitvorming over de ontwikkeling van producten, diensten of wetgeving (DPIA)[21], etc. Het voornemen bestaat om de organisatie, met uitzondering van het systeem (dat is voorzien voor 2022) aan het einde van 2019 AVG-proof te hebben.
- De vraag die opkomt is of de gemeente Bergen in staat is alles zelf te blijven doen of dat de gemeente gelet op de beperkte omvang van het ambtelijk apparaat samenwerking moet gaan zoeken. Zeker aangezien de functies Functionaris Gegevensbeheer, Privacy-adviseur en Adviseur informatiebeveiliging geen fulltime functies betreffen en bij voorkeur niet gecombineerd mogen worden. Ook de vervanging ten aanzien van de beveiligingsbeheerders zoals bijvoorbeeld BGT[22] kan hierin mee worden genomen. Afweging daarbij is welke functie(s) de gemeente 'in huis' wil houden en welke functies in een samenwerkingsverband of via uitbesteding zouden kunnen worden vervuld.
- Ook op het HRM-terrein is men druk doende om de omgang met persoonsgegevens van medewerkers aan te passen aan de privacyregelgeving. Speciale aandacht verdient daarbij de actualiteit van personeelsoverzichten en werkwijze/handhaving ten aanzien van de thema's Bring Your Own Device[23], Social media, Thuiswerken en Clean Desk en Clear Screen.
- Over hoe wordt omgegaan met de gegevens van externen zijn (nog) geen afspraken vastgelegd.

[19] Op dit moment is niet zeker of deze uitbesteding doorgaat. Aan de voorgenomen uitbesteding aan ICT NML ligt geen raadsbesluit ten grondslag. De raad heeft het college verzocht alternatieven te onderzoeken.
[20] Inmiddels ligt er een rapportage van een extern bureau die wordt meegenomen in de begroting van 2020.Het voornemen is dat indien de raad begin november 2019 akkoord gaat met de aanbevelingen direct gestart wordt met de voorbereidingen. Het management verwacht dat de uitbesteding dan in mei 2020 gerealiseerd kunnen hebben. Voor de ondersteuning van windows 2007 wordt er voor de tussenliggende periode een supportcontract afgesloten.
[21] DPIA: Data Protection Impact Assessment: een instrument om vooraf privacyrisico's van een gegevensverwerking in kaart te brengen, om maatregelen te kunnen nemen om de risico's te verkleinen.
[22] BGT: Basisregistratie Grootschalige Topografie: een digitale kaart van Nederland waarop gebouwen, wegen, waterlopen, terreinen en spoorlijnen eenduidig zijn vastgelegd.
[23] Medewerkers hun eigen smartphones, laptops en tablets laten gebruiken heet *Bring Your Own Device* (BYOD).

- Tot mei van dit jaar was slechts 1 incident gemeld, dat alert is opgepakt. Dat is relatief gezien een laag aantal meldingen. De vraag die dit oproept is of dit lage aantal het gevolg is van het feit dat zich geen andere incidenten hebben voorgedaan of dat deze wel hebben plaats gevonden, maar niet gemeld zijn. Tijdens een phishingtest[24] is gebleken dat medewerkers bang zijn om een incident te melden. Dit is een obstakel om te komen tot een lerende organisatie op het gebied van informatiebeveiliging. Daarbij hoort een cultuur waarin het geen schande is als men een keer op een linkje geklikt heeft.

5 Conclusies

In algemene zin hebben wij geconstateerd dat de gemeentelijk organisatie op dit moment veel inzet pleegt op het terrein van Informatiebeveiliging. Bergen is in het bezit is van alle registers en procedures die verplicht zijn gesteld onder de AVG, maar nog niet AVG-proof. Vanaf april 2019 is privacybescherming voortvarend opgepakt en erop gericht om voor het grootste deel AVG-proof te zijn voor 2020. Ook de evaluatie en herijking van het Integrale informatieveiligheidsplan is in 2019 voorzien.

Tevens hebben wij tijdens de interviews ervaren dat de sleutelfiguren op het gebied van Informatiebeveiliging een grote betrokkenheid bij het onderwerp tonen en een positieve houding ten opzichte van het verder verbeteren van Informatiebeveiliging binnen de gemeente Bergen. Dit blijkt mede uit het feit dat in de periode tussen de gevoerde interviews en de totstandkoming van dit rapport al diverse maatregelen ambtelijk zijn opgepakt en uitgevoerd.

In de volgende paragrafen vindt u de antwoorden op de verschillende deelvragen.

5.1 Bekendheid van de Baseline Informatiebeveiliging Gemeenten en de Algemene Verordening Gegevensbescherming

De medewerkers die dagelijks met persoonsgegevens werken zijn bekend met de Baseline Informatiebeveiliging Gemeenten, maar de kennis en het risicobewustzijn bij de overige medewerkers is beperkt. Daarnaast wordt het belang van informatiebeveiliging door het management beperkt uitgedragen. Dit voor zover wij hebben kunnen vaststellen tijdens het uitvoeren van deze quick scan.
De gemeente Bergen heeft het privacybeleid in het kader van de AVG pas recent vastgesteld en derhalve is dit nog geen gemeengoed binnen de organisatie. Wel is inmiddels gestart met een voorlichtingscampagne om medewerkers hierover te informeren.

5.2 Beveiligingsorganisatie

Binnen de gemeente Bergen is op ambtelijk niveau een beveiligingsorganisatie ingericht. Twee tot vier maal per jaar komt het overleg Informatieveiligheid bij elkaar. Daaraan nemen de sleutelfunctionarissen deel op het terrein van de Baseline Informatiebeveiliging Gemeenten en de Algemene Verordening Gegevensbescherming. Het schema van de beveiligingsorganisatie dateert van 23 oktober 2018 en is niet meer up-to-date.

[24] Phishing is een samentrekking tussen de woorden fishing (vissen) en phreaking (computerfraude). Het wordt omschreven als het 'vissen naar gegevens'. Er wordt dan ook naar persoonlijke gegevens gevist. Met een phising test je medewerkers en maak je hen weerbaar tegen een phishing-aanval.

Het integraal Informatieveiligheidsbeleid is niet gebaseerd op een systematische analyse en assessment van de risico's. Evaluatie en bijstelling van het Informatieveiligheidsbeleid is gepland in de tweede helft van 2019. De samenhang met het algemene veiligheidsbeleid is in de praktijk nog niet doorontwikkeld. Informatiebeveiliging is nu nog geen onderdeel van de reguliere planning- en control cyclus, maar de voorbereidingen hiervoor worden getroffen.

5.3 Bestuurlijke en ambtelijke verantwoordelijkheden

De verantwoordelijkheid voor informatiebeveiliging is zowel bestuurlijk als ambtelijk belegd. Informatiebeveiliging is binnen het college van burgemeester en wethouders niet als specifieke portefeuille bestempeld maar wordt uitgevoerd binnen de portefeuille Informatie en automatisering (inclusief website).
In april/mei 2019 is de beveiligingsorganisatie opnieuw ingericht. Functieomschrijvingen zijn vastgesteld, een Privacy-adviseur en een Functionaris gegevensbescherming zijn benoemd. Daarnaast is ervoor gekozen om de functie van Adviseur informatiebeveiliging (CISO), dé spin in het web met betrekking tot informatiebeveiliging binnen de gemeente, uit te besteden bij ICT Noord- en Midden-Limburg voor 8 uur per week. Het hoofd Bedrijfsvoering vervult meerdere rollen binnen de beveiligingsorganisatie, wat risico's met zich mee brengt. Daarnaast zijn de lijnmanagers binnen de gemeentelijke organisatie in de dagelijkse praktijk nog niet verantwoordelijk voor de integrale beveiliging van hun organisatieonderdelen en systemen en sturen dezen nog niet actief op gedrag en risicobewustzijn. Het voornemen bestaat om dit eigenaarschap voor het einde van 2019 in overleg met de lijnmanagers nader uit te werken en in te vullen.
Omdat het beleidsplan niet is gebaseerd op een systematische analyse en assessment van de risico's, heeft het college van burgemeester en wethouders ook geen keuzes gemaakt over welke risico's zij wel accepteert en welke niet en daarover gerapporteerd. Aangezien deze informatie ontbreekt, wordt de gemeenteraad onvoldoende in staat gesteld om haar kaderstellende en controlerende rol te vervullen op het gebied van informatiebeveiliging.

5.4 Klaar voor de toekomst?

Informatiebeveiliging kampt in veel gemeenten (politiek, bestuur en management) met een imagoprobleem. Zo ook in de gemeente Bergen. Informatiebeveiliging draagt niet direct en zichtbaar bij aan de dienstverlening aan inwoners en ondernemers, maar wordt gezien als bijzaak, en soms zelfs als drempel of last. Terwijl de gevolgen van incidenten juist ook voor de bedrijfsvoering van de gemeente groot kunnen zijn.
De organisatie is nog niet klaar voor de toekomst. Zo is de gemeente Bergen op dit moment nog niet AVG-proof, maar hier wordt vanaf april 2019 wel stevig en voortvarend op ingezet.
Wellicht de grootste bedreiging voor de toekomst ligt, anno nu, op het gebied van de ICT. Het feit dat Microsoft vanaf 14 januari 2020 stopt met de ondersteuning van windows 7 en windows server 2008 R2, gecombineerd met de beperkte technische performance van de huidige hardware en het feit dat de mogelijke uitbesteding aan ICT NML vertraagd is, betekent dat, zonder ingrijpen, de informatiebeveiliging vanaf 2020 gevaar loopt. Indien de gemeenteraad tijdens de begrotingsbehandeling besluit over te gaan tot uitbesteding van ICT taken, blijft er sprake van een krappe tijdspanne om alle benodigde maatregelen te treffen om deze uitbesteding binnen de periode van november 2018 tot mei 2019 te kunnen realiseren.
Daarnaast zijn de drie sleutelposities in het informatiebeveiligingsbeleid pas zeer recent ingevuld (mei 2019) met relatief onervaren medewerkers. Op dit moment kan nog niet worden vastgesteld of het aantal uren dat men aan de uitvoering van de functies kan besteden voldoende is, dan wel uitspraken worden gedaan over de kwaliteit van de uitvoering.

Tenslotte kan geconcludeerd worden dat de manier waarop de medewerkers in de organisatie omgaan met risico's aandacht verdient. Hoewel er inmiddels wordt ingezet op het vergroten van kennis en bewustzijn bij medewerkers op het gebied van privacy is de gemeente nog geen lerende organisatie op het gebied van informatiebeveiliging. Belangrijk is om daarbij te beseffen en uit te dragen dat daarvoor een cultuur nodig is waarin het geen schande is als men een keer op een linkje geklikt heeft en medewerkers niet bang zijn om een incident te melden.

6 Aanbevelingen

6.1 Aanbevelingen voor de Raad

Zet Informatiebeveiliging op de agenda.
Het is belangrijk dat u als raad zo gepositioneerd bent dat u uw kaderstellende en controlerende taken adequaat kunt vervullen. Dat kan door afspraken te maken over de informatievoorziening aan uw raad, maar ook door het stellen van kaders bij de voorgenomen evaluatie en bijstelling van het Integraal Informatie Beveiligingsbeleid. De gemeente Bergen is op dit moment niet AVG-proof, maar hier wordt door de organisatie wel volop op ingezet. Het voornemen bestaat om de organisatie, met uitzondering van het systeem (dat is voorzien voor 2022) aan het einde van 2019 AVG-proof te hebben. Het is aan te bevelen om u als raad periodiek te laten informeren over de voortgang van dit proces.

Zet Informatiebeveiliging op de agenda.

1. Maak met het College van B&W afspraken over de wijze waarop u periodiek geïnformeerd wilt worden over Informatiebeveiliging en privacybescherming. Bijvoorbeeld doordat u zich vertrouwelijk (i.v.m. kritische bedrijfsinformatie) laat informeren met een separate rapportage informatieveiligheid en privacy bescherming (inclusief de zelfevaluatie, een IT audit, een verklaring van het College en een passage over informatieveiligheid in het jaarverslag).
2. Maak met het College van B&W afspraken over hoe u geïnformeerd wilt worden over de voortgang van het AVG-proof maken van de organisatie, bijvoorbeeld middels een korte kwartaalrapportage over de voortgang van de actiepunten.
3. Spreek met het College van B&W af dat in de voorgenomen evaluatie en bijstelling van het integraal Informatiebeveiligingsbeleid specifiek aandacht te besteden aan:
    a. Vaststelling en analyse van risico's op Informatiebeveiliging, welke risico's beheerst of geaccepteerd worden, inclusief de bijbehorende maatregelen.
    b. Wijze waarop wordt ingezet op het vergroten van kennis en bewustzijn binnen de organisatie.

Neem maatregelen om het ICT probleem op te lossen
Op dit moment loopt de informatiebeveiliging vanaf 2020, zonder ingrijpen, gevaar als gevolg van de beperkte performance van de huidige hardware en de vertraging van de mogelijke uitbesteding aan ICT Noord- en Midden-Limburg. Het is belangrijk om dit gevaar voortvarend op te pakken af te wenden. De aanbevelingen ten aanzien van uitbesteding van ICT zijn opgenomen in de concept begroting van 2020.

Neem maatregelen om het ICT probleem op te lossen.

4. Neem in overleg met het College van B&W besluiten gericht op het afwenden van het ontstane ICT probleem vanaf 2020. Laat u periodiek informeren over de voortgang van de eventuele uitbesteding.

6.2 Aanbevelingen voor het College

Versterk de menselijke schakel
Betrouwbare informatievoorziening is een absolute randvoorwaarde voor elke gemeente. Dat vereist dat de top van de organisatie doordrongen is van het belang van informatiebeveiliging en een voorbeeldfunctie vervult. Alleen zo ontstaat er een cultuur met voldoende aandacht voor informatiebeveiliging. Dit komt tevens tot uiting in de "10 bestuurlijke principes voor informatiebeveiliging" die vanaf 1 januari 2020 van kracht worden, tegelijkertijd met de in de Baseline Informatiebeveiliging Overheid (BIO)[25]. Hiermee komt meer nadruk te liggen op risicomanagement en wordt de rol van bestuurder en de lijnmanagers explicieter. Het is daarom belangrijk om Informatiebeveiliging op de agenda van het college te plaatsen en ervoor te zorgen dat lijnmanagers verantwoordelijkheid kunnen nemen. De Adviseur informatiebeveiliging vervult een sleutelpositie en dient zijn tijd te verdelen tussen plannen, ondersteunen, controleren en bijsturen om de gemeente weerbaarder te maken tegen huidige en toekomstige digitale bedreigingen. Het bevorderen van informatiebewust en informatieveilig handelen bij medewerkers vraagt om permanent en cyclisch leren.

Versterk de menselijke schakel.

4. Koester en maak optimaal gebruik van de grote betrokkenheid van de sleutelfiguren Informatiebeveiliging bij het onderwerp en hun positieve houding ten opzichte van het verder verbeteren van Informatiebeveiliging binnen de gemeente Bergen.
5. Bestempel Informatiebeveiliging als specifieke portefeuille en benoem het tevens als strategisch agendapunt voor het College.
6. Pas de taakverdeling in de huidige uitvoeringspraktijk dusdanig aan dat er geen sprake meer is van cumulatie van rollen bij het afdelingshoofd bedrijfsvoering. Dit kan door verantwoordelijkheid van de lijnmanagers te versterken en te zorgen voor een duidelijke afbakening van verantwoordelijkheden van met name het afdelingshoofd Bedrijfsvoering en de Adviseur informatiebeveiliging.
7. Update het schema van de Informatiebeveiligingsorganisatie en zorg dat deze een goede weerspiegeling is van de uitvoering in de praktijk.
8. Versterk de positie van de Adviseur informatiebeveiliging (ook wel CISO genoemd). Positioneer de CISO strategisch onafhankelijk binnen de gemeente en geef hem de ruimte, mandaat en middelen om zijn taak goed te kunnen uitvoeren. Laat de Adviseur informatiebeveiliging regelmatig rapporteren over de effectiviteit van de processen aan het hogere management en het college (de bestuurlijk portefeuillehouder).
9. Bevorder dat elke lijnmanager de risico's binnen zijn afdeling in beeld heeft en hiervoor een passend beveiligingsplan opstelt en actueel houdt.
10. Evalueer tussentijds (bijvoorbeeld na een half jaar) het functioneren van de nieuwe Beveiligingsorganisatie zodat eventueel benodigde aanvullende maatregelen snel kunnen worden getroffen.
11. Richt permanent en cyclisch leren in waarbij er, naast training en aansturing op gedrag door het management, ook een cultuur ontstaat waarin fouten maken mag. Toets het risicobewustzijn periodiek door bijvoorbeeld de inzet van een professionele Mystery Guest, ga door met phishing testen en werkplekcontroles .

[25] De Baseline Informatiebeveiliging Overheid (BIO) is de opvolger van de Baseline Informatiebeveiliging Gemeenten (BIG).

7 Bijlagen

7.1 Reactie van het college van B & W

gemeente
BERGEN

Rekenkamercommissie gemeente Bergen
t.a.v. de heer W. Elemans
i.a.a. de heer I. van 't Hof, secretaris
Postbus 140
5854 ZJ BERGEN

Postbus 140, 5854 ZJ Bergen
Telefoon (0485) 34 83 83
Telefax (0485) 34 28 44
E-mail info@bergen.nl
www.bergen.nl

VERZONDEN 31 OKT. 2019

Datum: 29 oktober 2019
Onderwerp: Reactie op quick scan informatieveiligheid / 7376

Geachte heer Elemans,

Op 3 oktober 2019 heeft ons College van u het concept-rapport "quick scan informatieveiligheid" ontvangen. Daarin wordt de mogelijkheid geboden om op het rapport te reageren. In het navolgende treft u onze reactie aan.

I. Reactie op de gehanteerde werkwijze
Uit de rapportage blijkt dat de door u gehanteerde werkwijze bij de uitvoering van de quick scan heeft bestaan uit het bestuderen van relevante documenten en het houden van (groeps)interviews met 14 sleutelfunctionarissen in de organisatie. Verder geeft u aan dat u op basis van eigen waarnemingen heeft vastgesteld hoe een en ander in onze gemeente is georganiseerd.

In het verloop van de quick scan plaatst u enkele kritische kanttekeningen bij de wijze waarop door het lijnmanagement uitvoering is gegeven aan de informatieveiligheid. Het lijnmanagement is, zoals u in het onderzoek aangeeft, verantwoordelijk voor de integrale veiligheid van hun organisatieonderdeel en wordt geacht te sturen op gedrag en risicobewustzijn van hun medewerkers. In de BIO wordt het belang van risicomanagement verder doorgetrokken. Dit komt onder meer tot uitdrukking in de positie van de lijnmanagers die explicieter is gemaakt. In het kader van deze ontwikkeling had het voor de hand gelegen om met het totale lijnmanagement een interview te houden. Het is jammer dat dit niet is gebeurd.

Vanwege het aanvaarden van een andere functie binnen de organisatie zijn de werkzaamheden van de voormalige Adviseur Informatieveiligheid (CISO) uitbesteed aan het samenwerkingsverband ICT Noord- en Midden-Limburg (ICT NML). Eén van de doelstellingen van de quick scan is om duidelijkheid te verkrijgen over de vraag of de organisatie qua informatieveiligheid klaar is voor de toekomst. Zoals u zelf ook aangeeft vervult de CISO hierin een sleutelpositie. In dit kader had de "nieuwe" CISO u kunnen informeren over de diverse acties die inmiddels zijn uitgezet, waaronder een actuele GAP-analyse. Dit had kunnen leiden tot een completer beeld van de huidige situatie.

II Reactie op de bevindingen van de quick scan
In onze reactie beperken wij ons tot de hoofdlijnen en zullen wij niet inhoudelijk reageren op elk punt afzonderlijk.

1. AVG
In uw onderzoek schrijft u dat "Bergen in het bezit is van alle registers en procedures die verplicht zijn gesteld onder de AVG, maar nog niet AVG-proof is". Daarvoor is volgens u nodig dat er nog een aantal stappen gezet dienen te worden zoals het ontwikkelen van domein specifiek beleid, het opstellen van werkprocessen, het maken van DPIA's en de voorlichting daarover. Dit staat voor ons ook niet ter discussie. De punten die nog moeten worden uitgevoerd zijn inzichtelijk en staan gepland. Er kan dan ook worden geconcludeerd dat de basis voor compliance staat. Alle registers en procedures die de AVG verplicht stelt zijn in Bergen aanwezig. Daarnaast is er een duidelijk privacybeleid en is voor

Bezoekadres:
Raadhuisstraat 2
5854 AX Nieuw Bergen

medewerkers een privacyreglement opgesteld, dat ook met hen is gecommuniceerd. Naast het juridische kader wordt vol ingezet op voorlichting en risicobewustzijn van de organisatie in de omgang met interne en externe persoonsgegevens om te komen tot een succesvolle implementatie van de AVG. Dit is een continu proces dat voortdurend aandacht vraagt, ook nadat de inhaalslag is afgerond. Wij nemen uw aanbeveling om optimaal gebruik te maken van de sleutelfiguren in de organisatie zeker ter harte.

U schrijft verder dat "het voornemen bestaat om de organisatie, met uitzondering van het systeem (dat is voorzien voor 2022) aan het einde van 2019 AVG-proof te hebben". Vanwege de omvang van de nog te verrichten werkzaamheden is de planning bijgesteld naar het 1ste kwartaal 2020. Om de voortgang van de actiepunten goed te monitoren wordt hiervan maandelijks verslag gedaan aan het MT en aan de portefeuillehouder door middel van een kwartaalrapportage. Op dit punt nemen wij uw aanbeveling om ook de raad periodiek te informeren over.

2. Informatieveiligheid

Voor wat betreft de informatieveiligheid kunnen wij ons vinden in het algemene beeld dat u schetst in het rapport. Hieruit komt duidelijk naar voren dat de situatie direct aandacht behoeft. Enkele van de aanbevelingen uit de quick scan zijn inmiddels opgestart, zoals een leercirkel iBewustzijn in de organisatie door middel van workshops en e-learning. Hierin zal iedereen in de organisatie worden meegenomen inclusief college en management. Ook voor de raad zal een bijeenkomst worden georganiseerd, waarin haar rol als toezichthouder zal worden uitgediept. Hiermee kunnen wij het permanent en cyclisch leren structureel inrichten voor de hele organisatie, zoals u in uw aanbeveling(en) heeft verwoord.

Het vertrekpunt om inzichtelijk te krijgen welke maatregelen genomen moeten worden is de GAP-analyse. Daarin wordt duidelijk gemaakt waar de organisatie op dit moment staat en wat er nog dient te gebeuren om BIO-compliant te worden. Dit zal in een plan van aanpak (nader) worden uitgewerkt. Wij kunnen u berichten dat de GAP-analyse inmiddels gereed is en op korte termijn ter kennis gebracht zal worden aan het MT. De volgende stap zal zijn het stellen van prioriteiten en waar nodig het ter beschikking stellen van middelen om de organisatie BIO-compliant te maken. Het voldoen aan de normen van de BIO is net als bij de AVG een proces van voortdurende ontwikkeling, dat nooit ophoudt. Om dit goed te borgen zal het college het onderwerp informatieveiligheid en privacy als een vast onderdeel opnemen op de bestuurlijke agenda.

Voor wat betreft de mogelijke uitbesteding van de automatiseringswerkzaamheden aan ICT NML delen wij u mee dat recent de keuze is gemaakt om de werkzaamheden in eigen beheer voort te zetten. Daarbij wordt wel een achtervang geregeld met een derde partij. De daarvoor benodigde middelen zijn vrijgemaakt in de conceptbegroting van 2020. In dit kader zal ook de opzet van de informatiebeveiligingsorganisatie worden geactualiseerd en zullen rollen en taken opnieuw worden beoordeeld en belegd conform de aanbevelingen in de BIO. Hierbij zal de rol van de Adviseur informatiebeveiliging (CISO) worden versterkt. Ook hier geldt dat wij uw aanbeveling om optimaal gebruik te maken van de kennis en betrokkenheid van de sleutelfiguren zullen overnemen.
Middels periodieke rapportages zal uw raad worden geïnformeerd over de voortgang van de ontwikkelingen op het gebied van de informatieveiligheid.

Wij zijn ervan overtuigd dat met de reeds ingezette koers een goede basis is gelegd voor de verdere ontwikkeling en compliance op het gebied van de AVG en de informatieveiligheid.

Hoogachtend,
Burgemeester en wethouders van Bergen,
de wnd. secretaris. de burgemeester,

W.P.G.M. Scheepens M.H.E. Pelzer

O.L.G.M. Eussen
(loco-secretaris)

7.2 Nawoord Rekenkamercommissie

De Rekenkamercommissie heeft met belangstelling kennis genomen van de reactie van het college van burgemeester en wethouders van 29 oktober. In algemene zin neemt het college onze aanbevelingen over, wat ons tot tevredenheid stemt. Daarnaast zijn wij positief over de voortvarendheid waarop dit thema op dit moment wordt opgepakt. Op enkele reacties zullen wij hieronder nader in gaan.

In haar reactie geeft het college aan dat het voor de hand had gelegen om met het totale lijnmanagement een interview te houden. We willen nogmaals benadrukken dat het hier een quick scan betrof en geen uitgebreid onderzoek. In dat kader is gekozen voor een select aantal interviews zoveel mogelijk in de volle breedte van het beleidsterrein. Daarnaast is de rol van het lijnmanagement niet specifiek onderzocht, maar als aandachtspunt naar boven gekomen uit de documentenstudie en interviews. Mogelijk dat wij in een verdiepend onderzoek daar meer aandacht aan zullen besteden.

Daarnaast constateert het college dat een gesprek met de "nieuwe" CISO had kunnen leiden tot een completer beeld van de huidige situatie. Wij willen daarbij opmerken dat ten tijden van ons documentenonderzoek en de gehouden interviews (mei 2019) nog geen "nieuwe" CISO was aangesteld. Een quick scan is een momentopname maar evengoed zijn wij van mening dat we, ondanks het feit dat we de "nieuwe" CISO niet hebben gesproken, een accuraat beeld hebben geschetst van de huidige situatie. Dat het college parallel aan ons onderzoek voortvarend aan de slag is gegaan met dit thema en in korte tijd aanzienlijke verbeterslagen heeft weten te realiseren, juichen wij uiteraard van harte toe.

Tenslotte verbaast het ons dat besloten is om niet over te gaan tot uitbesteding van ICT taken. Tijdens de interviews was de ambtelijke organisatie ervan overtuigd dat dit zou gebeuren. Zelfs in de ambtelijke reactie op ons concept-rapport is dit aangegeven. Wij zijn benieuwd welke nieuwe inzichten hebben geleid tot dit besluit.

Hoogachtend,

De rekenkamercommissie van de gemeente Bergen (L),

W. Elemans, H. Meeuwsen, S. Joosten

7.3 Geraadpleegde documenten

- Gemeentebreed Informatieveiligheidsbeleid (collegebesluit 29-11-2016), gemeente Bergen.
- Rollen en namen Informatiebeveiligingsorganisatie (23 oktober 2018), gemeente Bergen; Bijlage bij gemeentebreed informatiebeveiligingsbeleid.
- Phishingtest (november 2018 en maart 2019).
- Borgen gegevensbescherming in de gemeentelijke organisatie; stand van zaken, (juli 2019), gemeente Bergen.
- Managementletter (januari 2019), KSG, en rapportage status aanbevelingen (gemeente Bergen).
- Privacybeleid; Privacyverklaring; privacyreglement; protocol datalekken; functieomschrijvingen Functionaris gegevensbescherming en Adviseur informatiebeveiliging; Procedure verzoeken betrokkenen, Planning AVG-bijeenkomsten, protocol Data Protection Impact Assessment, de verwerkersovereenkomst en de toestemmingsverklaring Wmo, Jeugdwet en Sociaal Domein (collegebesluit van 16 april 2019), gemeente Bergen.
- Register datalekken, gemeente Bergen.
- Evaluatie Informatieveiligheid 2016, controle procedures 2016 Handboek Informatieveiligheid (januari 2017), gemeente Bergen (ambtelijk).
- Informatieveiligheidsanalyse Gemeente Bergen L (januari 2017), gemeente Bergen (ambtelijk).
- GAP-analyse gemeente Bergen (januari 2016), gemeente Bergen (ambtelijk).
- Actieplan Informatieveiligheid; overzicht van de verbeteracties 2017 (januari 2017); gemeente Bergen (ambtelijk).
- Beheer en Bestuur paspoorten en Nederlandse Identiteitskaarten bronhouder Bergen (L) Verantwoordingsrapportage 2018 (collegebesluit 26 februari 2019), gemeente Bergen.
- Rapportage Uitwijktest (mei 2018), gemeente Bergen (ambtelijk).
- ENSIA kwartaalrapportages DigiD, Suwinet, BAG en BGT jaren over de jaren 2017 en 2018.
- ENSIA assurance rapport Suwinet 2017 gemeente Bergen (L) (april 2018), BKBO.
- ENSIA assurance rapport DigiD en Suwinet verantwoordingsjaar 2018 gemeente Bergen (L) (maart 2019), BKBO.
- Verslag Visitatiecommissie Informatieveiligheid gemeente Bergen (L) (maart 2016), VNG.
- Borging AVG (december 2018) VNG/IBD
- ENSIA Syllabus VNG/KING.
- Handreiking Introductie aanpak BIO (januari 2019), VNG/IBD.
- De 10 bestuurlijke principes voor informatiebeveiliging (januari 2019), VNG.
- Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten (2018) 2019/2020, VNG/IBD.
- Voortgang AVG-compliance gemeente Bergen (September 2019), The Privacy officers.

7.4 Startnotitie Quick scan Informatiebeveiliging

Notitie voor : Presidium gemeente Bergen (L)

Van : Rekenkamercommissie Bergen (L)

Datum : 07 september 2018

Onderwerp : onderzoeksopzet quick scan informatieveiligheid

Inleiding:

Afgesproken is dat er een onderzoeksopzet wordt voorgelegd over de stand van zaken rondom Informatieveiligheid binnen de gemeente Bergen (L). Hierbij spelen diverse aspecten een rol zoals:

a. de toepassing van de Baseline Informatiebeveiliging Gemeenten (BIG)
b. de onlangs in werking getreden AVG,
c. de toepassing van de wet datalekken
d. de organisatorische inbedding van een en ander.

Inhoudelijk:

Zoals bekend is er momenteel veel gaande op dit terrein. Met name de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) ingaande 25 mei 2018 heeft er voor gezorgd dat er veel activiteiten hebben plaats gevonden die te maken hebben met privacy.

Eerder hebben wij aangegeven, door middel van een quick scan, te willen vaststellen hoe een ander binnen de gemeente is georganiseerd, wat is er wel gedaan, hoe is de stand van zaken etc. Dit om richting de gemeenteraad duidelijk te maken hoe binnen de gemeente Bergen (L) wordt omgegaan met informatieveiligheid.

Daarbij willen wij op de volgende vragen duidelijkheid verkrijgen:

1. hoe staat het met de bekendheid van de Baseline Informatiebeveiliging Gemeenten en de Algemene Verordening Gegevensbescherming binnen de gemeentelijke organisatie? Hoe is/wordt dit toegepast?
2. Is er een beveiligingsorganisatie en zo ja hoe is de organisatie op beveiligingsgebied ingericht?
3. Is de verantwoordelijkheid bestuurlijk en ambtelijk belegd en zo ja hoe?
4. Is de organisatie qua informatieveiligheid klaar voor de toekomst? En daaraan gekoppeld is er voldoende duidelijkheid over rollen etc. van onder meer de security officer(s), de beveiligingscoördinator?

Als normenkader willen wij uitgaan van het volgende:

1. de richtlijnen zoals opgenomen in de wet bescherming persoonsgegevens zoals geldend vanaf 1 januari 2016, inclusief meldplicht datalekken?
2. de beveiligingsmaatregelen zoals omschreven in de Baseline Informatiebeveiliging Gemeenten
3. de richtlijnen die voortkomen uit de Algemene Verordening Gegevensbescherming

Doelstelling:

De doelstelling is ,dat de RKC met deze quickscan een peilstok in de gemeentelijke organisatie wil steken, om zicht te krijgen op de actuele stand van zaken rondom informatieveiligheid. Dit alles met als doel de informatieveiligheid op een (nog) hoger niveau te tillen.

Onderzoeksmethode:

Naast het bestuderen van de relevante documenten worden er enkele interviews gehouden met zowel bestuurlijk als ambtelijke vertegenwoordigers. Verder willen wij op basis van onze eigen waarnemingen, alsmede de inbreng van kennis en ervaringen, trachten vast te stellen hoe een en ander binnen de gemeente Bergen (L) georganiseerd is.
Op basis van onder andere deze uitkomsten worden conclusies getrokken en aanbevelingen gedaan

Planning:

Er lopen thans twee onderzoeken waarbij de organisatie is betrokken, namelijk inzake het onderzoek handhaving en de risicobeheersing energielandschap. Het advies over de doorontwikkeling bestuursrapportage is inmiddels uitgebracht en kan nu geïmplementeerd worden.

Het lijkt ons dan ook gepast om eind 2018/begin 2019 deze quick scan uit te voeren.

Uitvoering geschiedt door de RKC zelf.

7.5 Informatiebeveiligingsorganisatie

Gemeentebreed Informatiebeveiligingsbeleid

I.v.m. Privacy zijn de namen in het oorpronkleijke doucument onherkenbaar gemaakt

Rollen en namen informatiebeveiligingsorganisatie

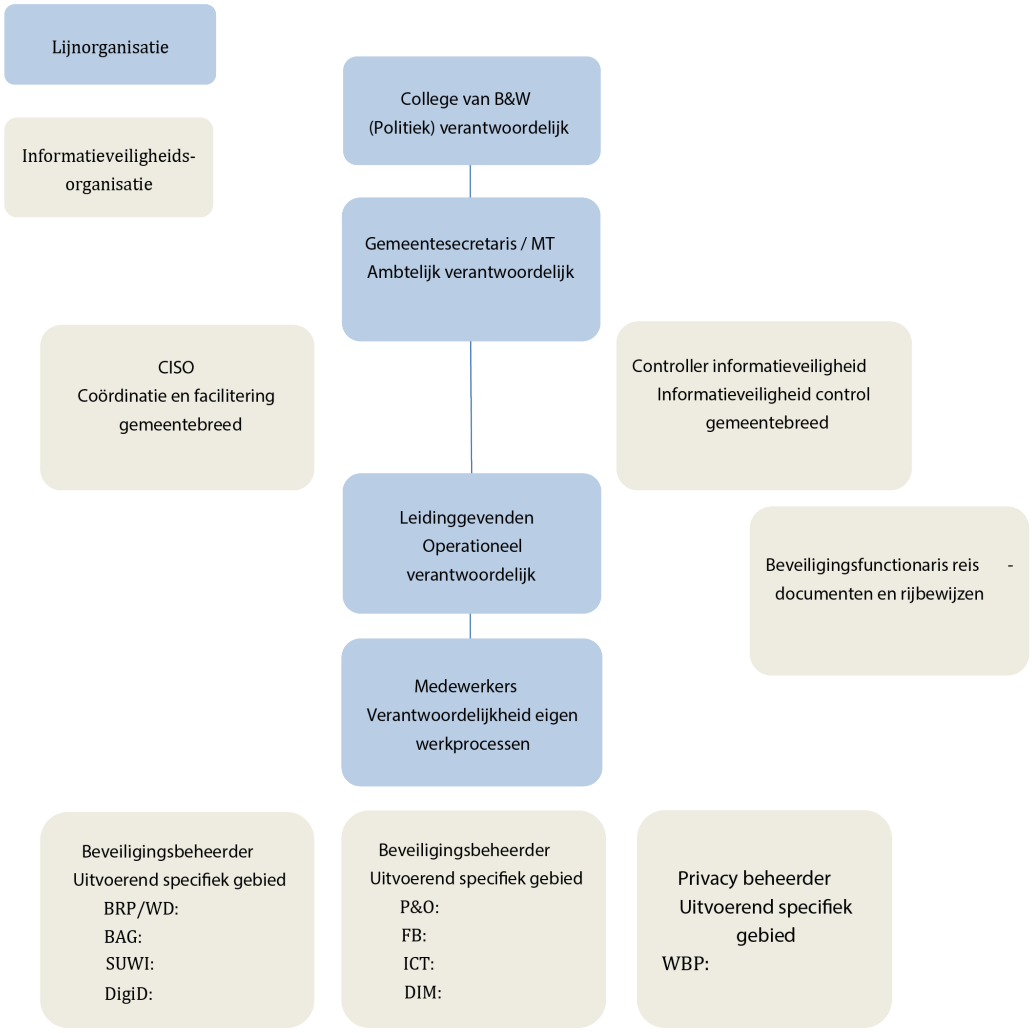
Bijlage bij Gemeentebreed Informatiebeveiligingsbeleid, d.d. 23 oktober 2018

Rol informatiebeveiliging	Naam	Functie	Vervanger	Functie
Voorzitter Werkgroep		Afdelingsmanager Bedrijfsvoering		Adviseur Informatiebeveiliging
Coördinator Informatieveiligheid (CISO)		Adviseur Informatiebeveiliging		Juridisch Adviseur
Controller Informatieveiligheid (CIO)		Adviseur Informatiebeveiliging		Financieel Controller
Privacy Beheerder		Juridisch Adviseur		Juridisch Adviseur
Beveiligingsbeheerder ICT		Consulent I&A		Consulent I&A
Beveiligingsbeheerder DigiD		Adviseur Communicatie		Medewerker Communicatie
Beveiligingsbeheerder BRP/WD		Consulent Burgerzaken		Medewerker Burgerzaken
Beveiligingsbeheerder Suwinet		Adviseur Informatiebeveiliging		Senior Adviseur Sociaal Domein
Beveiligingsbeheerder BAG		Specialist I & A		Medewerker GEO
Beveiligingsbeheerder BGT		Medewerker GEO		Specialist I & A
Beveiligingsbeheerder BRO		Specialist Milieu		Toezichthouder Omgevingsrecht
Beveiligingsbeheerder P&O		Consulent P&O		Consulent P&O
Beveiligingsbeheerder DIM		Adviseur DIM		Medewerker Informatievoorziening
Beveiligingsbeheerder FZ		Specialist Facility		Medewerker Facility
Beveiligingsfunctionaris Reisdocumenten en Rijbewijzen		Financieel Controller		Consulent Burgerzaken
Communicatie Werkgroep		Adviseur Communicatie		Medewerker Communicatie

ACIB (IBD)		Consulent I&A Adviseur Informatiebeveiliging		
VCIB (IBD)		Afdelingsmanager Bedrijfsvoering Adviseur Informatiebeveiliging		

Gemeentebreed Informatiebeveiligingsbeleid

Organisatieschema



7.6 De 10 bestuurlijke principes voor informatiebeveiliging

Behorende bij de Baseline Informatiebeveiliging Overheid (BIO)

VNG

Baseline

De 10 bestuurlijke principes voor informatiebeveiliging

Behorende bij de Baseline Informatiebeveiliging Overheid (BIO)

Colofon

Met dank aan
De expertgroep, de reviewgemeenten en de Informatiebeveiligingsdienst voor Gemeenten die hebben bijgedragen aan het vervaardigen van dit product.

Versiebeheer
Het beheer van dit document berust bij de Vereniging van Nederlandse Gemeenten (VNG).

Opmaak
Chris Koning (VNG)

Informatiebeveiliging en de gemeentelijke bestuurder

Gemeenten wisselen op alle beleidsterreinen informatie uit en beheren dat op vele manieren. Binnen de eigen organisatie, maar ook daarbuiten: met inwoners, ondernemers, ketenpartners en medeoverheden. Door informatie te delen kunnen gemeenten onder andere hun dienstverlening beter organiseren, de veiligheid van inwoners verbeteren en meer mensen aan het werk krijgen. Als professionele organisatie past hierbij dat gemeenten ook de beveiliging van informatie adequaat organiseren. Informatie moet immers beschikbaar, actueel, volledig en betrouwbaar zijn en mag alleen door bevoegden zijn in te zien. Bij de uitwisseling moeten gemeenten te allen tijde rekening houden met beveiligings- en privacyaspecten omdat ze een maatschappelijke en wettelijke verantwoordelijkheid[1] hebben om de gegevens van hun inwoners onder alle omstandigheden te beschermen. De risico's rondom de vertrouwelijkheid, integriteit en beschikbaarheid van informatie(systemen) maken dat het onderwerp informatiebeveiliging niet mag ontbreken op de bestuurstafel.

Mens, proces en techniek

Informatieveiligheid is veel meer dan ICT, het gaat in veel gevallen om de mens in de organisatie en de manier waarop deze met risico's omgaat. Is de medewerker zich bewust van die risico's? Zijn bestuurders zich bewust van de risico's van en voor de organisatie? Gemeentelijke bestuurders zijn verantwoordelijk voor de informatiebeveiliging binnen gemeentelijke organisatie. Beveiliging van gegevens en systemen is een zaak van organisatie, procedures, werkprocessen en in de laatste plaats techniek. Het gaat om de mens, de manier waarop deze werkt en het gereedschap waarmee het werk verricht wordt.

Risicomanagement is de basis

De bestuurder is verantwoordelijk voor een veilige informatievoorziening. Het is daarom aan de bestuurder om de risicobereidheid te bepalen en daarmee ook te controleren of de maatregelen binnen de organisatie de risico's terugbrengen tot een voor de bestuurder acceptabel niveau. Overschrijding van dat niveau vereist expliciete besluitvorming. Risicomanagement staat daarmee aan de basis van informatiebeveiliging. Er dient een continu proces van identificatie en beoordeling van risico's plaats te vinden om te bepalen wat nodig is om informatie adequaat te beschermen. Hierbij moet worden opgemerkt dat het risico *nul* niet bestaat en dat het aan het bestuur is om te bepalen hoeveel of welk risico acceptabel is. En de risico's zijn talrijk: privacyschendingen door een datalek, economische schade door het uitlekken van vertrouwelijke plannen, fysieke schade door storingen in systemen in de openbare ruimte.

Normen en regels

De ontwikkelingen in de informatietechnologie gaan steeds sneller en de wetgeving rondom de bescherming van persoonsgegevens is aangescherpt. De internationale norm om informatie(systemen) adequaat te beveiligen is vastgelegd in de ISO27001/2. Voor de Nederlandse overheid is deze norm vertaald naar een zogenaamde *Baseline Informatiebeveiliging Overheid* (BIO) met daarin de regels waaraan alle overheidslagen dienen te voldoen. Door middel van een zelfevaluatie (ENSIA) verantwoorden gemeenten zich over deze norm.

Bestuurlijke aanvulling op de normen en regels

In aanvulling op de baseline bevat dit document de bijbehorende principes voor bestuurders. Daarmee gaat dit document over waarden die u zichzelf als bestuurder oplegt. Deze waarden dienen verbonden te zijn aan de waarden van uw organisatie. Dit document is de bestuurlijke aanvulling op de baseline en helpt u om de juiste dingen te doen. De principes gaan daarom vooral over u en uw rol bij het borgen van informatiebeveiliging in uw organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement.

1 O.a. de Algemene wet gegevensbescherming, Wet BRP, PUN, DigiD, BAG, BGT en SUWI

De 10 principes voor informatiebeveiliging

Informatiebeveiliging creëert waarde, voorkomt schade en draagt bij aan de bedrijfsdoelstellingen van de organisatie. Om dat te bewerkstelligen zijn de volgende principes belangrijk:

1 Bestuurders bevorderen een veilige cultuur

Menselijk gedrag en cultuur beïnvloeden op significante wijze alle aspecten van risicomanagement op elk niveau en in elk stadium.

Ik ben mij bewust van de voorbeeldfunctie van een bestuurder en ik draag uit dat risicomanagement van iedereen is. Ik zorg daarom voor een cultuur waarin iedereen vrij is om dreigingen waar te nemen en te melden. In eerste instantie bij de verantwoordelijke, maar indien nodig ook bij mij als bestuurder. Ik spoor managers aan om voorwaarden te scheppen zodat iedereen binnen de organisatie deelgenoot wordt van het proces van risicomanagement. Ik zorg ervoor dat fouten besproken kunnen worden en dat daarmee een lerende organisatie ontstaat. Ten slotte geef ik in mijn eigen doen en laten het goede voorbeeld van hoe je verantwoordelijk omgaat met informatie.

Toelichting

Zonder open cultuur waar iedereen vrij is om te spreken is het niet goed mogelijk om risico's te identificeren en als de risico's niet bekend zijn, kunt u ze ook niet adresseren. Als u in uw organisatie een cultuur bevordert waarin mensen zich vrij voelen om risico's te melden en maatregelen voor te stellen, dan kunt u adequaat reageren op dreigingen en samenhangende risico's.

2 Informatiebeveiliging is van iedereen

Passende en tijdige betrokkenheid van belanghebbenden maakt het mogelijk dat hun kennis, opvattingen en percepties in aanmerking worden genomen. Dit resulteert in een verbeterd bewustzijn en goed geïnformeerd risicomanagement.

Ik maak medewerkers bewust van de risico's van het werken met informatie en ik maak risicomanagement onderdeel van het MT-overleg en laat het anderen in vergaderingen agenderen. Ik zorg ervoor dat iedereen risicomanagement toepast en dat het gezien wordt als vanzelfsprekend en nuttig. Ik ben transparant naar de raad en zorg ervoor dat hij ook zijn rol kan pakken op dit onderwerp.

Toelichting

Iedereen moet betrokken worden bij risicomanagement, in alle lagen van de organisatie. Maak gebruik van de kennis en verantwoordelijkheid van proces- en systeem eigenaren. Gebruik uw Chief Information Security Officer (CISO), Functionaris Gegevensbescherming (FG) en Controller als onafhankelijke adviseur en laat ze samenwerken in een risicoteam, waar u vanzelfsprekend ook zitting in heeft. Laat uw interne communicatie aandacht besteden aan het verspreiden van de boodschap, het belang en het voordeel van risicomanagement binnen uw organisatie. Goed uitgevoerd risicomanagement creëert waarde voor de organisatie omdat de kwaliteit van besluiten toeneemt en de kans op falen afneemt.

3 Informatiebeveiliging is risicomanagement

Risicomanagement wordt bewust toegepast bij alle organisatie activiteiten.

Ik zorg dat risicomanagement een onderdeel is van het bestuurlijk overleg en dialoog. Daarnaast zal ik het integreren in het risicobewustzijn van alle medewerkers en het onderdeel laten zijn van de samenwerking met partners en ik zorg ervoor dat risicomanagement integraal onderdeel uitmaakt van uitbestedingen en

samenwerkingen. Ik zorg ervoor dat risicomanagement geformaliseerd wordt binnen de hele organisatie met een duidelijke verdeling van verantwoordelijkheden en heldere besluitvorming.

Toelichting
Risicomanagement werkt alleen als het geïntegreerd is in alle werkprocessen van de organisatie. Dat kan alleen bereikt worden als risico's regelmatig op de agenda staan en als risico's een plek/paragraaf krijgen in alle bestuurlijke documenten. Maak lijnmanagers verantwoordelijk voor risicomanagement door afspraken met ze te maken over uw risicobereidheid. Lijnmanagers zijn verantwoordelijk voor de maatregelen en rapportage daarover.

4 Risicomanagement is onderdeel van de besluitvorming

Risicomanagement is onderdeel van alle besluiten en risicomanagement is chefsache.

Ik maak medewerkers mede-eigenaar van het risicoproces op het vlak van informatieveiligheid en ik maak informatiebeveiliging onderwerp van alle overlegstructuren. Ik draag er zorg voor dat besluiten ten aanzien van de omgang met risico's expliciet genomen en vastgelegd worden. Ik laat risicomanagement naadloos aansluiten op de strategische en beleidsmatige doelstellingen van de organisatie. Op deze wijze bied ik een duidelijk kader waarbinnen de medewerkers kunnen opereren.

Toelichting
U kunt als bestuurder alleen de juiste richting aangeven als informatie u bereikt. Door dreigingen en risico's mee te nemen in de vragen die u stelt aan uw managers kunt u er in uw beslissingen ook rekening mee houden. Zo kunt u bijsturen voordat risico's manifest worden en escalatie voorkomen.

5 Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking

Het risicomanagementproces is aangepast en staat in verhouding tot de externe en interne context van de organisatie die verband houdt met haar doelstellingen.

Ik zorg dat ik de risico's ken die een gevaar vormen voor de informatievoorziening van de bedrijfsvoering van de gemeente en ik anticipeer op risico's die voortkomen uit het werken in ketens en ik houd rekening met de complexiteit, de onzekerheid en ambiguïteit in de samenwerking met anderen. Bij samenwerken of uitbesteden van (delen) van de organisatie of processen zorg ik ervoor dat de risico's in kaart gebracht zijn, verantwoordelijkheden verdeeld en dat de juiste maatregelen getroffen worden.

Toelichting
Het risicomanagementproces moet passen bij de organisatie en ondersteunen aan de organisatiedoelstellingen. De keten is zo sterk als de zwakste schakel. De gemeente dient met ketenpartners en leveranciers regelmatig het gesprek te voeren over risico's en de maatregelen die ervoor zorgen dat de risico's tot een acceptabel niveau worden teruggebracht.

6 Informatiebeveiliging is een proces

Risico's kunnen ontstaan, veranderen of verdwijnen als de externe en interne context van een organisatie verandert. Risicomanagement detecteert en anticipeert op die veranderingen en gebeurtenissen op een gepaste en tijdige manier.

Ik zorg ervoor dat risicomanagement cyclisch is en daarmee kan ik reageren op veranderingen en toekomstgericht sturen. Het staat daarom regelmatig op de agenda.

Toelichting
Risicomanagement moet een cyclisch, iteratief en terugkerend proces zijn, want dreigingen veranderen, doelstellingen veranderen, de omgeving verandert en wetgeving verandert. Indien u in uw risicomanagement geen rekening houdt met een veranderende omgeving, dan zijn uw maatregelen op termijn wellicht niet doeltreffend of doelmatig.

7 Informatiebeveiliging kost geld

Risico's moeten behandeld worden en er zijn vele manieren om veiligheid te realiseren, maar aan alle zijn kosten verbonden.

Ik zorg ervoor dat er voldoende middelen beschikbaar zijn om de onderkende risico's op een adequate manier te behandelen. Als gebleken is dat een risico een bedreiging is voor de organisatiedoelstellingen en er maatregelen genomen moeten worden, dan zorg ik er ook voor dat de middelen beschikbaar zijn om deze maatregelen uit te voeren.

Toelichting

Risico's kunt u ontwijken, mitigeren, overdragen of wegnemen door het nemen van preventieve-, repressieve- en/of correctieve maatregelen. Welke strategie u ook kiest, ze kosten allemaal middelen in termen van tijd en geld. Voor maatregelen kan derhalve een kosten-batenanalyse worden gemaakt.

8 Onzekerheid dient te worden ingecalculeerd

De input voor risicomanagement is gebaseerd op historische en actuele informatie, evenals op toekomstige verwachtingen. Risicomanagement houdt expliciet rekening met eventuele beperkingen en onzekerheden die aan dergelijke informatie en verwachtingen zijn verbonden. Informatie moet tijdig, duidelijk en beschikbaar zijn voor relevante belanghebbenden.

Risicomanagement is gebaseerd op de best beschikbare informatie vanuit mijn organisatie en vanuit mijn samenwerkingen. Ik zorg ervoor dat alle belanghebbenden op een gestructureerde en voorspelbare wijze informatie delen die bijdraagt aan risicomanagement.

Toelichting

Zonder goede informatie kunt u geen goede risico-inschattingen en besluiten nemen. Zonder goede en tijdige informatie bent u niet bekend met de risico's die uw organisatie loopt.

9 Verbetering komt voort uit leren en ervaring

Risicobeheer wordt voortdurend verbeterd door leren en ervaring.

Door mijn inzet zorg ik ervoor dat risicogestuurd werken doorontwikkeld wordt. Ik reflecteer op ervaringen en ik nodig medewerkers uit tot het delen van ervaringen met betrekking tot de risico's die de informatievoorziening bedreigen. Ik zorg ervoor dat de organisatie kan leren van incidenten en dat de organisatie leert te ontdekken wat wel en wat niet werkt.

Toelichting

Risicomanagement gedijt het beste in een organisatie die leert van ervaringen en op basis hiervan verbeteringen doorvoert. Hoe goed u uw informatiehuishouding ook beveiligt, incidenten zullen altijd voorkomen. Door te zoeken naar verbeterpunten en de wil om te leren bouwt u doorlopend aan het verhogen van uw digitale weerbaarheid.

10 Het bestuur controleert en evalueert

Risicomanagement is het controleren en evalueren van resultaten, evenals het nemen van eindverantwoordelijkheid en het doorhakken van lastige knopen.

Ik geef opdracht om de werking van risicomanagement binnen mijn organisatie op effectiviteit en efficiency te (laten) controleren. Naast managementrapportages zijn (externe) controles de manier om te weten te komen of en hoe het beleid in de praktijk uitwerkt. Als bestuurder weeg ik goed geïnformeerd risico's en belangen af en neem ik mijn verantwoordelijkheid om knopen door te hakken.

Toelichting

Controle is belangrijk om goed inzicht te krijgen in de mate waarin het informatiebeveiligingsbeleid en risicomanagement ingebed zijn in de organisatie. Naast verslagen en managementrapportages zijn incidenten, en dan vooral de manier waarop ze afgewikkeld worden, een goede graadmeter om te zien hoe de organisatie

omgaat met het onderwerp. Medewerkers kunnen erop vertrouwen dat besluiten op bestuursniveau genomen worden, wanneer de situatie daar om vraagt.

Vereniging van
Nederlandse Gemeenten

Nassaulaan 12
2514 JS Den Haag
+31 70 373 83 93
info@vng.nl

januari 2019

vng.nl