HORDIJK & HORDIJK
ADVISEURS VOOR ORGANISATIE EN FINANCIËN B.V.

Rekenkamercommissiecommissie Maasdriel

Vijftiende onderzoek

Memorandum

Beveiliging van informatie

22 januari 2018

Rekenkamercommissiecommissie Maasdriel

Beveiliging van informatie

22 januari 2018

Inhoud

HORDIJK & HORDIJK
ADVISEURS VOOR ORGANISATIE EN FINANCIËN B.V.

Memorandum

I Beveiliging van informatie

Ter introductie

De Rekenkamercommissiecommissie van de gemeente Maasdriel heeft in 2017 – met een stukje overloop naar 2018 – twee onderzoeken verricht. Het betreft (1) een wat groter onderzoek inzake het lokale onderwijsbeleid in Maasdriel, waarover een separaat memorandum is uitgebracht, alsmede (2) een klein onderzoek naar een als zodanig heel breed onderwerp: de beveiliging van informatie. De uit dat tweede onderzoek voortgekomen bevindingen zijn in het voorliggende memorandum opgenomen.

Zoals bekend fungeert Frank Hordijk, het enige lid van de Rekenkamercommissie van Maasdriel, in de gemeente Aalsmeer in een vrijwel identieke Rekenkamer-rol. Conform aankondiging in het Jaarplan 2017 van de Rekenkamercommissie is het onderzoek inzake de beveiliging van informatie parallel in die twee gemeenten uitgevoerd. Dit memorandum is daarom qua opzet – en overigens ook qua strekking van de verschillende bevindingen en aanbevelingen – grotendeels vergelijkbaar met het stuk dat in Aalsmeer is opgeleverd. Overigens is de bedoelde parallelle uitvoering inhoudelijk vruchtbaar gebleken: de Rekenkamercommissie kon verkregen documenten, procedures, rapportages en wat dies meer zij goed vergelijken in termen van opzet, inhoud, borging, interne verspreiding en communicatie, evaluatie en bestuurlijke aandacht.

Uit het Jaarplan voor 2017

In het Jaarplan 2017 van de Rekenkamercommissie Maasdriel is onder meer opgenomen dat de Rekenkamercommissie onderzoek wil doen:

- naar de maatregelen, die de gemeente Maasdriel heeft getroffen in het kader van de beveiliging van informatie (techniek, afspraken en procedures, borging, opvolging van eventuele incidenten).

  Als vertrekpunt voor dit onderzoek speelt als hoofdvraag:

  draagt de gemeente Maasdriel, waar aan de orde in samenwerking met de gemeente Zaltbommel en afgezet tegen in dit verband gangbare normen, zorg voor een adequate beveiliging van alle informatie, waarvan niet-geautoriseerde inzage en/of gebruik door interne en/of externe derden moet worden voorkomen?

Aanleiding en normenkader

Was of is er een concrete aanleiding voor dit (kleine) onderzoek? Nee en ja.

Nee, omdat het beveiligen van informatie al van oudsher de aandacht van ook iedere gemeente moet hebben. Van het toegangsbeleid voor medewerkers en bezoekers via het frequent wijzigen van wachtwoorden tot het direct melden van een per ongeluk naar een verkeerd extern adres verzonden mailtje, waarbij (dat zal je altijd zien!) een bijlage met gevoelige informatie was gevoegd: alles rond het thema 'beveiliging van data' moet al jaren op de agenda staan.

Toch ook ja, omdat het onderwerp in de voorbije jaren steeds relevanter is geworden en de consequenties van onverhoopte incidenten enorm kunnen zijn. 2018 is in dit verband in die zin een sleuteljaar, dat op 25 mei 2018 de zogenoemde *Algemene verordening gegevensbescherming* in werking treedt.

Op de site van de Vereniging van Nederlandse Gemeenten is de onderstaande tekst te vinden, die uitstekend de taak samenvat waarvoor alle gemeenten – dus ook Maasdriel, al dan niet in samenwerking met Zaltbommel – zich voor nu en de komende jaren gesteld ziet. Op enkele plaatsen, aangegeven met (…), is het citaat door de Rekenkamercommissie ingekort.

De VNG-tekst is voor de Rekenkamercommissie de norm geweest, waaraan de werkelijkheid in de gemeente Maasdriel is getoetst. Tussen de regels hieronder door is die norm op enkele plaatsen praktisch uitgewerkt.

**

> **Ter introductie**
>
> Geregeld komen organisaties in het nieuws omdat persoonsgegevens op straat liggen door een datalek. Dat overkomt ook gemeenten. Het is een inbreuk op de privacy van de burgers en een strop voor de gemeente. Die wordt geconfronteerd met negatieve publiciteit, imagoschade, hoge kosten en eventuele boetes. Hoe kun je het voorkomen?
>
> Datalekken zijn nooit helemaal te voorkomen, maar gemeenten kunnen hun organisatie wel zo inrichten dat de kans zo klein mogelijk wordt. Een extra zetje om dit te doen is dat op 25 mei 2018 de Algemene verordening gegevensbescherming (AVG) ingaat. Deze verordening komt in de plaats van de huidige Wet bescherming persoonsgegevens (Wbp).

De AVG

De AVG is een Europese verordening die rechtstreeks doorwerkt in de nationale wetgeving van de EU-lidstaten. Dat betekent borging op Europees niveau van onze gemeenschappelijke normen op het gebied van privacy en gegevensbescherming.

De AVG heeft twee doelen. De eerste gaat over de bescherming van persoonsgegevens. De tweede is het mogelijk maken van het vrije verkeer van persoonsgegevens binnen de EU. Aan de ene kant bescherming, en de andere kant het vrij kunnen stromen van gegevens. Dit lijkt tegenstrijdig, maar het gaat in feite over een voortdurende afweging tussen de belangen van de personen over wie persoonsgegevens verwerkt worden (burgers, klanten) en de belangen van de organisaties (zoals gemeenten) die gegevens verwerken. Privacy en gegevensbescherming zijn grondrechten en die kunnen worden beperkt als dat noodzakelijk is. Dit was al zo onder de huidige Wet bescherming persoonsgegevens en dat blijft zo onder de AVG. Ook de regels voor gegevensbescherming blijven hetzelfde. Die regels gaan over wanneer je welke gegevens voor welk doel mag verwerken, en met wie je ze mag delen (doel, grondslag, noodzaak).

Wat is nieuw?

Onder de AVG zijn organisaties, zoals gemeenten, verplicht om hun organisatie zo in te richten dat de privacyregels structureel worden nageleefd, en dat organisatie dit kan verantwoorden en bewijzen. Dat anders inrichten van de eigen (gemeentelijke) organisatie vereist een grote inspanning en vaak zelfs een cultuuromslag. Daarnaast krijgen betrokkenen (zoals burgers) een sterkere rechtspositie als het gaat om inzage in en rectificatie van de verwerking van persoonsgegevens. (…).

Hoever gemeenten zijn

Gemeenten zijn, net als andere organisaties, intensief bezig met de implementatie van de AVG. Desondanks staan zij nog voor een aanzienlijke uitdaging om voor de datum van inwerking-treding te voldoen aan alle vereisten van de AVG. (…). Voor het beheerst toegroeien naar een situatie die de AVG volledig ondersteunt, ligt de verantwoordelijkheid bij bestuurders.

1. De Rekenkamercommissie heeft willen vaststellen in hoeverre het onderwerp ‘beveiliging van informatie’ de aantoonbare, actieve aandacht van het college heeft.

Verantwoording en transparantie zijn hier belangrijk. Dit kan in de vorm van een duidelijk en concreet plan, waarin inzichtelijk is welke stappen er nog gezet moeten worden, wat de aanpak en planning is. Juist als nog niet aan alle AVG vereisten volledig wordt voldaan, is het van groot belang om ‘in control’ te zijn over de resterende werkzaamheden.

(…)

Wat is goed privacymanagement?

In het kort gaat het bij privacymanagement om alle maatregelen die genomen worden om ervoor te zorgen dat de AVG-regels worden nageleefd en dat daarover verantwoording kan worden afgelegd. Bij veel gemeenten is de IT-afdeling daar al druk mee bezig, al dan niet samen met een privacy-officer of functionaris gegevensbescherming (FG). Maar dit is niet genoeg. De implementatie van de AVG moet doordringen in alle lagen van de gemeentelijke organisatie, van de baliemedewerker tot aan de burgemeester. Daarvoor is het college van B en W verantwoordelijk.

Ter ondersteuning van de verantwoordingsplicht van het college van B en W bevat de AVG een aantal (verplicht voorgeschreven) instrumenten:

- de aanwijzing van een functionaris voor gegevensbescherming
- het opzetten en bijhouden van een verwerkingsregister
- het uitvoeren van een privacy impact assessment
- toepassen van privacy by design/default-principe
- informatiebeveiliging
- de meldplicht datalekken.

2. De Rekenkamercommissie heeft onderzocht of in de bovenstaande instrumenten is voorzien.

Bewustwording

Het invoeren van de hiervoor genoemde instrumenten gebeurt - in de ideale situatie - in de vorm van een proces waarbij de hele ambtelijke organisatie wordt betrokken (…). Het proces is in feite een privacy bewustwordingsproces. Het college van B en W is eindverantwoordelijk en kan een deel van die verantwoordelijkheid delegeren aan lijnmanagers en procesmanagers, die vervolgens de professionals op de werkvloer aansturen. (…).

3. De Rekenkamercommissie heeft willen beoordelen op welke wijze het onderwerp ‘beveiliging van informatie’ de actieve aandacht van alle medewerkers van de gemeente heeft, waar aan de orde met expliciet zichtbare bestuurlijke betrokkenheid. Daarbij is het de intentie ook te bezien in hoeverre medewerkers zich vrij voelen om risico’s en eventuele incidenten te melden: niet met de dreiging om ergens in welke vorm dan ook voor te worden gestraft, maar juist om een cultuur te stimuleren waarin betrokkenen op het gebied van informatiebeveiliging hun kwetsbaarheden tonen, waarvan door henzelf en anderen gericht kan worden geleerd.

Het borgen van privacy is een *ongoing process*

Het gaat niet om het eenmalig treffen van een aantal privacymaatregelen. Verwerkingen van gegevens, doelgroepen, technische mogelijkheden, privacyregels, en maatschappelijke opvattingen kunnen veranderen. De effectiviteit van de maatregelen moet daarom regelmatig worden beoordeeld en waar nodig aangepast.

Controle door de raad

Voor het goed regelen van privacy is het college van B en W aan zet. De gemeenteraad moet vervolgens controleren of er voldoende wordt gedaan op het gebied van privacybewustwording en of de AVG-maatregelen correct en goed worden uitgevoerd. Zo kan de raad controleren wat de stand van zaken is van het invoeringstraject van de AVG. En of de invoering van de AVG aan de orde is geweest in de verschillende gemeentelijke kadernota's en begrotingsramingen voor 2018. En, zijn er voor de komende jaren bestuurlijke en budgettaire maatregelen genomen en vastgelegd om de gevolgen van de invoering van de AVG op te vangen? (…).

4. De Rekenkamercommissie stelt graag vast – maar dat kan pas feitelijk bij de behandeling van dit memorandum – in hoeverre de raad de hierboven bedoelde controle (1) met de vereiste diepgang kan uitoefenen en (2) dat ook aantoonbaar doet, bijvoorbeeld door het stellen van vragen aan het college of het bijwonen van presentaties of informatiebijeenkomsten.

Aanpak

Hoe heeft de Rekenkamercommissie het uitgevoerde, bewust kleine onderzoek aangepakt? Als volgt:

- via de gemeentesecretaris is contact gezocht met de ambtelijk medewerker, die het eerste aanspreekpunt voor het onderwerp vormt

- de Rekenkamercommissie kwam aldus terecht bij twee betrokkenen: de teammanager informatisering en automatisering van de Bedrijfsvoeringseenheid Bommelerwaard en de zogenoemde Chief Information Security Officer (CISO), ook werkzaam vanuit de Bedrijfsvoeringseenheid. Beiden zijn actief voor zowel Maasdriel als Zaltbommel

- door omstandigheden is in eerste instantie alleen met laatstbedoelde, dus met de CISO een goed voorbereid, maar bewust 'open' interview afgenomen. Nadien, toen die CISO wegens ziekte langer afwezig was, zijn contacten onderhouden met de plaatsvervangend CISO (gegevensbeheerder-informatiebeveiligingsfunctionaris)

- op specifiek verzoek van de Rekenkamercommissie, maar ook op eigen initiatief van de CISO is vervolgens een grote hoeveelheid documenten ontvangen en bestudeerd. Uit de combinatie van stukken, uitkomsten van het interview en opvolgende contacten met de plaatsvervangend CISO heeft de Rekenkamercommissie zich een beeld gevormd van de opzet, inbedding, werking, borging en bestuurlijke aandacht van (en voor) het onderwerp beveiliging van informatie

- dat verkregen beeld is verbreed en deels ook (nader) getoetst in een gesprek met de verantwoordelijk bestuurder, in casu burgemeester Henny van Kooten. Aan dat gesprek namen ook de teammanager informatisering en automatisering en de plaatsvervangend CISO deel.

De Rekenkamercommissie (dus Frank Hordijk) heeft het onderzoek niet alleen gedaan: hij heeft zich laten bijstaan door ing. Gerald Schaapman CISSP, ook afkomstig uit Culemborg en al jarenlang een zakelijk contact van Hordijk, die in Nederland op het hoogste niveau bijdragen levert aan onder meer het zoveel mogelijk ongestoorde verloop van het internetverkeer. Schaapman mag zich als zodanig een specialist op het technische, maar ook procedurele deel van het onderzoeksterrein mag noemen.

Zoals steeds is de Rekenkamercommissie heel positief over alle onverkort en waar aan de orde heel openhartig verkregen medewerking. De onderzoekers, maar als eerste en voornaamste de Bedrijfsvoeringseenheid werden geconfronteerd met de plotselinge en langdurige uitval van de CISO, die juist een fase van ‘bouwen en structureren’ van alle noodzakelijke procedures en andere instrumenten leek te kunnen afsluiten. Zijn voorlopige opvolging is naar het zich laat aanzien adequaat geregeld, hoewel in dit verband ook meteen de relatieve kwetsbaarheid van een goed ingevoerde CISO – in dit geval werkzaam voor twee gemeenten – is ervaren.

Overigens liet de plaatsvervangend CISO meteen zien hoe het moet bij het ons toesturen van diverse documenten: die kwamen per mail, maar waren alleen te openen met een wachtwoord dat de onderzoekers individueel per SMS werd gezonden.

**

Als bijlage bij dit memorandum is de reactie opgenomen, die de Rekenkamercommissie ontving op het op 22 januari 2018 aangeboden concept van dit memorandum. Uit de reactie blijkt dat onze aanbevelingen worden onderschreven – en blijkt tegelijk de urgentie van de suggesties, die de Rekenkamercommissie doet.

II Aantekeningen en suggesties

Aspecten

De Rekenkamercommissie heeft hieronder een samenvatting van de gehanteerde referenties en gemaakte aantekeningen opgenomen. Die kunnen hier en daar wat technisch overkomen, maar vormen in onze visie (toch) zonder uitzondering de minimale aspecten waarvoor alle gemeentelijke actoren – ambtelijk, de verantwoordelijk portefeuillehouder en het college als geheel, raadsleden en ook de raad als geheel – aandacht zouden moeten hebben.

We hebben als referentie mede gebruik gemaakt van de internationale standaarden voor informatie-beveiliging: NEN/ISO 27001 en NEN/ISO 27002. De eerste standaard (27001) biedt een richtlijn voor de implementatie en planmatige borging van informatiebeveiliging binnen de organisatie, ook wel het information security management system (ISMS) genoemd. De tweede standaard (27002) bevat een zeer uitgebreide verzameling van zogenaamde *best practices* voor een praktische en concrete aanpak van informatiebeveiliging binnen de organisatie. Door de *Informatie-beveiligingsdienst voor gemeenten* (IBD) is aan de hand van deze ISO normering de zogenaamde standaard *Baseline Informatiebeveiliging Nederlandse Gemeenten* (BIG) opgesteld. De IBD is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING).

We hebben er, gegeven het eerder in dit memorandum uitgewerkte normenkader, voor gekozen een aantal aspecten uit de BIG specifieke aandacht te geven. Dat betreft:

- het informatiebeveiligingsbeleid
  - meest recente versie en status document?

De Rekenkamercommissie ziet diverse (verplichte) documentatie, maar stelt tegelijk vast dat die op meerdere punten nog concepten bevatten of onvolledig zijn. Het plan voor het informatie-beveiligingsbeleid was in het najaar van 2017 nog niet door het college van Maasdriel vastgesteld.

- de informatiebeveiligingsmaatregelen gericht op de medewerkers
  - awareness (bewustwording)?

Er is sinds eind 2017 een communicatieplan. De Rekenkamercommissie stelt vast dat op basis daarvan op een goede manier kan worden gewerkt aan ‘awareness’ onder de medewerkers, maar denkt dat daaraan nog veel – en op heel korte termijn – moet worden gedaan. Uiteraard vanuit de Bedrijfs-voeringseenheid en gericht op zowel Maasdriel als Zaltbommel, maar voor wat betreft Maasdriel ook zichtbaar en actief gesteund door de gemeentesecretaris-algemeen directeur en door persoonlijke bemoeienis *in* en *vanuit* het college.

- de status van het Informatie Security Management Systeem
  - incidentregistratie: procedure c.q. systeem?

De Rekenkamercommissie heeft vastgesteld dat er sinds kort een incidentregistratie is ingericht. De komende tijd zal moeten worden beoordeeld in hoeverre medewerkers alle incidenten (en eventuele bijna-incidenten) melden en of die meldingen, na een eerste zichtbare weging, gestructureerd worden opgevolgd. Hiervoor geldt hetzelfde als wat bij het vorige punt is opgenomen: er is beslist behoefte aan merkbare aandacht vanuit het hoogste ambtelijke niveau en vanuit het college van de gemeente Maasdriel.

- zelfreflectie / GAP analyse – ofwel, hoe staan we ervoor versus de standaarden
  - nulmeting en/of GAP analyse-document?

De Rekenkamercommissie stelt vast dat er een zogenoemde GAP-analyse is uitgevoerd. Die is echter (nog) niet vertaald in een veranderplan, waarin specifieke en zichtbaar afgewogen prioriteiten zijn gesteld. In algemene zin zijn de diverse documenten en procedures ingericht, maar moet een eenduidige, cyclische benadering nog (nader) worden vormgegeven: nulmeting c.q. GAP-analyse, verbeterplan voor een bepaalde periode, vast-frequente voortgangsrapportages over de voortgang van het verbeterplan en een vertaling in een aangepast verbeterplan voor een volgende periode (waarbij expliciet wordt vastgesteld welke oorzaken aan niet, niet volledig of niet tijdig gerealiseerde verbeteringen ten grondslag liggen).

Totaalbeeld en suggesties

Informatiebeveiliging is zeker niet alleen een kwestie van procedures maken en die handhaven. Sterker nog: ook met prachtige procedures kan een enorm probleem spelen als een WMO-medewerker een aanvraag van een burger, waarin veel privacygevoelige informatie staat, snel op een niet-beveiligde USB-stick zet ‘om vanavond thuis die beschikking te kunnen afmaken, ik moet nu naar de crèche om mijn zieke kind op te halen’, om die stick vervolgens uit zijn of haar jas of tas te laten glippen.

Is iets menselijks de gemiddelde medewerker van de gemeente Maasdriel vreemd? Nee natuurlijk. Ook de ambtenaar, die ’s morgens bij het thuis weggaan slingers bij de buren ziet hangen en bij een collega van burgerzaken aanwaait om ‘even te kijken hoe oud de buurman is geworden’, vertoont heel logisch gedrag. Maar: dergelijk gedrag is verboden onder de AVG, en waarschijnlijk ook om andere redenen onwenselijk. Soortgelijke issues kunnen en zullen uiteraard ook voor de leden van het college en de raad spelen.

Terug naar de vier normen, die de Rekenkamercommissie eerder in dit document aan het VNG-citaat heeft gekoppeld. Zoals gebruikelijk verbindt de Rekenkamercommissie aan haar centrale bevindingen enkele suggesties voor de raad. Als volgt:

1. De Rekenkamercommissie heeft willen vaststellen in hoeverre het onderwerp 'beveiliging van informatie' de aantoonbare, actieve aandacht van het college heeft.

De Rekenkamercommissie ervaart de persoonlijke betrokkenheid van de portefeuillehouder van Maasdriel, dat is burgemeester Henny van Kooten, maar zou graag zien dat het onderwerp vaker en explicieter letterlijk op de agenda van het college van Maasdriel staat, mede met de intentie om

(1) doorlopend ook de andere collegeleden bij de opzet en werking van het geïmplementeerde instrumentarium betrokken te houden en

(2) doorlopend gericht te kunnen schakelen in de zeshoek portefeuillehouder Maasdriel – portefeuillehouder Zaltbommel – algemeen directeur Maasdriel – algemeen directeur Zaltbommel – teammanager informatisering en automatisering van de Bedrijfsvoeringseenheid – CISO.

Uit het frequent agenderen van het onderwerp volgt logischerwijs ook dat de andere collegeleden vaker een halfuurtje in een afdelings- of teambespreking aanschuiven, waarin het onderwerp aan de hand van dagelijkse casuïstiek of dilemma's aan de orde komt. Informatiebeveiliging is van iedereen en gaat iedereen binnen de gemeente Maasdriel immers in hoge mate aan.

De Rekenkamercommissie adviseert de raad (1) de bovenbedoelde specifieke, doorlopende en aantoonbare aandacht van het college te vragen en (2) zich daarover periodiek te laten informeren.

2. De Rekenkamercommissie heeft onderzocht of in de noodzakelijke instrumenten is voorzien.

Ja, zij het dat meerdere stukken nog 'losse eindjes' kennen, die snel zullen moeten worden verbonden. De Rekenkamercommissie heeft daarnaast zorgen over de bezetting-in-continuïteit van de CISO-functie, die op dit moment door een enthousiaste en deskundige, maar weinig ervaren medewerker wordt waargenomen. Het meldsysteem voor incidenten is pas sinds kort operationeel.

Hoewel in zekere zin een operationeel punt: de Rekenkamercommissie adviseert de raad bij het college te vragen naar de wijze waarop voor de komende jaren structureel wordt voorzien in een blijvend adequate invulling van de CISO-positie (logischerwijs blijvend binnen de Bedrijfsvoerings-eenheid Bommelerwaard).

3. De Rekenkamercommissie heeft willen beoordelen op welke wijze het onderwerp 'beveiliging van informatie' de actieve aandacht van alle medewerkers van de gemeente heeft, waar aan de orde met expliciet zichtbare bestuurlijke betrokkenheid. Daarbij is het de intentie ook te bezien in hoeverre medewerkers zich vrij voelen om risico's en eventuele incidenten te melden: niet met de dreiging om ergens in welke vorm dan ook voor te worden gestraft, maar juist om een cultuur te stimuleren waarin betrokkenen op het gebied van informatiebeveiliging hun kwetsbaarheden tonen, waarvan door henzelf en anderen gericht kan worden geleerd.

Op dit punt heeft de Rekenkamercommissie geen vaststellingen kunnen doen.

De Rekenkamercommissie adviseert de raad om zich periodiek en gericht over de invulling van het communicatieplan te laten informeren. In dat verband moet ook beslist worden bewaakt dat medewerkers knelpunten, dilemma's en incidenten 'veilig' kunnen melden en dat ook doen.

Aanvullend adviseert de Rekenkamercommissie de raad om via de griffie te (laten) vaststellen op welke manier ook raadsleden risico's en onverhoopte incidenten kunnen melden, bespreken en in leerpunten kunnen omzetten.

4. De Rekenkamercommissie stelt graag vast – maar dat kan pas feitelijk bij de behandeling van dit memorandum – in hoeverre de raad de eerder in dit memorandum bedoelde controle (1) met de vereiste diepgang kan uitoefenen en (2) dat ook aantoonbaar doet, bijvoorbeeld door het stellen van vragen aan het college of het bijwonen van presentaties of informatiebijeenkomsten.

De hierboven gekozen woorden geven het al aan: de Rekenkamercommissie gaat hierover (nog) graag met de raad in gesprek.

**

Rekenkamercommissiecommissie Maasdriel
Beveiliging van informatie
22 januari 2018
Bijlage

Bijlage

Ambtelijk-bestuurlijke reactie

Verzonden: maandag 19 februari 2018 19:58
Aan: Frank Hordijk (Hordijk & Hordijk) <frank@hordijk.org>
CC: Henny van Kooten <H.vanKooten@maasdriel.nl>;

Onderwerp: FW: Concept-memorandum Rekenkamercommissie - informatie

Beste heer Hordijk,

De rekenkamercommissie verzocht de ambtelijke organisatie een inhoudelijke reactie te geven op de constateringen in het Memorandum. De teammanager Informatie & Automatisering en de Interim CISO verzorgden de inhoudelijke reactie die hieronder is weergegeven en eveneens is aangeboden aan het College van Maasdriel.

Blz 11 – eerste bullet:

Onze incidentregistratie loopt al vanaf 1 januari 2017. In september 2017 stapten we over op een incidentenregistratie in Topdesk om een betere historie/kennisbank op te kunnen bouwen en omdat Topdesk ook logging biedt. Daarnaast kunnen we vanuit Topdesk beter sorteren op de verschillende categorieën waarin incidenten ingedeeld kunnen worden. Waarschijnlijk hebben we het in het gesprek met de Rekenkamercommissie over de registratie in Topdesk gehad, waardoor het lijkt of de incidentregistratie pas sinds kort is ingericht.

Blz 11 – tweede bullet:

Het vertalen van de GAP-analyse in een veranderplan was op het moment van het onderzoek inderdaad nog niet gebeurd. Dit omdat er door het uitvallen van de CISO tijdelijk minder capaciteit beschikbaar was. Inmiddels vertaalden we de GAP-analyse in een Informatiebeveiligingsplan 2018. Dit plan hoort bij het Informatiebeveiligingsbeleid 2018-2019 en is inmiddels ook aan de orde geweest in het gezamenlijk MT Maasdriel-Zaltbommel.

Rekenkamercommissiecommissie Maasdriel
Beveiliging van informatie
22 januari 2018
Bijlage

Algemeen:

Burgemeester Van Kooten wees op André Biesheuvel (Duthler Associates) als een autoriteit op het gebied van de AVG en privacy bewustzijn. Dit als gevolg van de aanbeveling dat het onderwerp informatiebeveiliging en privacy aantoonbare en actieve aandacht van het college zou moeten hebben. Inmiddels is er een gesprek geweest met de heer Biesheuvel over dit onderwerp. Naar aanleiding van dit gesprek leverde Duthler Associates een voorstel aan en deed het aanbod voor een bewustwordingscampagne met betrekking tot privacy en de Algemene Verordening Gegevensbescherming (AVG) die op 25 mei 2018 in werking treedt. Ze richten zich hierbij op bewustwording bij het bestuur en de directie.
Daarnaast hebben ze een voorstel gedaan om het volwassenheidsniveau op het gebied van privacy te bepalen en vast te leggen in een verklaring van accountability. Met de verklaring van accountability wordt aangegeven hoe een organisatie 'in control' is en hoe de verplichtingen vanuit wetgeving worden nageleefd. Daarnaast biedt het een handvat om de vooruitgang in volwassenheid op het gebied van privacy te monitoren, te plannen en te bewaken.

Mochten er over bovenstaande nog vragen zijn, dan horen wij deze graag.

**